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

№ 11 (листопад)

Київ – 2020

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., 2020– №11 (листопад) . – 281с.

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, 2020

© Національна бібліотека України імені В.І. Вернадського, 2020

ЗМІСТ

Стан кібербезпеки в Україні 4
Національна система кібербезпеки 10
Правове забезпечення кібербезпеки в Україні 11
Кібервійна проти України 12
Боротьба з кіберзлочинністю в Україні 15
Міжнародне співробітництво у галузі кібербезпеки 18
Коронавірус COVID-19 та питання кібербезпеки 19
Світові тенденції в галузі кібербезпеки 27
Сполучені Штати Америки 47
Країни ЄС 51
Російська Федерація та країни ЄАЕС 54
Інші країни 65
Протидія зовнішній кібернетичній агресії 67
Створення та функціонування кібервійськ 78
Кіберзахист критичної інфраструктури 80
Захист персональних даних 81
Кібербезпека Інтернету речей 126
Кіберзлочинність та кібертерроризм 129
Діяльність хакерів та хакерські угруповування 173
Вірусне та інше шкідливе програмне забезпечення 185
Операції правоохоронних органів та судові справи проти кіберзлочинців 246
Технічні аспекти кібербезпеки 247
Виявлені вразливості технічних засобів та програмного забезпечення 249
Технічні та програмні рішення для протидії кібернетичним загрозам 270

«У Києві стартувало навчання «Bug Bounty», організоване Національним координаційним центром кібербезпеки при РНБО України за підтримки Фонду цивільних досліджень та розвитку США (CRDF Global).

Про це повідомляє пресслужба РНБО.

У РНБО відзначили, що програма реалізується спільно з приватною компанією CyberUnit.

“Представники основних суб’єктів забезпечення кібербезпеки України та працівники критичної інфраструктури протягом п’яти днів здобуватимуть навички проведення пентесту об’єктів критичної інфраструктури, створення комплексної системи захисту таких об’єктів і посилення власних технічних спроможностей”, – йдеться у повідомленні.

За словами заступника секретаря РНБО Сергія Демедюка, щодня у кіберпросторі виникають нові тенденції і нові загрози, і українські фахівці разом із закордонними партнерами спільно працюють над тим, аби вчасно реагувати на них і попереджувати у майбутньому.

“Такі практичні навчання є невід’ємною складовою вдосконалення національної системи кібербезпеки. Обмін досвідом є запорукою великих спільних досягнень”, – додали в РНБО». ***(Галина Мельник. В Україні запустили навчання за програмою для “білих хакерів” // #ШоТам (https://shotam.info/v-ukraini-zapustyly-navchannia-za-prohramoiu-dlia-bilykh-khakeriv/). 10.11.2020).***

***

«…У дайджесті з кібербезпеки OLX пояснює, з чого складається багатоетапний процес захисту користувачів платформи і попереджає про нову шахрайську схему. Значення безпеки в онлайні навряд чи можна переоцінити. Адже в інтернеті ми лишаємо персональну інформацію та витрачаємо кошти. І звісно є ті, хто не проти цим скористатися. Завадити їм можуть технологічні рішення, які запроваджують компанії, та кіберграмотність користувачів.

Аби питання онлайн-безпеки на платформі стали українцям більш зрозумілими, OLX розповів про те, з яких елементів складається безперервний процес захисту користувачів. Контроль у два етапи — підозрілі не пройдуть Перш ніж оголошення потрапляють на платформу, вони проходять автоматичну модерацію. Їх перевіряють на відповідність правилам платформи приблизно за сотнею різноманітних параметрів. За статистикою компанії, через модерацію проходять понад 130 тисяч нових оголошень на день. В результаті 88% з них потрапляють на сайт. Решта проходять більш глибинну перевірку моделями штучного інтелекту (ШІ) та ручну модерацію. Наприклад, завдяки ручній перевірці в середньому блокуються понад 3 тисяч оголошень на день. Ще одна складова захисту — щоденний аналіз поведінки приблизно 15 тисяч підозрілих акаунтів (зареєстрованих користувачів) на предмет фішингу, щоб потім виявити потенційних шахраїв. Якщо ШІ з високою ймовірністю визначає чиїсь дії як підозрілі, їхні акаунти автоматично блокуються.

Боротьба з фішингом — загальносвітова тенденція, адже з цим видом шахрайства стикається величезна кількість міжнародних компаній. Так, за даними Brand Phishing Report за 3 квартал 2020 року, трійка брендів, на які відбувалося найбільше фішингових атак, — Microsoft (19% від глобальної кількості), DHL (9%) та Google (9%). Головна мета фішингу — отримати особисту інформацію або платіжні дані людини. Які питання з безпеки в онлайні цікавлять українців найбільше? З настанням карантину люди активніше почали обирати онлайн-шопінг. Підвищення інтересу до нього підтверджують і дані OLX: кількість активних користувачів платформи навесні одразу зросла на 6%.

Та разом із розвитком шопінгу в мережі збільшуються апетити шахраїв. Згідно з даними дослідження CBR 1, 29% українців стикалися із шахраями під час покупок в інтернеті. Тому OLX розповідає українцям активніше про кіберграмотність. Так, головну сторінку центру підтримки клієнтів OLX з корисною інформацією як захиститися від шахраїв у липні відвідали на 8% більше людей, ніж попереднього місяця. У серпні їхня кількість зросла ще на 19%, а у вересні — ще на 20%.

Загалом в останні пів року українці найбільше цікавилися такими питаннями:

● безпечні покупки
● доставка
● приватність
● захист особистих даних

“Ми в OLX постійно працюємо над удосконаленням кіберзахисту на платформі, щоб наші користувачі могли здійснювати безпечні угоди. Однак варто пам’ятати, що захищеність в онлайні залежить від кожного з нас. Шахраї використовують методи соціальної інженерії. Вони добре знають, якими діями та словами схилити “клієнта” до швидкої та необдуманої угоди. Коли користувачі більше цікавляться безпекою у мережі та прокачують свої знання, а компанії створюють власні ініціативи, можна ефективніше боротися з шахраями та насолоджуватися безпечним онлайн-шопінгом”, — коментує Віктор Нобіуз, керівник відділу бізнес-аналітики OLX Україна.

А що по схемах шахрайства?

Зараз шахраї активно переключилися на продавців і використовують схему з підробленим посиланням: псевдопокупець пише продавцеві в чаті онлайн-платформи, запитує про товар і пропонує для зручності перейти в інший месенджер. Коли він опиняється за межами платформи, то повідомляє, що зважився на покупку і вже сплатив товар. Відправляє посилання на сайт-копію нібито для отримання оплати. Продавець вводить всі дані платіжної картки, і сума списується з його рахунку.

Важливо пам’ятати, що в послузі OLX Доставка такого функціоналу не існує: для її оформлення та отримання оплати не потрібні сторонні посилання. Єдине, що продавець може повідомити покупцеві, — це 16-значний номер картки та ПІБ, причому останнє необов’язково.

Базові правила, що допоможуть продавати та купувати безпечно:

1. Ставтеся з обережністю до занадто привабливих пропозицій.

2. Не покидайте офіційний чат платформи та не переходьте за зовнішніми посиланнями, отриманими від сторонніх осіб.

3. Користуйтеся безпечними сервісами доставки на кшталт OLX Доставка.

4. Перевіряйте сайт на якому плануєте здійснити чи отримати оплату.

5. Ніколи не розкривайте всі персональні та платіжні дані, особливо незнайомцям». ***(Щодня блокуємо 3 тисячі оголошень після ручної перевірки — OLX розповів, як створюється безпека в онлайні // ОКІА "Новини Полтавщини" (https://np.pl.ua/2020/11/shchodnia-blokuiemo-3-tysiachi-oholoshen-pislia-ruchnoi-perevirky-olx-rozpoviv-iak-stvoriuiet-sia-bezpeka-v-onlayni/). 05.11.2020).***

***

«Национальный оператор связи «Киевстар» сообщает, что разработал и внедрил новую услугу для противодействия кибермошенничеству, аналогов которой, как утверждается, нет в Украине – «Защита альфанумерических имен». Это сервис для бизнес-клиентов, с помощью которого отслеживаются и блокируются SMS-сообщения с фишинговых ресурсов. Он призван защитить пользователей от «похищения» личной информации и возможных материальных убытков.

Альфанумерическое имя – это буквенная или цифровая подпись, которая отображается в строке отправителя SMS. Его защита может быть полезна всем компаниям и учреждениям, которые используют в работе SMS, такие как банки, почтовые операторы, ритейл, представители сферы услуг и др. Чаще всего фишинговые SMS отправляются с использованием коммерческих наименований и торговых марок известных на рынке компаний. Потому в ряде сообщений со схожих альфа-имен абоненты могут не заметить разницы и автоматически предоставить мошенникам данные о себе либо своем банковском счете.

При отправке SMS абонентам «Киевстар» оператор будет совершать постоянный мониторинг и контроль за использованием альфанумерических имен или их вариаций только партнером, а не третьим лицом. Доставка абонентам SMS, где используются оригинальные и визуально похожие альфанумерические имена партнера, которые приходят от лиц, не уполномоченных на такие рассылки, будет блокироваться автоматически». ***(«Киевстар» поможет розничным бизнесам защитить клиентов от фишинговых SMS // Компьютерное Обозрение(https://ko.com.ua/kievstar_pomozhet_roznichnym_biznesam_zashhitit_klientov_ot_fishingovyh_sms_135105). 02.11.2020).***

***

«Вчора, 11 листопада, начальник Департаменту кіберполіції Олександр Гринчак та директор асоціації «Інформаційні технології України» Костянтин Васюк підписали меморандум про співпрацю.

Сторони мають на меті забезпечити взаємний обмін інформацією та досвідом у сфері безпечного використання інформаційних і телекомунікаційних систем, а також запобігання витоку в Інтернеті інформації з обмеженим доступом, персональних даних.

Така співпраця дозволить ефективніше забезпечувати захист прав і свобод громадян, інтересів суспільства та держави від протиправних посягань у кіберпросторі.

Крім цього, угодою передбачено організацію та проведення спільних освітніх заходів, науково-практичних конференцій, семінарів, нарад тощо. У межах своїх повноважень сторони розроблятимуть методологію та відповідні рекомендації щодо протидії кібератакам.

«Минулого року ми розробили концепцію розвитку кіберполіції, де один з основних елементів – створення екосистеми безпечного кіберпростору, куди входять, зокрема, і бізнес-структури. Тому для нас заключення меморандумів та налагодження співпраці є пріоритетним питанням для досягнення поставлених цілей» – зазначив очільник Департаменту кіберполіції Олександр Гринчак.

В свою чергу, директор Асоціації «Інформаційні технології України» Костянтин Васюк підкреслив:

«Питання кібербезпеки стосуються не лише бізнес-компаній, а й кожного громадянина, який користується Інтернетом. Розуміючи важливість цього, ми хочемо налагодити співпрацю з тими, хто є професіоналами та представляє державу в сфері кібербезпеки».

Наприкінці заходу полковник поліції Олександр Гринчак висловив сподівання, що спільними зусиллями вдасться суттєво підвищити якість протидії кіберзагрозам у приватному секторі нашої країни». ***(Кіберполіція співпрацюватиме з асоціацією «Інформаційні технології України» для ефективнішої протидії кіберзлочинам // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-spivpraczyuvatyme-z-asocziacziyeyu-informaczijni-texnologiyi-ukrayiny-dlya-efektyvnishoyi-protydiyi-kiberzlochynam-2712/). 12.11.2020).***

***

«Приватні енергетичні компанії, які належать до об’єктів критичної інфраструктури, активно співпрацюють з РНБО щодо кіберзахисту.

Про це в коментарі Укрінформу повідомив заступник секретаря Ради нацбезпеки та оборони України Сергій Демедюк, відповідаючи на запитання, чи дозволяють енергетичні компанії, які перебувають у приватній власності та належать до об’єктів критичної інфраструктури, контролювати державі стан їхнього захисту.

«Не всі хочуть, щоб держава втручалася у певних питаннях у їхню діяльність, але що стосується забезпечення кібербезпеки, то з приватними компаніями у нас дуже хороша взаємодія, і вони самі бажають, щоб їм надавали певні консультації, певну методичну допомогу. З деякими ми ведемо переговори, щоб ми змогли їм забезпечувати відповідний кіберзахист в тих функціях, які належать до Національного координаційного центру», - повідомив Демедюк.

Він також нагадав, що Національний координаційний центр кібербезпеки активно співпрацює з приватним сектором, оскільки саме там початково відпрацьовуються кібератаки перед тим, як вони здійснюються на державні органи влади та об’єкти критичної інфраструктури. Приватний сектор допомагає тестувати

різного роду програмне забезпечення на предмет виявлення вразливостей чи шкідливого коду та нових методів захисту систем, щоб надалі ці знання використовувати для захисту державних установ.

Заступник секретаря РНБО також поінформував, що до кінця поточного року відбудеться ще один практичний захід для фахівців з кіберзахисту, а також тематична лекція…». ***(Приватні енергокомпанії співпрацюють з РНБО щодо кіберзахисту // Укрінформ (https://www.ukrinform.ua/rubric-economy/3132660-privatni-energokompanii-spivpracuut-z-rnbo-sodo-kiberzahistu.html). 09.11.2020).***

***

«Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (ДЦКЗ Держспецзв'язку) проведе діагностичний аудит в комунікаційних системах Державного підприємства «ДІЯ».

…це передбачає Меморандум про організацію взаємодії у сферах кібербезпеки та кіберзахисту, підписаний Держцентром кіберзахисту та ДП «ДІЯ», повідомляється на сайті Держспецзв'язку.

«Першочерговими заходами взаємодії передбачено проведення діагностичного аудиту інформаційної безпеки інформаційної інфраструктури з метою: визначення стану відповідності ISO/IEC 27001; визначення ризиків інформаційної безпеки та підготовки рекомендацій, у т.ч. в частині застосування сервісів кіберзахисту технологічної інфраструктури Державного центру кіберзахисту Державної служби спеціального зв’язку та захисту інформації України; надання допомоги у ідентифікації та оцінки критичності об’єктів інформаційної інфраструктури Державного підприємства “ДІЯ” та віднесенні їх до певної категорії», - йдеться в повідомленні.

Зазначається, що Меморандум укладено для об’єднання зусиль та досягнення спільного результату у сфері забезпечення кібербезпеки, кіберзахисту та реагування на ймовірні інциденти інформаційної безпеки, виявлених в комунікаційних системах Державного підприємства «ДІЯ».

Очікуваним результатом спільної діяльності стане підвищення рівня кіберзахисту інформаційної інфраструктури Державного підприємства «ДІЯ», ефективності обміну інформацією про кіберзагрози та кіберінциденти між державним підприємством «ДІЯ» та урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA…». ***(Держспецзв'язку проведе діагностичний аудит у комунікаційних системах «ДІЇ» // Укрінформ (https://www.ukrinform.ua/rubric-economy/3144475-derzspeczvazku-provede-diagnosticnij-audit-u-komunikacijnih-sistemah-dii.html). 27.11.2020).***

***

«Міністерство цифрової трансформації України запропонує хакерам з усього світу спробувати зламати мобільний застосунок "Дія"

Тим, хто знайде вразливості в застосунку, обіцяють виплатити 1 млн гривень, саме стільки становить призовий фонд. Про це повідомив на своїй сторінці в Facebook голова міністерства Михайло Федоров.

«Мінцифри запускає багбаунті з пошуку вразливостей у застосунку „Дія“ з призовим фондом 1 млн грн. Ми постійно працюємо над посиленням безпеки застосунку. Для нас надзвичайно важливо, щоб користувачі були впевнені в захищеності своїх персональних даних», — зазначив Федоров.

За його словами, зараз міністерство фіналізує деталі про правила багбаунті, умови участі та класифікацію типів вразливостей за категоріями. А в грудні буде відкрито прийом заявок.

Взяти участь у пошуку вразливостей зможуть «білі хакери з усього світу».

«Плануємо провести багбаунті для білих хакерів з усього світу на платформі Bugcrowd — це одна з найвідоміших міжнародних компаній, що спеціалізується на кібербезпеці та багбаунті-програмах», — уточнив Федоров.

За його словами, весь процес відбуватиметься онлайн.

Призовий фонд складе $ 35 тисяч або 1 млн гривень. Нагороди будуть розподілені за 5 категоріями вразливостей: від найменш до найбільш небезпечних.

Міністр також запевнив, що персональним даним користувачів застосунку ніщо не загрожує.

«Чи загрожує багбаунті застосунку „Дія“? Ні. Білі хакери ламатимуть „тестовий застосунок“. Ми створимо окреме середовище для пошуку багів, яке не буде містити персональні дані», — розповів Федоров». ***(Мільйон за атаку: Мінцифри пропонує хакерам зламати «Дію» за винагороду // Високий Замок Online (https://wz.lviv.ua/news/425113-milion-za-ataku-mintsyfry-proponuie-khakeram-zlamaty-diiu-za-vynahorodu). 28.11.2020).***

***

«Нещодавно Український фонд стартапів оголосив переможців конкурсу стартапів. Найближчим часом збираються профінансувати 7 проєктів, кожен із яких отримає по 25 або 50 тис. доларів на реалізацію.

Як розповіли 032.ua у пресслужбі УФС, загалом на конкурсі презентувлаи 32 стартапи. Серед них обрали 5, які перебувають на етапі pre-seed (грант 25 000 доларів) та 2 - на етапі seed (грант 50 000 доларів). Українці запропонували такі ідеї:

RE-leaf PAPER - крафтовий папір, який виготовлений за технологією RE-leaf, на основі волокнистої маси із опалого листя;

iceFood - заморожені ready-to-eat здорові та корисні перші страви, другі страви, десерти, смузі та хелсі боули, на приготування яких достатньо 3-5 хв;

AI Impulsar - програмне забезпечення Impulsar може "зазирнути в майбутнє" і врятувати життя. Impulsar допомагає контролювати і аналізувати стан людей з аутизмом та деменцією, і заздалегідь сповіщає людей з епілепсією про ймовірність розвитку кризового стану;

Muscreators - онлайн-сервіс для ефективного та масштабного промоушену артиста. Надає готові рішення для ефективних промо кампаній на світові та локальні ринки. Muscreators - надійний міст між артистом та фаном через media канали по всьому світу;

Smart Way - сервіс для міжнародних перевезень. Мобільний додаток для: водія, перевізника, відправника/отримувача товару, з метою швидкого

проходження кордону, замовлення онлайн митних послуг та отримання корисних сервісів в дорозі. Мобільний додаток для для простої взаємодії з митницею на кордоні;

eSalesPlatform - e-commerce платформа, що допомагає ритейлеру розширити ринки збуту на міжнародні маркетплейси, такі як Amazon та eBay;

HackenAI - мобільний додаток для особистої кібербезпеки. ХакенAI поєднує в собі найбільш необхідні засоби кібербезпеки, такі як парольний менеджер, моніторинг скомпроментованих аккаунтів, двохфакторна аутентифікація, ВПН, захищене хранилище, антифішинг та багато іншого. Інтерактивні навчальні модулі, нагороди, предмети колекціонування мотивуватимуть користувачів більш відповідально відноситись до своєї особистої кібербезпеки та навчатимуть їх найкращих практик, щоб уникнути майбутніх проблем». ***(Євгенія Пласконь. Крафтовий папір, заморожені страви та Impulsar: які стартапи підтримають в Україні // 032.ua - Сайт міста Львова (https://www.032.ua/news/2948426/kraftovij-papir-zamorozeni-stravi-ta-impulsar-aki-startapi-pidtrimaut-v-ukraini). 24.11.2020).***

***

Національна система кібербезпеки

«Заступники Голови Держспецзв'язку Олександр Потій та Володимир Трофименко представили колективу Державного центру кіберзахисту Держспецзв'язку нового керівника – полковника Андрія Кузміча.

Олександр Потій, вітаючи нового керівника ДЦКЗ, побажав йому успіхів у подальшій роботі та наголосив на стратегічній важливості Державного центру кіберзахисту Держспецзв'язку і Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA в захисті національної кібербезпеки. «Державний центр кіберзахисту та CERT-UA сьогодні – наш форпост у забезпеченні кібербезпеки об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури. Відповідно до нової концепції реформування Держспецзв'язку буде передбачене нарощування потужностей ДЦКЗ, зокрема технічне оснащення та посилення взаємодії з іншими суб'єктами національної системи кібербезпеки, з органами державної влади та бізнесу. В ДЦКЗ та CERT-UA працюють унікальні фахівці, наш інтелектуальний потенціал, справжні фанати своєї справи. Бережіть їх», – сказав Олександр Потій». ***(Відбулось представлення нового керівника Державного центру кіберзахисту Держспецзв'язку // ITUA.info (http://itua.info/internet/40311.html). 11.11.2020).***

***

«В Україні розпочато реалізацію фінансованого Євросоюзом проекту EU4DigitalUA з бюджетом 9,6 млн євро.

Його метою є підтримка українського уряду в подальшій цифровій трансформації країни. Керуватиме процесом імплементації та досягнення цілей Естонська Академія електронного урядування (e-Governance Academy).

Установча зустріч нового проекту відбулася 25 листопада. «Ми вдячні ЄС за підтримку цифрової трансформації України. Вже понад рік команда Мінцифри будує цифрову державу. Цифрова трансформація є ключем до реформи будь-якої сфери. Ми вже це продемонстрували на прикладі галузі містобудування та адміністративних послуг. Підтримка цифрової трансформації в Україні — це одночасно підтримка всіх ключових реформ і антикорупційної діяльності. Ми готові обмінюватись досвідом з іншими країнами та щодня вдосконалювати проекти, над якими працюємо. Завдяки допомозі ЄС Україна отримає більше якісних змін», — заявив віце-прем'єр-міністр — міністр цифрової трансформації України Михайло Федоров, повідомляє Урядовий портал.

Назву EU4DigitalUA можна перекласти як «ЄС для цифрової України». Проект концентруватиметься на подальшому розвитку надання державних послуг онлайн, зміцнення кібербезпеки та безпеки персональних даних. Він значною мірою базуватиметься на результатах проекту EGOV4Ukraine, також фінансованого ЄС та низкою його держав-членів. Зокрема, в рамках того проекту протягом 2014—2020 років було створено та запущено систему безпечного обміну даними «Трембіта», яка забезпечує взаємодію між електронними реєстрами органів виконавчої влади та місцевого самоврядування.

Новий проект EU4-DigitalUA є частиною ширшої програми підтримки української цифрової трансформації та гармонізації з Єдиним цифровим ринком ЄС із загальним бюджетом 25 млн євро. «ЄС підтримує подальший розвиток цифрових технологій в Україні з метою підвищення конкурентоспроможності країни і сприяння подальшому наближенню України до Єдиного цифрового ринку ЄС», — зауважив під час установчого засідання голова Представництва ЄС в Україні Матті Маасікас.

«Ми застосовуємо передовий досвід, отриманий при розбудові «цифрового уряду» Естонії, щоб допомогти Україні в подальших кроках до створення більш прозорого і ефективного суспільства», — наголосив Ханнес Асток, виконавчий директор Академії електронного управління.

Проект EU4DigitalUA реалізується спільно Академією електронного управління (Естонія) і Міжнародним та Іберо-американським фондом державного управління і громадської політики (Іспанія). Він триватиме до березня 2024 року». ***(ЄС надасть Україні 25 млн євро на цифрову трансформацію // Голос України (http://www.golos.com.ua/article/338932). 27.11.2020).***

***

Правове забезпечення кібербезпеки в Україні

«Кабінет Міністрів схвалив законопроєкт "Про внесення змін до деяких законів України", відповідно до якого Державна служба спеціального зв'язку та захисту інформації України буде зобов'язана зберігати резервні копії державних електронних інформаційних ресурсів.

Як передає кореспондент Укрінформу, відповідне рішення уряд ухвалив на засіданні 11 листопада.

Згідно з текстом пояснювальної записки, зазначений законопроєкт вносить зміни до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» та Закону України «Про основні засади забезпечення кібербезпеки України» з метою покладення на Державну службу спеціального зв'язку та захисту інформації обов'язків щодо збереження резервних копій інформації та відомостей державних електронних інформаційних ресурсів та виправлення технічних помилок у частині вживання термінів «кібербезпека» та «кіберзахист».

Таким чином в Україні на законодавчому рівні буде врегульовано питання щодо здійснення резервного копіювання інформації та відомостей державних електронних інформаційних ресурсів державними органами, військовими формуваннями, утвореними відповідно до законів України, державними підприємствами, установами та організаціями, а також питання щодо централізованого зберігання службою цих копій». ***(Держспецзв'язку можуть зобов'язати зберігати резервні копії // Ваші новини (https://news.vash.ua/news/polityka/derzhspetszvyazku-mozhut-zobovyazaty-zberigaty-rezervni-kopiyi-80306). 11.11.2020).***

***

Кібервійна проти України

«Другий день поспіль заблокована робота сайту Уповноваженого ВРУ з прав людини через чергові сторонні хакерські атаки. Про це у Facebook написала омбудсмен Людмила Денісова…

Вона зазначила, що всю актуальну інформацію можна прочитати на публічних сторінках у Facebook та Telegram.

…через постійні кібератаки у травні також було заблоковано роботу сайту Омбудсмена…». ***(Антоніна Карташева. Хакерські атаки заблокували роботу сайту Омбудсмена – Денісова // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1901996-khakerski-ataki-zablokuvali-robotu-saytu-ombudsmena-denisova). 10.11.2020).***

***

«З 4 по 11 листопада було зафіксовано та заблоковано 14 DDoS-атак, переважна більшість — на вебресурси Національного антикорупційного бюро України…

Повідомляється, що система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала 1 594 221 підозрілих подій, що на 21% менше, ніж попереднього тижня. Переважна більшість зафіксованих підозрілих подій стосується спроб мережевого сканування (92%) та застосування нестандартних протоколів (7%).

"Система захищеного доступу державних органів до мережі Інтернет заблокувала 38 662 атак різних видів, що на рівні кількості атак, заблокованих попереднього тижня. Переважна більшість — це мережеві атаки прикладного рівня

(99%). Також зафіксовано і заблоковано 14 DDoS-атак (переважна більшість — на вебресурси НАБУ)", — йдеться в повідомленні.

Окрім того, урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 2 047 кіберінцидентів, що на рівні кількості кіберінцидентів, опрацьованих попереднього тижня.

"Переважна більшість опрацьованих інцидентів стосується недержавного сектору (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (97%)", — зазначається в повідомленні…». ***(Анна Мурашко. За тиждень зареєстровано низку кібератак на сайт НАБУ // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1901994-za-tizhden-zareyestrovano-nizku-kiberatak-na-sayt-nabu). 10.11.2020).***

***

«Цілеспрямованих масових кібератак під час проведення місцевих виборів в Україні 25 жовтня зафіксовано не було.

Про це повідомив заступник секретаря РНБО України Сергій Демедюк…

Чиновник зазначив, що аналіз та моніторинг продовжується.

"Під час виборів цілеспрямованих масових атак не зафіксовано. Ми сьогодні також продовжуємо аналіз та моніторинг таких можливих спроб, і їх, на щастя, не фіксується і потенційно ми не прогнозуємо. Це, можливо, пов'язано з тим, що у різних регіонах відбувається основний підрахунок, і завершальний етап відбувається на території, яка не входить у єдину інформаційну систему ЦВК. Тому я думаю, що це з цим пов'язано", – повідомив Демедюк…» ***(Під час місцевих виборів цілеспрямованих масових кібератак не зафіксовано, – РНБО // UA|TV (https://uatv.ua/pid-chas-mistsevyh-vyboriv-tsilespryamovanyh-masovyh-kiberatak-ne-zafiksovano-rnbo/). 09.11.2020).***

***

«Хакери найчастіше атакують органи енергетичної галузі, зв'язку та телекомунікації.

Про це розповів очільник Державної служби спеціального зв'язку та захисту інформації України Юрій Щиголь…

Найбільший інтерес зловмисники проявляють, насамперед, до об'єктів критичної інфраструктури, а також до ресурсів, на яких обробляються персональні дані.

За словами голови Держспецзв'язку, географія кібератак різноманітна, проте найбільше таких втручань фіксується з Російської Федерації.

"Зрозуміло, що основна причина проблем – країна-агресор, вона найактивніша в розрізі хакерських атак і зламів мережі. Але географічні дані щодо аномалій мереж складно структурувати, бо часто визначити справжнє джерело атаки неможливо. Не обов'язково вони відбуваються зі, скажімо, території Росії. Безпосередні виконавці можуть працювати з будь-якої точки земної кулі, й країни, з яких працюють хакери, не завжди за це відповідальні", – розповів Юрій Щиголь». ***(Найбільше хакерських атак на українські держоргани відбувається з Росії, –***

очільник Держспецзв'язку // UA|TV (https://uatv.ua/najbilshe-hakerskyh-atak-na-ukrayinski-derzhorgany-vidbuvayetsya-z-rosiyi-ochilnyk-derzhspetszv-yazku/). 06.11.2020).

***

«У Києві хакери за допомогою комп'ютерного вірусу заволоділи нежитловою будівлею в центрі міста площею 250 кв. м.

Як повідомляє Міністерство внутрішніх справ, шахраї відправили державному нотаріусу електронного листа з вірусом. Після його відкриття вони отримали віддалений доступ до комп'ютера нотаріуса і змінили дані в Держреєстрі прав власності на нерухоме майно.

Хакери відписали будівлю «замовнику», якого вже встановили правоохоронці. В його будинку із залученням бойового спецпідрозділу провели обшуки. У будинку вилучили комп'ютери, на яких збереглися дані про втручання в роботу реєстру.

Поліція розслідує справу за статтею про шахрайство (ч. 3 ст. 190 КК). Причетним загрожує до 8 років в'язниці…». ***(Поліція викрила групу хакерів, які заволоділи будівлею в центрі Києва за допомогою вірусу // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/25881/2020-11-03-politsiya-vikrila-grupu-khakeriv-yaki-zavolodili-budivleyu-v-tsentri-kieva-za-dopomogoyu-virusu/). 03.11.2020).***

***

«За тиждень з 18 по 24 листопада система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала більше 1,7 млн підозрілих подій, що на 11% менше за попередній тиждень…

"Система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала 1 714 146 підозрілих подій (з 18 по 24 листопада), що на 11% менше ніж попереднього тижня. Переважна більшість зафіксованих підозрілих подій стосується спроб мережевого сканування (91%), застосування нестандартних протоколів (7%)", - йдеться у повідомленні.

Зазначається, що система захищеного доступу державних органів до мережі Інтернет заблокувала 47 337 атаки різних видів, що на 2% більше, ніж попереднього тижня. Переважна більшість - це мережеві атаки прикладного рівня (95%) та атаки типу "Harvest Attack" (3%). Також зафіксовано і заблоковано 3 DDoS-атаки.

"Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 1 866 кіберінцидентів, що на 39% менше, ніж попереднього тижня. Переважна більшість опрацьованих інцидентів належить доменній зоні UACOM (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (98%)", - йдеться у повідомленні…». ***(Антоніна Карташева. За тиждень зафіксовано більше 1,7 млн кібератак на державні інформаційні ресурси // Інформаційне агентство «Українські***

Національні Новини (https://www.unn.com.ua/uk/news/1904373-za-tizhden-zafiksovano-bilshe-1-7-mln-kiberatak-na-derzhavni-informatsiyni-resursi). 24.11.2020).

***

Боротьба з кіберзлочинністю в Україні

«Служба безпеки України затримала групу хакерів, які торгували відповідями на екзаменаційні білети у вишах Вінницької області. За версією СБУ, кіберзлочинці скоювали атаки на системи навчальних закладів і заволодівали файлами з відповідями.

«Зловмисники протиправно змінювали офіційну інформацію навчальних закладів та отримували доступ до файлів, які містять, зокрема, відповіді на екзаменаційні білети. Незаконно отриману інформацію реалізовували за грошову винагороду. Для блокування роботи вишів під час складання іспитів, організатори також здійснювали DDoS-атаки на інформаційно-телекомунікаційні системи навчальних закладів»

— Служба безпеки України

Правоохоронці відкрили кримінальну справу за ч. 2 ст. 361 ККУ та провели обшуки у помешканнях хакерів…» ***(Хакери викрали відповіді на екзаменаційні білети: зловмисників затримала СБУ // UA.NEWS (https://ua.news/ua/hakery-pohytyly-otvety-na-ekzamenatsyonnye-bylety-zloumyshlennykov-zaderzhala-sbu/). 10.11.2020).***

***

«…Співробітники відділу протидії кіберзлочинам в Хмельницькій області Департаменту кіберполіції НПУ спільно зі слідчими слідчого управління ГУНП в Хмельницькій області за процесуального керівництва Хмельницької обласної прокуратури викрили жителя Хмельницького, який причетний до несанкціонованого розповсюдження інформації з обмеженим доступом.

Мешканець обласного центру здійснював розповсюдження конфіденційної інформації користувачів мережі Інтернет, серед якої були логіни та паролі доступу до різних інтернет-ресурсів, електронних поштових скриньок, облікових записів соціальних мереж та електронних гаманців.

“Отриману інформацію правопорушник перевіряв на факт відповідності відомостей для входу до різноманітних вебресурсів та в подальшому здійснював розповсюдження одержаних даних на закритих форумах та в одному із популярних месенджерів.

Досудовим розслідуванням встановлено факт розповсюдження фігурантом бази даних, яка містить відомості відносно 2,8 мільйонів авторизаційних даних облікових записів користувачів мережі Інтернет”, – йдеться у повідомленні.

За даним фактом відкрито кримінальне провадження за ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка

зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України». ***(2,8 млн особистих даних: затримали українського хакера, який продавав дані користувачів // ОКІА "Новини Полтавщини" Україна (https://np.pl.ua/2020/11/2-8-mln-osobystykh-danykh-zatrymaly-ukrains-koho-khakera-iakyy-prodavav-dani-korystuvachiv/). 09.11.2020).***

***

«…Співробітники відділу протидії кіберзлочинам в Хмельницькій області Департаменту кіберполіції НПУ спільно зі слідчими слідчого управління ГУНП в Хмельницькій області за процесуального керівництва Хмельницької обласної прокуратури викрили жителя м. Хмельницького, який причетний до несанкціонованого розповсюдження інформації з обмеженим доступом.

Мешканець обласного центру здійснював розповсюдження конфіденційної інформації користувачів мережі Інтернет, серед якої були логіни та паролі доступу до різних інтернет-ресурсів, електронних поштових скриньок, облікових записів соціальних мереж та електронних гаманців.

Отриману інформацію правопорушник перевіряв на факт відповідності відомостей для входу до різноманітних вебресурсів та в подальшому здійснював розповсюдження одержаних даних на закритих форумах та в одному із популярних месенджерів.

Досудовим розслідуванням встановлено факт розповсюдження фігурантом бази даних, яка містить відомості відносно 2,8 мільйонів авторизаційних даних облікових записів користувачів мережі Інтернет.

За даним фактом відкрито кримінальне провадження за ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України». ***(У Хмельницькому кіберполіцейські викрили чоловіка, який займався розповсюдженням облікових даних громадян // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/u-xmelnyczkomu-kiberpoliczejski-vykryly-cholovika-yakyj-zajmavsya-rozpovsyudzhennyam-oblikovyx-danyx-gromadyan-5217/). 06.11.2020).***

***

«…Працівники кіберполіції Київщини спільно зі слідчими Васильківського відділу поліції встановили факт незаконного заволодіння нерухомістю у Києві завдяки використанню шкідливого програмного забезпечення.

За попередніми даними, зловмисники надіслали електронного листа, що містив «вірус» державному нотаріусу. Таким чином вони отримали віддалений доступ до його комп'ютера. Далі правопорушники внесли неправдиві відомості до Державного реєстру речових прав на нерухоме майно.

Відтак змінили право власності на нежитлову будівлю у центрі Києва площею близько 250 квадратних метрів.

Співробітники кіберполіції встановили «замовника» таких послуг. У його оселі провели обшук із залученням спецпризначенців Київщини. За результатами вилучено комп'ютерну техніку, що містить докази причетності до несанкціонованого втручання у роботу комп'ютера державного нотаріуса. Речові докази направлено на проведення відповідних експертних досліджень.

Відкрито кримінальне провадження за ч. 3 ст. 190 (Шахрайство) Кримінального кодексу України. Санкція статті передбачає позбавлення волі на строк до восьми років. Досудове розслідування триває». ***(У Києві кіберполіція викрила факт шахрайського заволодіння нерухомістю за допомоги комп'ютерного вірусу // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/u-kyyevi-kiberpolicziya-vykryla-fakt-shaxrajskogo-zavolodinnya-neruxomistyu-za-dopomogy-kompyuternogo-virusu-3654/). 03.11.2020).***

***

«Ильичевский районный суд г. Мариуполя приговорил к 1 году тюрьмы ранее судимого украинца за установку нелицензионного программного обеспечения…

Во время суда было установлено, что подсудимый в августе 2020 года с целью получения прибыли установил и при помощи специального ПО активировал на компьютере пользователя программу «ARCHICAD 23», имущественные авторские права на которую принадлежат компании «Graphisoft SE» (Венгрия). Своими действиями обвиняемый нанес компании ущерб в сумме 3850 евро.

Действия обвиняемого квалифицированы по ч. 1 ст. 176 УК Украины (незаконное воспроизведение компьютерных программ, причинившее материальный ущерб в значительном размере).

На судебном заседании мужчина полностью признал свою вину.

Суд признал обвиняемого виновным в совершении уголовного правонарушения, предусмотренного ч. 1 ст. 176 УК Украины и назначил наказание в виде 1 года лишения свободы. Т.к. подсудимым были совершены другие правонарушения, по совокупности преступлений путем поглощения менее строгого наказания более строгим, мужчине окончательно назначен срок в виде 1 года и 3 месяцев лишения свободы». ***(Артем Сереженок. Суд приговорил украинца к году тюрьмы за установку нелицензионного ПО // Internetua (http://internetua.com/sud-prigovoril-ukrainca-k-godu-tuarmy-za-ustanovku-nelicenzionnogo-po). 20.11.2020).***

***

«…Співробітники Управління протидії кіберзлочинам у Львівській області спільно зі слідчими Шевченківського відділу поліції викрили 30-річного мешканця Львова, який за допомогою шкідливого програмного забезпечення, здійснював кібератаки та зламав облікові записи більш як 1,5 тисяч користувачів мережі Інтернет. Отримавши незаконним шляхом доступ до

авторизаційних даних користувачів вебсайтів, зловмисник формував бази даних з паролів та логінів, які в подальшому продав одному з хакерських сайтів.

Під час санкціонованих обшуків правоохоронці виявили та вилучили комп'ютерну техніку, мережеве обладнання, цифрові носії інформації, на яких зафіксовано електронні сліди вчинення злочину та інші речові докази.

19 листопада слідчі повідомили зловмиснику про підозру у скоєнні кримінальних правопорушень, передбачених ч. 1 ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), ч. 1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) та ч. 1 ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається комп'ютерах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України. Максимальне покарання, передбачене санкціями статей – до трьох років позбавлення волі.

Процесуальне керівництво у справі здійснює Львівська місцева прокуратура №2

Досудове розслідування завершене, обвинувальний акт скеровано на розгляд суду». ***(Поліцейські повідомили про підозру львів'янину, причетному до розповсюдження шкідливого програмного забезпечення // Кіберполіція України (https://cyberpolice.gov.ua/news/policzejski-povidomyly-pro-pidozru-lvivyanynu-prychetnomu-do-rozpovsyudzhennya-shkidlyvogo-programnogo-zabezpechennya-550/). 20.11.2020).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Секретарь СНБО Украины Алексей Данилов обсудил с чрезвычайным и полномочным послом Королевства Норвегия в Украине Эриком Сведалом расширение сотрудничества в сфере киберзащиты. Об этом сообщает пресс-служба СНБО. "Во время встречи украинская сторона подчеркнула важность активизации и расширения межгосударственного сотрудничества в сфере киберзащиты и взаимодействия НКЦК с аналогичными центрами стран-партнеров, налаживания устойчивого обмена информацией о киберинцидентах, проведение совместных расследований", - говорится в сообщении.

Отмечается, что Алексей Данилов ознакомил Эрика Сведала с возможностями Национального координационного центра кибербезопасности при СНБО Украины. Во время встречи Алексей Данилов подчеркнул, что сегодня НКЦК, который является ключевой государственной структурой по выявлению, предотвращению и реагированию на киберинциденты, координирует работу всех ключевых структур национальной системы кибербезопасности, а также активно сотрудничает с частным сектором. "Данилов назвал обеспечение

кибербезопасности Украины приоритетным вопросом в условиях гибридной войны с Россией, учитывая целенаправленную киберинтервенцию в ущерб нашим национальным интересам, добавив, что за кибератаками российских хакерских группировок стоят спецслужбы, которые координируют их деятельность. Секретарь СНБО Украины также отметил, что в новой Стратегии национальной безопасности Украины значительное место уделено кибербезопасности, и специалисты НКЦК уже начали разработку Стратегии кибербезопасности", - указано в сообщении. Сообщается, что по мнению Данилова, обмен информацией в режиме реального времени позволит Украине и ее иностранным партнерам вовремя локализовать и обезвредить кибератаки. "Среди прочего, было акцентировано на важности не только развития мощной системы киберзащиты, но и ведения в киберпространстве собственных активных наступательных операций, в частности, превентивных, с целью обезвреживания компьютерных систем противника. В свою очередь, господин посол выразил мнение о перспективности двустороннего сотрудничества в сфере киберзащиты", - сообщили в пресс-службе». ***(Данилов обсудил с послом Норвегии расширение сотрудничества в сфере киберзащиты // информационный портал "ua.today" (http://ua.today/news/politics/danilov_obsudil_s_poslom_norvegii_rasshirenie_sotrudnichestva_v_sfere_kiberzashity). 03.11.2020).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Платформа, используемая медицинскими работниками на Филиппинах и предназначенная для обмена данными о случаях COVID-19, содержала несколько недостатков, которые раскрывали данные медицинских работников и потенциально могли привести к утечке данных о пациентах.

Уязвимости, обнаруженные как в веб-платформе платформы COVID-KAYA, так и в приложениях для Android, позволяют неавторизованным пользователям получать доступ к личным данным о пользователях платформы и потенциально данным пациентов, согласно отчету исследователей из Citizen Lab, междисциплинарной лаборатории, расположенной при Университете г. Торонто.

Отчет Citizen Lab является последним примером того, как пандемия COVID-19 привела к возникновению множества проблем с безопасностью для сектора здравоохранения, включая защиту данных и атаки программ-вымогателей. Помимо оппортунистических угроз, использующих пандемию и связанные с ней проблемы для собственной выгоды в фишинговых и других кампаниях, связанных с социальной инженерией, поток новых данных, связанных с пандемией, также проверяет безопасность систем, используемых для хранения и обмена этими данными.

COVID-KAYA был развернут 2 июня, чтобы позволить передовым медицинским работникам на Филиппинах автоматизировать сбор и обмен информацией о случаях коронавируса с Министерством здравоохранения страны.

Приложение имеет веб-версии, версии для iOS и Android и было создано с использованием Cordova, кроссплатформенной среды разработки приложений, которая позволяет разработчикам создавать приложения с использованием веб-технологий, а затем развертывать один и тот же код как на веб-платформах, так и на мобильных платформах.

«Наш анализ показал, что обе эти версии COVID-KAYA содержат уязвимости, раскрывающие данные, в противном случае защищенные учетными данными «суперпользователя», - говорится в отчете, написанном Пеллеоном Лином из Citizen Lab, Джеффри Нокелем, Адамом Сенфтом, Ирен Поэтранто, Стефани Тран, и Рон Дейберт.

Исследователи указывают на две уязвимости, которые с тех пор были исправлены - одна в веб-приложении COVID-KAYA, а другая в приложении для Android, - которые злоумышленники могли использовать для раскрытия конфиденциальных данных из системы.

Недостаток веб-приложения заключался в логике аутентификации. Уязвимость позволила «иначе ограничить доступ к конечным точкам API, раскрывая названия и расположение медицинских центров, а также имена более 30 000 поставщиков медицинских услуг, которые подписались на использование приложения», - заявили исследователи. Они также заявили, что приложение могло раскрыть конфиденциальные данные пациентов, хотя это остается неподтвержденным.

Между тем, Android-приложение COVID-KAYA использовало жестко запрограммированные учетные данные API, которые также позволяли доступ к именам поставщиков медицинских услуг и потенциально конфиденциальным данным пациентов, пишут исследователи.

Команда Citizen Lab раскрыла уязвимость веб-приложения разработчикам приложения, в том числе официальным лицам из Dure Technologies, Министерства здравоохранения Филиппин и Всемирной организации здравоохранения (ВОЗ) Филиппин, 18 августа, а также уязвимости приложения для Android 14 сентября. Исследователи подтвердили, что оба недостатка были обнаружены и исправлены по состоянию на 29 октября, и все утечки учетных данных были признаны недействительными.

Ошибка аутентификации в веб-приложении проистекает из страницы входа, используемой для аутентификации действительных пользователей с помощью имени пользователя и пароля. На первый взгляд казалось, что страница функционирует нормально; Исследователи сообщили, что если кто-то вошел в систему с недопустимым именем пользователя и / или паролем, это сообщит этому человеку.

«Однако в ходе нашего тестирования мы обнаружили, что после попытки входа в систему с недопустимым именем пользователя или паролем веб-приложение, похоже, предоставило нам без уведомления доступ к конечным точкам API и инструментам, обычно недоступным для пользователей, которые не вошли в систему,» Писали исследователи. «Эти конечные точки API и инструменты было легко обнаружить».

Например, группа обнаружила конечную точку API, взяв общедоступную конечную точку для сброса забытого пароля пользователя и затем удалив часть URL-адреса. Новый URL-адрес перенаправлял их на страницу, которая, по-видимому, была главным каталогом конечных точек API, одна из которых, по-видимому, могла перечислить всех, перечисляя всех 30 087 (на момент доступа) пользователей приложения, говорят исследователи.

Дальнейшее изменение URL-адреса позволило им получить доступ к системе и просмотреть все медицинские центры и поставщиков медицинских услуг, связанных с приложением, с разбивкой по странам и городам, а также получить доступ к другим конфиденциальным данным, говорят исследователи.

В своем анализе приложения COVID-KAYA для Android версии 1.4.7 исследователи обнаружили недостаток в том, как исходный файл исходного кода приложения обрабатывал жестко закодированные учетные данные, используемые для доступа к веб-интерфейсу приборной панели системы. По словам исследователей, уязвимость может использоваться для доступа к конфиденциальным данным с конечных точек API, позволяя неавторизованный вход в систему для входа в панель управления.

Две недели назад произошла еще одна утечка данных, связанная с COVID-19, когда кибератака поразила производителя вакцины COVID-19 Dr. Reddy's Laboratories, подрядчика российской вакцины против COVID-19 «Sputinik V», которая вот-вот войдет в Фазу 2. испытания. Компания закрыла свои заводы в Бразилии, Индии, России, Великобритании и США, а также остановила отдельные центры обработки данных для применения исправлений». ***(Elizabeth Montalbano. COVID-19 Data-Sharing App Leaked Healthcare Worker Info // Threatpost (https://threatpost.com/covid-19-data-leaked-healthcare-worker-info/161108/). 11.11.2020).***

***

«Microsoft сообщила, что кибератаки, исходящие из Северной Кореи и России, были нацелены на компании, проводящие исследования вакцин и средств лечения COVID-19. своем новом сообщении в блоге, Компания заявляет, что атаки были нацелены на семь ведущих фармацевтических компаний и исследователей в США, Канаде, Франции, Индии и Южной Корее.

«Среди целей большинство - производители вакцин, у которых вакцины COVID-19 находятся на различных стадиях клинических испытаний», - говорится в сообщении блога Тома Берта, корпоративного вице-президента Microsoft по безопасности и доверию клиентов. Microsoft не назвала компании и не предоставила подробностей о том, какая информация могла быть украдена или взломана, но сообщила, что уведомила организации и предложила помощь в тех случаях, когда атаки были успешными.

По данным Microsoft, большинство атак было заблокировано ее средствами защиты.

Согласно сообщению в блоге, хакеры использовали различные методы для проведения атак, в том числе попытки грубой силы для кражи учетных данных, а также целевые фишинговые атаки, в которых хакеры выдавали себя за рекрутеров,

ищущих кандидатов на работу, и как представителей мира Организация здравоохранения.

«Вызывает тревогу то, что эти проблемы теперь слились воедино, поскольку кибератаки используются для подрыва организаций здравоохранения, борющихся с пандемией», - написал Берт. «Мы считаем эти нападения бессовестными и должны быть осуждены всем цивилизованным обществом».

Число новых случаев коронавируса растет в США и других частях мира, но есть некоторые многообещающие признаки в разработке вакцины. Pfizer и BioNTech объявили, что их вакцина на 90 процентов эффективна в предотвращении симптоматического COVID-19 в ходе клинических испытаний. Эти предварительные данные еще не были изучены независимыми исследователями, но эксперты назвали новость «чрезвычайно обнадеживающей». Ожидается, что кандидат на вакцину от Moderna вскоре опубликует первоначальные данные». ***(Microsoft says hackers from Russia and North Korea attacked COVID-19 vaccine makers // Vox Media (https://www.theverge.com/2020/11/14/21565136/microsoft-hackers-russia-north-korea-attacked-covid-19-vaccine-coronavirus). 14.11.2020).***

***

«Специалисты по поиску ошибок в GitHub Security Labs помогают укрепить безопасность немецких приложений для отслеживания контактов, поддерживая сотрудничество с открытым исходным кодом.

Уязвимость системы безопасности в инфраструктуре, лежащая в основе официальной COVID-19 бесконтактную трассировкой приложения Германии, называется Корона-Предупреждать-App (КИ), позволили бы предварительно заверенному удаленному выполнению кода (RCE).

Исследователь Альваро Муньос написал в отчете на этой неделе, что он и его команда из GitHub Security Labs искали уязвимости RCE на платформе и нашли одну в инфраструктуре, поддерживающей CWA для Android и ОС. Команда заявила, что работала с SAP над устранением проблемы, добавив в качестве проблемы на стороне сервера, что сами мобильные приложения не пострадали, и что не было собрано никаких данных за пределами IP-адреса устройства.

«Похоже, что в сервере приложений Corona-Warn-App Server обнаружена RCE-уязвимость перед аутентификацией, которая управляет инфраструктурой приложений для отслеживания контактов COVID-19 в Германии», - сказал Муньос. «Эта уязвимость потенциально могла повлиять на целостность реакции Германии на COVID-19 и, как таковая, требовала немедленного ответа со стороны нашей команды».

Ошибка

Уязвимый код находился в службе отправки, которая представляет собой микросервис, разработанный на основе платформы Spring Boot и отвечающий за проверку информации, отправляемой пользователями CWA.

При этом используется функция под названием SubmissionController, которая проверяет различные аспекты предоставленной пользователем информации, например, убедитесь, что все обязательные поля заполнены. Данные проверяются валидатором ValidSubmissionPayload.

«Как объяснялось в нашем предыдущем исследовании уязвимостей Java Bean Validation, если какие-либо проверенные свойства bean передаются в настраиваемый шаблон нарушения ограничений, [] свойство, контролируемое злоумышленником, будет оцениваться как выражение Expressional Language (EL), что позволяет производить оценку произвольного кода Java», - пояснил исследователь.

Оказывается, это справедливо для двух проверок достоверности предоставленных пользователем материалов: одна проверяет, чтобы убедиться, что информация о «посещенных странах» действительна, а другая проверяет, действительна ли страна происхождения.

В результате, по словам исследователя, любые запросы POST, отправляемые в конечную точку Submission, разрешены по умолчанию и не требуют дополнительной авторизации или аутентификации. А сама конечная точка представления является общедоступной, что позволяет осуществлять удаленный контакт.

CWA был заказан правительством Германии и построен SAP и Deutsche Telekom с использованием платформы разработки GitHub. Он функционирует путем обмена анонимными токенами через API уведомления о воздействии от Apple и Google через Bluetooth Low Energy. Журнал хранится 14 дней. Если пользователь дает положительный результат, анонимный журнал отправляется на сервер CWA, который отслеживает воздействие и может, в свою очередь, предупреждать людей о необходимости изолировать его после установленного количества воздействий.

«Приложение сообщает нам, контактировали ли мы с человеком, у которого диагностирован COVID-19», - говорится на сайте CWA. «Он защищает нас и окружающих, а также нашу конфиденциальность».

По данным SAP, приложение было выпущено в июне после 50 дней разработки. График был увеличен за счет того, что проект с открытым исходным кодом стал общедоступным на GitHub.

«Более 109 000 посетителей просмотрели код, и примерно 7250 участников сообщества и проекта приняли участие», - говорится в заявлении SAP в июне о выпуске приложения. «Corona-Warning-App - крупнейший проект с открытым исходным кодом, когда-либо реализованный в Германии от имени правительства Германии».

Со своей стороны, GitHub рекламирует обнаружение ошибки как успех как для открытого исходного кода, так и для борьбы с COVID-19.

«Это исследование - еще один пример того, как открытый исходный код спасает положение - без вовлечения более широкого сообщества разработчиков GitHub Security Lab не смогла бы обнаружить и помочь исправить эту уязвимость, рискуя критически важной частью инфраструктуры в глобальной борьбе с COVID. -19, - сказал Threatpost Джейми Кул, вице-президент по управлению продуктами и безопасности GitHub.

Отслеживание контактов и конфиденциальность

Проблемы конфиденциальности были препятствием для внедрения приложений для отслеживания контактов, которые требуют широкого

использования, чтобы быть ценными. Люди с подозрением относятся к передаче данных о своем местонахождении государственным учреждениям.

В сентябре некоммерческая организация Electronic Frontier Foundation предупредила о возможных последствиях использования приложений для отслеживания контактов для подавления защиты свободы слова, в частности, подчеркнув, что Калифорния не учитывает соображения конфиденциальности при разработке приложения для отслеживания для штата.

«Защита конфиденциальности необходима для программ общественного здравоохранения, особенно когда программа требует высокого уровня участия, чтобы быть эффективной, - написала Хейли Цукаяма из EFF в своем блоге в сентябре. «Люди не будут использовать приложения, которым они не могут доверять. Вот почему EFF и другие группы по обеспечению конфиденциальности призвали губернатора Ньюсома установить основные ограничения конфиденциальности для любой программы отслеживания контактов, проводимой государством или совместно с государством».

Кроме того, в мае прошлого года было раскритиковано приложение Юты «Здоровые вместе» за отказ от API Google и Apple, который назначает маяк анонимного идентификатора для защиты конфиденциальности, и вместо этого за использование системы, разработанной для сайта социальной сети, которая, по словам критиков, собирала большие объемы данных о местоположении пользователей.

Муньос сказал, что создание этих приложений с открытым исходным кодом не только обеспечивает прозрачность для пользователей в отношении того, какие данные собираются и куда они направляются, но также позволяет другим помогать обнаруживать бреши в безопасности, что, в свою очередь, создает критическое общественное доверие». ***(Becky Bracken. German COVID-19 Contact-Tracing Vulnerability Allowed RCE // Threatpost (https://threatpost.com/german-covid-19-contact-tracing-vulnerability-rce/161419/). 19.11.2020).***

***

«В последние недели подозреваемые северокорейские хакеры пытались взломать системы британского производителя лекарств AstraZeneca, сообщили Reuters два человека, знающих об этом, в то время как компания спешит развернуть свою вакцину от вируса COVID-19.

По словам источников, хакеры выдавали себя за рекрутеров на сетевом сайте LinkedIn и WhatsApp, чтобы обратиться к персоналу AstraZeneca с поддельными предложениями о работе. Затем они отправили документы, якобы описывающие должностные обязанности, с добавлением вредоносного кода, предназначенного для получения доступа к компьютеру жертвы.

По словам одного из источников, попытки взлома были нацелены на «широкий круг людей», в том числе на сотрудников, работающих над исследованием COVID-19, но не были успешными.

Миссия Северной Кореи при ООН в Женеве не ответила на запрос о комментарии. Пхеньян ранее отрицал факт проведения кибератак. У него нет прямого контакта с иностранными СМИ.

AstraZeneca, которая вошла в тройку ведущих разработчиков вакцины против COVID-19, отказалась от комментариев.

Источники, которые говорили на условиях анонимности для обсуждения закрытой информации, заявили, что инструменты и методы, использованные в атаках, показали, что они были частью продолжающейся хакерской кампании, которую официальные лица США и исследователи кибербезопасности приписали Северной Корее.

Кампания ранее была сосредоточена на оборонных компаниях и СМИ, но в последние недели переключилась на цели, связанные с COVID, по словам трех человек, расследовавших атаки.

Кибератаки на органы здравоохранения, ученых-вакцин и производителей лекарств резко возросли во время пандемии COVID-19, поскольку поддерживаемые государством и криминальные хакерские группы пытаются получить последние исследования и информацию о вспышке.

Западные официальные лица заявляют, что любую украденную информацию можно продать с целью получения прибыли, использовать для вымогательства у жертв или дать иностранным правительствам ценное стратегическое преимущество в их борьбе за сдерживание болезни, от которой погибло 1,4 миллиона человек во всем мире.

В этом месяце Microsoft заявила, что видела две северокорейские хакерские группы, нацеленные на разработчиков вакцин в разных странах, в том числе путем «рассылки сообщений с сфабрикованными описаниями должностей». Microsoft не назвала ни одну из целевых организаций.

Южнокорейские законодатели заявили в пятницу, что спецслужбы страны пресекли некоторые из этих попыток.

Рейтер ранее сообщал, что в этом году хакеры из Ирана, Китая и России пытались взломать ведущих производителей лекарств и даже Всемирную организацию здравоохранения. Тегеран, Пекин и Москва опровергли обвинения.

По словам одного из источников, некоторые из учетных записей, использованных в атаках на AstraZeneca, были зарегистрированы на российские адреса электронной почты, что, возможно, было попыткой ввести следователей в заблуждение.

Прокуратура США обвинила Северную Корею в некоторых из самых дерзких и разрушительных кибератак в мире, включая взлом и утечку электронных писем от Sony Pictures в 2014 году, кражу 81 миллиона долларов из Центрального банка Бангладеш в 2016 году и запуск программы-вымогателя Wannacry. вирус в 2017 году.

Пхеньян назвал эти обвинения частью попыток Вашингтона опорочить свой имидж». ***(Jack Stubbs. Exclusive: Suspected North Korean hackers targeted COVID vaccine maker AstraZeneca – sources // Reuters (https://www.reuters.com/article/us-healthcare-coronavirus-astrazeneca-no/exclusive-suspected-north-korean-hackers-targeted-covid-vaccine-maker-astrazeneca-sources-idUSKBN2871A2). 27.11.2020).***

***

«Личная и медицинская информация более чем 16 миллионов бразильских пациентов с COVID-19 просочилась в сеть после того, как в этом месяце сотрудник больницы загрузил электронную таблицу с именами пользователей, паролями и ключами доступа к конфиденциальным государственным системам на GitHub.

Среди систем, в которых были раскрыты учетные данные, были E-SUS-VE и Sivep-Gripe, две правительственные базы данных, используемые для хранения данных о пациентах с COVID-19.

E-SUS-VE использовался для регистрации пациентов с COVID-19 с легкими симптомами, а Sivep-Gripe использовался для отслеживания госпитализированных случаев.

Две базы данных содержали конфиденциальные данные, такие как имена пациентов, адреса, идентификационные данные, а также медицинские записи, такие как история болезни и режимы приема лекарств.

Утечка обнаружилась после того, как пользователь GitHub обнаружил электронную таблицу с паролями к личной учетной записи GitHub сотрудника больницы Альберта Эйнштейна в городе Сан-Паулу.

Позже пользователь уведомил бразильскую газету Estadao, которая проанализировала данные и уведомила больницу и министерство здравоохранения Бразилии.

Журналисты Estadao сообщили, что данные о бразильцах из всех 27 штатов были включены в две базы данных, в том числе такие известные фигуры, как президент страны Жаир Болсонару, семья президента, семь министров правительства и губернаторы 17 бразильских штатов.

В конечном итоге электронная таблица была удалена с GitHub, а правительственные чиновники изменили пароли и отозвали ключи доступа, чтобы обезопасить свои системы.

С начала пандемии COVID-19 у нескольких правительств и государственных подрядчиков возникли проблемы с защитой своих приложений и баз данных, связанных с COVID-19.

Уязвимости и утечки были обнаружены в приложениях и системах COVID-19, используемых в Германии [1, 2], Уэльсе, Новой Зеландии, Индии и других странах.

Согласно исследованию, опубликованному Intertrust в сентябре этого года, около 85% приложений для отслеживания контактов COVID-19 тем или иным образом утекают данные». ***(Catalin Cimpanu. Personal data of 16 million Brazilian COVID-19 patients exposed online // Zero Day (https://www.zdnet.com/article/personal-data-of-16-million-brazilian-covid-19-patients-exposed-online/). 26.11.2020).***

***

«Джеральд Бешелт, директор по информационной безопасности в LogMeIn, смотрит в будущее кибербезопасности и предполагает, что в ближайшее время рабочие места будут лишены пароля.

Этот год стал одним из самых сложных для многих организаций по всему миру. В условиях пандемии, вызвавшей широкомасштабный переход к удаленной работе, и киберпреступной деятельности, использующей эту ситуацию, безопасность в Интернете находится в центре внимания. Недавние исследования показали, что 67% взломов вызваны кражей учетных данных и атаками социальной инженерии, которые используют такие моменты времени, как COVID-19. И сегодняшние ИТ-команды тратят в среднем шесть часов в неделю только на вопросы, связанные с паролями, что на 25% больше, чем в 2019 году. Учитывая растущее разочарование как ИТ-специалистов, так и пользователей, а также растущие риски, возникает вопрос: почему мы продолжаем полагаться на пароли?

Укоренившаяся любовь к паролям

С тех пор, как мы себя помним, пароли были реальностью повседневной жизни. Они продолжают оставаться самой простой и наиболее часто используемой формой аутентификации как на корпоративном, так и на личном уровне. Тем не менее, они также продолжают оставаться одной из основных причин возникновения уязвимостей, и с учетом того, что в обозримом будущем персонал будет работать удаленно, крайне важно найти решение, которое снижает риск.

В нашем последнем отчете LastPass «От паролей к беспарольному» мы обнаружили, что безопасность паролей является одним из основных источников разочарования ИТ-отдела, особенно когда проблемы возникают из-за поведения пользователей, например, повторного использования пароля. Главное разочарование сотрудников заключается в удобстве, например, регулярной смене паролей, запоминании нескольких паролей и вводе длинных сложных паролей. Существует явное несоответствие между приоритетами безопасности ИТ и требованиями сотрудников к пользовательскому опыту. Итак, что можно сделать, чтобы решить проблему с паролем?

Несмотря на вопросы о будущем пароля, 85% опрошенных ИТ-специалистов не думают, что пароли исчезнут полностью. Тем не менее, более 92% считают, что предоставление конечным пользователям возможностей без пароля - это будущее их организации. Ответ на затруднительное положение с паролем прост: вместо того, чтобы полностью удалять пароли, измените способ взаимодействия с ними. Вот тут и появляется беспарольная аутентификация.

Как будет работать вход без пароля?

Вход в систему без пароля означает, что, хотя пароли могут все еще существовать в ИТ-инфраструктуре, сотруднику не придется вручную вводить пароль во время входа в систему. Это дает несколько преимуществ, таких как снижение затрат на ИТ за счет устранения рисков, связанных с паролями, повышение производительности труда сотрудников, поскольку они экономят время на запоминание и / или смену паролей, а также более высокий уровень безопасности за счет защиты каждой точки доступа с помощью более безопасных

форм аутентификации. Однако переход к беспарольному подходу требует выбора и внедрения технологии, которая соответствует потребностям вашей организации. Некоторые из методов на выбор:

Внедрение единого входа (SSO) может помочь защитить и упростить управление доступом независимо от того, где находятся сотрудники. С помощью протокола, такого как язык разметки утверждения безопасности (SAML), система единого входа устанавливает безопасную линию между поставщиком удостоверений и поставщиком услуг, то есть создает связь между тем, где ИТ-отдел управляет информацией о доступе сотрудников, и приложениями, в которые пользователи хотят войти. Единый вход позволяет сотрудникам сократить количество паролей, которые они должны запомнить или обновить, повышая их производительность и сводя к минимуму риски, связанные с учетными данными.

Включение многофакторной аутентификации (MFA) предоставляет ИТ-отделам инструменты для управления доступом на уровне отдельных пользователей, определенных групп или даже по должностным обязанностям. MFA учитывает множество факторов, таких как местоположение, IP-адрес или биометрические данные (идентификатор лица), по сравнению с одним фактором - например, паролем - перед предоставлением доступа к приложению. Запрашивая у пользователя дополнительную информацию при входе в систему, ИТ-отдел может быть уверен, что человек, запрашивающий доступ, действительно является тем, кем они себя называют. Это также упрощает процесс для конечного пользователя, который будет иметь более быстрый и легкий вход в систему.

Что делать дальше на рабочем месте?

Организации и пользователи должны помнить, что пароли будут использоваться еще долгое время. Сочетание беспарольного опыта входа в системе с менеджером паролей будет лучшим способом обеспечить все точки доступа, обеспечивая при этом опыте бесшовной входы.

Поскольку мы продолжаем ориентироваться в мире «работы из любого места», многие элементы находятся вне контроля ИТ-команд. От устройств пользователей и подключения к Wi-Fi до приложений и веб-сайтов, которые они часто посещают, удаленная работа увеличивает риски и увеличивает количество переменных, которые необходимо учитывать. Готова ли ваша организация отказаться от пароля? Начните изучать лучший способ реализовать простой, оптимизированный и безопасный способ для сотрудников входить во все свои рабочие места, где бы они ни находились - уже сегодня». ***(Is the future of cybersecurity passwordless? // Open Access Government (https://www.openaccessgovernment.org/passwordless/97090/). 09.11.2020).***

***

«Світові експерти визначили дефіцитну у 2021 році професію. Про це йдеться в дослідженні міжнародної аудиторської компанії PricewaterhouseCoopers (PwC), передає Главком.

За їх висновками, значна частина компаній – 51% у світі планує збільшувати штат співробітників в області кібербезпеки.

«В умовах пандемії коронавірусу багатьом організаціям довелося переглянути і переосмислити стратегії забезпечення кібербезпеки», – зазначив партнер, керівник практики з кібербезпеки і безперервності бізнесу PwC в Росії Віталій Соколов. Він додав, що майже всі учасники опитування (96%) заявили про готовність це зробити.

Так, керівник пресслужби HeadHunter Олександр Джабаров підтвердив, що у сфері кібербезпеки спостерігається зростання потреби фахівців. За його словами, за 2018 рік було відкрито понад 17 тисяч вакансій, однак із січня по жовтень 2020 року – вже майже 30 тисяч. Він зазначив, що конкуренція в цій сфері дуже низька, одна-дві людини на місце при нормі в п'ять-шість, що говорить про гострий дефіцит.

В опитуванні взяли участь понад три тисячі керівників компаній, відділів технологій та інформаційної безпеки з різних галузей. Опитування для дослідження проводився в липні і серпні цього року». ***(Експерти назвали професію 2021 року, що матиме найбільший попит // Судово-юридична газета (https://sud.ua/ru/news/abroad/183821-eksperti-nazvali-nayzatrebuvanishu-profesiyu-2021-roku). 02.11.2020).***

***

«Белые» хакеры в рамках завершившегося накануне состязания по кибербезопасности взломали ряд культовых приложений, программ и устройств. Меньше всего времени «спортсменам» понадобилось на обретение доступа к содержимому iPhone 11 Pro, информирует тематический онлайн-ресурс Mydrivers.

Имя турнира — Tianfu Cup. Место его проведения — г. Ченду. Название команды-победительницы – Team 360 Vulcan из финансируемого властями Поднебесной Института исследований уязвимостей в сфере правительственной и корпоративной безопасности (англ. Enterprise Security and Government Vulnerability Research Institute).

Полученное лидером вознаграждение — $744,5 тыс. Суммарный призовой фонд конкурса — $1,21 млн. Общее количество участников – 15. Всем им отводилось по три попытки на взлом избранной «цели» с помощью своих фирменных «штучек». Число протестированных «мишеней» — 16, из них взломанных – 12. Совокупное количество сделанных попыток – 23.

Быстрее всего «пала» установленная на iPhone 11 операционная система iOS 14. На обретение доступа к содержавшимся на смартфоне документам, файлам и контактам конкурсантам понадобилось чуть более 10 секунд…

По уверениям организаторов, все без исключения разработчики взломанных приложений проинформированы о результатах. Хакеры уведомили их о выявленных недоработках и предоставили свои рекомендации по устранению оных». ***(За считанные секунды взломали iPhone 11 Pro с iOS 14 // ProstoMob (https://prostomob.com/34978-za-schitannye-sekundy-vzlomali-iphone-11-pro-s-ios-14). 10.11.2020).***

***

«Компания Fortinet, мировой лидер в области глобальных интегрированных и автоматизированных решений для обеспечения кибербезопасности, публикует данные исследования, проведенного TelecomTV, совместно с HardenStance и ETSI, согласно которым респонденты из сектора телекоммуникаций демонстрируют оптимизм относительно возможностей извлечения прибыли из 5G, но только в случае если новые услуги 5G будут более безопасными и в то же время соответствующими благоприятным сценариям корпоративного использования.

5G имеет потенциал для развития потребительского и корпоративного рынка, принося ряд преимуществ, таких как высокая скорость, меньшая задержка сигнала и большая пропускная способность. Пятое поколение мобильного стандарта также открывает путь к развитию таких сфер, как здравоохранение, автономный транспорт или умные города, предлагая новые возможности и улучшая качество жизни. С другой стороны, 5G значительно увеличивает количество подключенных устройств, что открывает новые возможности для киберпреступников. Учитывая это, операторы мобильных сетей и предприятия должны иметь эффективную стратегию кибербезопасности, которая может защитить всю их инфраструктуру, от мобильных сетей и до периферии.

Выдающаяся возможность для бизнеса

В целом почти 90% респондентов ожидают роста среднего дохода на пользователя (ARPU) от своих инвестиций. Ожидается, что этот рост будет равномерно разделен между общедоступными и частными сетями 5G, но поскольку по крайней мере половина всех частных сетей, вероятно, будет построена и управляться операторами, они потенциально могут захватить до 75% всего бизнеса 5G.

Однако критически важным для достижения этих результатов, по мнению 64% респондентов, будет повышение качества кибербезопасности, как с точки зрения архитектуры, так и с точки зрения операций, а также адаптация решений к конкретным бизнес-сценариям использования, которые являются критическими или очень важными для почти 75% респондентов, особенно в рамках ключевых вертикалей – транспорта, логистики, автоматизации, производства и здравоохранения.

Ключевое значение этого состоит в том, что старой бизнес-модели предоставления недифференцированных услуг мобильной связи больше не будет достаточно. Чтобы добиться успеха, большинству потребуется заключить партнерство и разделить ответственность с другими поставщиками, а также с корпоративными клиентами.

Потребность в партнерстве с другими поставщиками экосистемы, даже с теми, которые признаны конкурентами, была очевидна среди респондентов: 44% видели поставщиков облачных услуг как партнеров или, по крайней мере, как частичных партнеров, и только 11% считали их чистыми конкурентами.

Эти результаты хорошо согласуются с существующим разделением ответственности между поставщиками облачных услуг и их корпоративными клиентами, где обслуживание и безопасность инфраструктуры возлагается на

поставщика, а предприятию остается защищать свои собственные данные и приложения.

Ценность сильного предложения по обеспечению безопасности

К счастью, кибербезопасность – одна из главных сфер, привлекающих внимание бизнеса. Более 80% респондентов считают, что функции безопасности, присущие спецификациям проекта партнерства 5G третьего поколения (3GPP), являются не более чем базовым уровнем для рынка 5G. 62% всех респондентов заявили, что некоторые или большинство сценариев использования 5G потребуют дополнительных функций безопасности.

Кроме того, предоставление ценностного предложения, выходящего за рамки возможностей подключения, поскольку 61% респондентов считают маловероятным рост бизнеса в ARPU, если они ограничиваются в основном или полностью уровнем подключения в цепочке создания стоимости 5G, и адекватно удовлетворяет возросшие требования безопасности 5G и варианты использования, которые он предоставит, были расценены как критические или очень важные почти 90% респондентов.

Ронен Шпирер, директор отдела маркетинга решений в Fortinet: «С точки зрения инфраструктуры, миграция современных мобильных сетей на 5G, особенно автономных (SA), создает новые требования безопасности, которые выходят далеко за рамки присущих 5G возможностей, определенных 3GPP. Виртуализированный, распределенный и динамический характер ядра 5G в сочетании с существенным увеличением масштабируемости, ростом использования граничных вычислений с множественным доступом (Multi-access Edge Computing (MEC) и общими критическими сценариями использования требует надежной безопасности для базовой инфраструктуры и бизнес-сценариев. Именно здесь доказанный успех Fortinet в обеспечении видимости и защиты пользовательских и управляющих плоскостей 4G и 5G, масштабируемости и соотношения цены и качества демонстрирует явное преимущество для тех, кто хочет воспользоваться этими новыми возможностями 5G».

С точки зрения Fortinet, появление 5G способствует развитию ландшафта киберугроз и заставят мобильные сети и предприятия принять целостный подход к безопасности, чтобы справиться с этой развивающейся средой.

Методология

В опросе TelecomTV, проведенном Fortinet, респондентам из телекоммуникационного сектора по всему миру было предложено высказать свое мнение об эволюции рынка 5G для корпоративных услуг, а также о требованиях, предъявляемых к решениям, обеспечивающим безопасность, безопасных бизнес-моделях, необходимых для поддержки этих корпоративных услуг.

Более одной трети респондентов – представители сообщества сетевых операторов / поставщиков услуг, включая основных глобальных операторов мобильной связи. Еще четверть – поставщики оборудования и программного обеспечения». ***(Новый опрос Fortinet: оптимизм в отношении 5G и важная роль кибербезопасности // AMC Ukraine (https://channel4it.com/publications/novyy-opros-fortinet-optimizm-v-otnoshenii-5g-i-vazhnaya-rol-kiberbezopasnosti.html). 10.11.2020).***

***

«Новый отчет о растущем переходе к удаленной цифровой работе от Duo Security, фирмы по ИТ-безопасности из Анн-Арбора, которая теперь входит в состав Cisco Systems Inc., обнаруживает отход от широко используемого типа двухфакторной аутентификации, рост биометрической аутентификации и продолжающийся рост облачных приложений.

Представители Duo говорят, что последствия этого перехода для безопасности будут отражаться в ближайшие годы, поскольку гибридное рабочее место требует, чтобы персонал был защищен, подключен и продуктивен из любого места.

В отчете о надежном доступе Duo за 2020 год подробно описано, как организации, получившие мандат на быстрый перевод всей своей рабочей силы на удаленный доступ, обратились к технологиям удаленного доступа, таким как виртуальные частные сети (VPN) и протокол удаленного рабочего стола (RDP), среди множества других усилий. В результате количество операций аутентификации для этих технологий увеличилось на 60 процентов, что помогло увеличить ежемесячные аутентификации Duo с 600 миллионов до 900 миллионов в месяц. Комплементарный обзор Cisco недавно обнаружил, что 96 процентов организаций внесли изменения кибербезопасности политики во время пандемии, более половины реализации многофакторной аутентификации.

Принятие облака также ускорилось. Ежедневная аутентификация в облачных приложениях выросла на 40 процентов в течение первых нескольких месяцев пандемии, большая часть которых пришлась на корпоративные и средние организации, стремящиеся обеспечить безопасный доступ к различным облачным сервисам.

В то время как организации пытались приобрести необходимое оборудование для поддержки удаленной работы, сотрудники тем временем полагались на личные или неуправляемые устройства. Следовательно, количество заблокированных попыток доступа из-за устаревших устройств в марте резко возросло на 90. В апреле этот показатель резко упал, что указывает на более здоровые устройства и снижение риска взлома из-за вредоносного ПО.

«Когда началась пандемия, приоритетом для многих организаций было держать свет включенным и принимать риски, чтобы достичь этой цели», - сказал Дэйв Льюис, главный консультант по информационной безопасности Duo. «Внимание теперь обращено на снижение риска за счет внедрения более зрелого и современного подхода к обеспечению безопасности, который учитывает традиционный корпоративный периметр, который был полностью перевернут».

Результаты отчета также включают:

Итак, SMS. Распространенность атак с заменой SIM-карт заставила организации усилить свои схемы аутентификации. По сравнению с прошлым годом процент организаций, применяющих политику, запрещающую аутентификацию при обмене текстовыми сообщениями, почти удвоился с 8,7 процента до 16,1 процента.

Бум биометрии - биометрия практически повсеместна среди корпоративных пользователей, открывая путь к будущему без пароля. На 80% мобильных устройств, используемых для работы, настроена биометрия, что на 12% больше, чем за последние пять лет.

Облачные приложения постепенно переходят к использованию локальных приложений. К следующему году использование облачных приложений постепенно превзойдет использование локальных приложений, чему способствует переход к удаленной работе. Облачные приложения составляют 13,2 процента от общего числа проверок подлинности Duo, что на 5,4 процента больше, чем в прошлом году, а на локальные приложения приходится 18,5 процента от общего числа проверок подлинности, что на 1,5 процента меньше, чем в прошлом году.

Вероятность быстрого обновления устройств Apple в 3,5 раза выше, чем у устройств Android. Различия в экосистемах имеют последствия для безопасности. 1 июня Apple iOS и Android выпустили обновления программного обеспечения для исправления критических уязвимостей в своих операционных системах. Вероятность обновления устройств iOS в течение 30 дней после обновления безопасности или патча в 3,5 раза выше, чем на Android.

Windows 7 остается в сфере здравоохранения, несмотря на риски безопасности. Более 30 процентов устройств Windows в организациях здравоохранения по-прежнему используют Windows 7, несмотря на то, что их срок службы истек, по сравнению с 10 процентами организаций в клиентской базе Duo. Поставщики медицинских услуг часто не могут обновить устаревшие операционные системы из-за требований соответствия и ограничительных положений и условий сторонних поставщиков программного обеспечения.

Устройства Windows и браузер Chrome доминируют в ИТ-отделах бизнеса. Windows продолжает доминировать на предприятии, составляя 59 процентов устройств, используемых для доступа к защищенным приложениям, за ней следует Mac OS X с 23 процентами. В целом на мобильные устройства приходится 15 процентов корпоративного доступа (iOS: 11,4 процента, Android: 3,7 процента). Что касается браузера, Chrome является королем с 44% всех проверок подлинности браузера, что приводит к более строгой гигиене безопасности для организаций.

Великобритания и ЕС следуют за США в обеспечении безопасности облака. Организации из Соединенного Королевства и Европейского союза преследуют американские предприятия по аутентификации пользователей в облачных приложениях, сигнализируя о меньшем использовании облака в целом или о большей доле приложений, не защищенных MFA.

Ежегодный отчет Duo Trusted Access Report проверяет 26 миллионов устройств, используемых для работы, и 700 миллионов событий аутентификации пользователей в месяц для более чем 500 000 уникальных корпоративных приложений на основе неидентифицированных и агрегированных данных из клиентской базы Duo. Чтобы просмотреть отчет, посетите http://duo.sc/tar-2020. У Duo более 25 000 клиентов по всему миру, включая Facebook, Lyft, Мичиганский университет, Yelp, Zillow и многие другие. Основанная в Анн-Арборе, Duo имеет офисы в Остине, штат Техас; Сан-Франциско, Калифорния; и Лондон». ***(Matt Roush. Duo Report Finds Changing Security Landscape As Pandemic Forces Remote***

Work // MITechNews.com (https://mitechnews.com/cyber-defense/duo-report-finds-changing-security-landscape-as-pandemic-forces-remote-work/). 12.11.2020).

***

«Несмотря на десятилетия крупных инвестиций в кибербезопасность, глобальная финансовая система остается уязвимой для кибератак, поскольку банки и регулирующие органы не могут координировать свою деятельность, говорится в докладе ведущего аналитического центра.

Такие события, как серия атак на фондовую биржу Новой Зеландии в августе, которая привела к остановке торгов, а также успешная кибератака на счета центрального банка Бангладеш в 2016 году, показывают, как уязвимости продолжают разрушать финансовый сектор. 233-страничный отчет Фонда Карнеги за международный мир.

«Печально то, что это риск, который никуда не денется. Мы должны продолжать работать, чтобы противостоять этому риску», - сказал управляющий Банка Англии Эндрю Бейли на виртуальной панели, организованной CEIP в среду. Банк Англии вместе с Международным валютным фондом, Советом Федеральной резервной системы США и рядом частных компаний, таких как Amazon.com Inc. и крупные банки, выступали в качестве консультантов при подготовке отчета, который был подготовлен в партнерстве с Федеральной резервной системой США. Всемирный Экономический Форум.

В докладе говорится, что хотя международные организации существуют для содействия экономическому сотрудничеству в сфере финансовых услуг, в том числе Группа семи стран и Группа 20 крупнейших экономик; экономические советы богатых стран; и Совет по финансовой стабильности, организация, состоящая из министерств финансов и управляющих центральных банков, вопросы кибербезопасности в значительной степени оставлены на усмотрение отдельных стран и учреждений.

Рекомендации CEIP включают разъяснение правительствами того, как они толкуют международное право с точки зрения кибербезопасности, и заключение дипломатических соглашений о том, что является неприемлемой деятельностью, например, кибератака на глобальную финансовую систему. В отчете также содержится призыв к правительствам продолжать проявлять сдержанность при проведении наступательных кибер-действий против финансовых учреждений другого государства, чтобы не нормализовать эту деятельность.

Он также рекомендует расширять сотрудничество между правительствами и финансовым сектором в области обмена информацией путем открытия доступа к конфиденциальной информации или ее рассекречивания, где это необходимо, а также совместных мер реагирования на атаки через правоохранительные органы.

На более техническом уровне в отчете содержится призыв к действиям в новых областях, которые могут представлять киберриски для финансовой системы, например, уязвимость данных и алгоритмов для атак, и изучение рисков, создаваемых большинством крупных организаций, использующих несколько облачных технологий. поставщики услуг. В последние месяцы органы, включая Национальный институт стандартов и технологий, предупреждали об уязвимостях

данных, а законодатели в США и других странах ставят под сомнение растущее системное значение поставщиков технологий для финансовых учреждений.

Г-н Бейли сказал, что Великобритания, которая в следующем году председательствует в Большой семерке, примет к сведению рекомендации отчета и что для сектора жизненно важно выделить ресурсы для кибербезопасности, несмотря на другие трудности, в том числе глобальные экономика подорвана пандемией коронавируса.

«Мы все очень загружены, имея дело с серьезной глобальной проблемой - крупной пандемией. И все же мы не можем ослаблять бдительность в вопросе киберпространства», - сказал он.

Бэнкс подчеркнул необходимость единого подхода к практике кибербезопасности через международные границы. Рами Хусаини, главный специалист по кибербезопасности и технологическим рискам, а также специалист по защите данных группы французского кредитора BNP Paribas SA, сказал, что, хотя в последние годы во всем мире был принят ряд законов о кибербезопасности и конфиденциальности, отсутствие стандартных практик создает вызов для крупных финансовых институтов.

«Мы стали свидетелями волны новых законов и руководящих принципов по кибербезопасности, которые были сформулированы впервые. Поэтому для меня очень важно, чтобы мы продвигали согласованные нормы, которые упростят и, откровенно говоря, повысят эффективность наших усилий», - сказал он, выступая на следующей дискуссии, организованной CEIP в среду.

Одна из ключевых рекомендаций отчета сосредоточена на увеличении числа сотрудников, занимающихся кибербезопасностью. Международный консорциум по сертификации безопасности информационных систем, отраслевая торговая ассоциация, оценивает, что для выполнения должностей по всему миру требуется еще 3,1 миллиона специалистов по кибербезопасности.

Джен Истерли, глава центра Fusion Resilience Centre Morgan Stanley, который занимается вопросами непрерывности бизнеса для банка, предложила на той же панели, что банки и другие финансовые учреждения должны рассмотреть возможность переподготовки работников, потерявших работу из-за пандемии, и рассмотреть более разных кандидатов.

«Это невероятно важная вещь, на которой мы все должны сосредоточиться», - сказала она.

CEIP планирует провести в декабре конференцию с участием МВФ, Всемирного банка и Всемирного экономического форума, чтобы начать работу по выполнению своих рекомендаций». ***(James Rundle. Think Tank Urges Financial Sector Action on Cyber Threats // Dow Jones & Company (https://www.wsj.com/articles/think-tank-urges-financial-sector-action-on-cyber-threats-11605868201). 20.11.2020).***

***

«За шесть дней мероприятия состоялось более 70 докладов и круглых столов, его посетило свыше 20 тысяч человек

К концу последнего дня на киберполигоне The Standoff атакующие взломали периметр всех шести организаций и закрепились в корпоративных сетях. Однако реализовать бизнес-риски оказалось сложнее: хакерам противостояли опытные команды специалистов по защите. Были выведены из строя системы аэропорта, парка развлечений, газораспределительной станции, нефтедобывающей компании и электростанции. Потери понесли банк и деловой центр. На рекламных экранах взломщики могли показывать что угодно. Но морской порт и железная дорога устояли.

По горячим следам рассказываем обо всем, что происходило во время The Standoff. В ходе онлайн-выступлений экспертов слушатели узнали, например, как получить физический доступ в помещение, подделать голос за пять секунд, расшифровать испорченные вирусом-вымогателем данные и перехватывать данные смартфона в сети 5G.

Победила команда Codeby (27 123 баллов), на втором месте back2oaz (24 463 баллов), за ними следуют DeteAct (18 508 баллов). Атакующим удалось реализовать 47% заложенных рисков. Два реализованных киберриска из 24 оказались новыми, не предусмотренными в программе соревнования. Всего жюри приняло более 50 отчетов об успешно выполненных заданиях.

Команды защитников смогли выявить более 200 инцидентов ИБ в своих инфраструктурах. Больше всего инцидентов обнаружили команды IZ:SOC и CT&MM. Команды провели 21 расследование инцидентов. В среднем на расследование с необходимой полнотой собранных фактов командам требовалось 11 часов 50 минут.

Все компании столкнулись с последствиями кибератак. Перечислим наиболее серьезные:

На нефтехимическом заводе Nuft произошла авария и утечка ядовитых веществ. Атакующим удалось получить доступ к системе управления заводом, они закрыли входной клапан в холодильный контур, что привело к перегреву и нарушению производственного процесса. А вскоре нападающие смогли полностью его остановить.

Из-за кибератаки остановилась работа нефтедобывающего оборудования, что привело к прекращению добычи нефти. Кроме того, нападающие смогли получить доступ к системе управления хранилищами нефтепродуктов и нарушили процесс транспортировки нефти в хранилище. Позже им удалось остановить работу контроллера, управляющего транспортировкой нефтепродуктов.

В парке развлечений 25 Hours упало колесо обозрения. Одна из команд получила доступ к системе управления аттракционом и увеличила скорость вращения колеса до максимальной — результат оказался плачевным. Затем нападающие остановили работу контроллера, управляющего колесом обозрения, чтобы посетители не могли покинуть аттракцион, и отключили его освещение.

Отметим и успешные атаки на банк, в ходе которых нападающие смогли украсть деньги со счетов горожан, а также узнать данные клиентов ДБО (имя, остаток на счете, PAN карты и т. п.).

В двух компаниях были украдены ценные документы, а похитить персональные данные сотрудников атакующие смогли из пяти компаний.

Уже в последние минуты соревнования команда back2oaz получила доступ к системе управления кондиционированием и смогла изменять температуру воздуха в офисных зданиях.

Реализация некоторых киберрисков была непосредственно связана с недостаточной защитой сайтов компаний. Например, сбои в работе онлайн-касс парка аттракционов, сервиса по продаже авиабилетов и системы регистрации пассажиров на рейс на сайте аэропорта.

Но в основном нападающим сначала нужно было получить доступ к локальной сети компании. И здесь мы тоже видим, что в первую очередь атакующие искали уязвимости в веб-приложениях и через них проникали в инфраструктуру. Об успешных попытках эксплуатации таких уязвимостей сообщали и команды защитников.

Первая уязвимость была найдена командой n0x в системе компании Nuft через 19 минут после старта соревнований. Жюри приняло 433 отчета о найденных уязвимостях. Почти половину из них составило внедрение SQL-кода и еще четверть — недостатки, позволяющие выполнить произвольный код на сервере. Две трети всех уязвимостей выявили в компаниях Nuft и Big Bro Group.

Самое большое число рисков — восемь — было реализовано в инфраструктуре компании 25 Hours, которая управляет деловым центром города, системой кондиционирования, светофорами и парком развлечений, на втором месте — нефтяная компания Nuft, где было реализовано семь уникальных рисков. Незатронутыми остались только железнодорожная станция и морской порт.

Каждый третий риск опасен для людей

По оценке Максима Филиппова, директора Positive Technologies по развитию бизнеса в России, треть рисков, представленных на киберполигоне, могут так или иначе влиять на физическую безопасность людей. Выступая на бизнес-сессии ИД «Коммерсантъ» в рамках The Standoff, он напомнил, что в этом году у киберпротивостояния есть ряд важных нововведений.

«Каждому объекту на киберполигоне присущи те или иные бизнес-риски: остановка производства, утечка персональных данных, потеря конфиденциальных документов и т. п., — рассказал Максим Филиппов. — Здесь нет векторов атак. Мы отдаем площадку в распоряжение атакующих команд (red teams), которые ломают системы, исследуют их. Мы же наблюдаем, как взламываются системы, анализируем трафик и цепочки атак. На выходе получаем ценную экспертизу, которая затем идет в наши продукты».

«Мы не ожидали, что половина рисков будет реализована, — поделился впечатлениями Дмитрий Серебрянников, директор по анализу защищенности Positive Technologies. — Это очень много, особенно учитывая, что было мало времени. В этом году уровень атакующих сильно вырос».

«В этом году защита должна была доказать, что может отследить инцидент поэтапно. Основная цель была следить за работой сервисов и как можно быстрее устранять сбои, вызванные действиями атакующих, — рассказал директор департамента базы знаний и экспертизы Positive Technologies Михаил Помзов. — Эффективность команд защитников оценивалась по количеству зафиксированных атак, по среднему времени расследования инцидента — и времени доступности

инфраструктуры: чем этот параметр ниже, тем слабее действуют защитники, а атакующие наносят больше вреда».

Как ломают двери, банки и 5G

Мечта многих хакеров — получить физический доступ к оборудованию. Роберт Селл, президент компании Trace Labs, в ходе своего доклада рассказал о восьми шагах, которые злоумышленники предпринимают, чтобы получить физический доступ к интересующему их помещению. Роберт рассказал, как преступники проводят разведку, что делают в ходе тестовых попыток проникновения — и какие объяснения заготавливают на случай поимки. Помимо этого, эксперт представил подробное описание инструментов для физического взлома замков и открытия дверей, а также способов спрятать их в нужном здании, чтобы воспользоваться в нужный момент.

Но для банка сегодня важнее не крепость дверей, а информационная безопасность. Директор по исследованиям Cyber R&D Lab Тимур Юнусов продемонстрировал, что многие банки мира довольно слабо защищены от финансовых махинаций. Тимур привел реальные примеры нескольких атак на европейские банки, в результате которых были украдены сотни тысяч и миллионы евро. Он проанализировал ошибки, которые совершают службы безопасности и риск-менеджмента финансовых организаций, а также дал практические советы, как избежать проблем. Так, для противодействия многим угрозам банкам даже не нужно использовать сложные решения — например, на основе искусственного интеллекта; достаточно просто устранять конкретные известные уязвимости и анализировать, сколько денег компания реально теряет от определенных видов атак, чтобы бороться с ними в первую очередь.

У сетей 5G много преимуществ: они позволяют развиваться инфраструктуре подключенных автомобилей, с их помощью легче управлять городским трафиком и повышать безопасность участников дорожного движения. Другая отрасль, расцвет которой связывают с 5G, — это телехирургия. Однако данных об этих технологиях с позиции информационной безопасности совсем мало, заявил в ходе своего выступления Дмитрий Курбатов, директор по информационной безопасности телекоммуникационных систем Positive Technologies. «Не хотел бы я, чтобы мои дети оказались во взломанном хакерами автобусе, который управляется автопилотом», — отметил докладчик. По его словам, архитектура 5G во многом основана на технологиях сетей предыдущих поколений, и поэтому все уязвимости этих сетей остаются актуальными. В своем выступлении на The Standoff Дмитрий продемонстрировал, как атакующий может с помощью MITM-атаки через уязвимости в протоколе PFCP перехватить данные подключенного к 5G смартфона, — и анонсировал новое исследование безопасности 5G, которое ожидается в конце года.

О проблемах вирусов-вымогателей

Неизвестные злоумышленники, используя вирус-шифровальщик STOP (Djvu), атаковали компьютер одного из друзей руководителя отдела анализа приложений Positive Technologies Дмитрия Склярова. Они зашифровали ценные данные и потребовали выкуп в биткойнах, эквивалентный сумме в 980 долларов. Друг исследователя решил, что «с террористами переговоров не ведут», и попросил

помощи у Дмитрия. В ходе выступления на The Standoff докладчик рассказал, как ему удалось восстановить данные и найти онлайн-ключи для жертв STOP (Djvu), используя различные криптографические методы.

Тему вымогателей продолжил ведущий специалист по компьютерной криминалистике Group-IB Олег Скулкин. Его доклад был посвящен тактикам, методам и процедурам различных операторов программ-вымогателей, таких как Conti, Ryuk, Prolock, DoppelPaymer, CI0p, Maze, TinyCryptor. Эксперт отметил, что шифровальщики стали наиболее заметной проблемой ИБ в уходящем году. Появилось огромное количество нового вымогательского ПО и атаковать стали крупные корпорации, такие как Canon и Garmin. В результате максимальные размеры выкупов значительно увеличились, например, Garmin пришлось заплатить за расшифровку 10 млн долларов.

С Олегом Скулкиным согласен руководитель глобального центра исследований и анализа угроз (GREAT) «Лаборатории Касперского» Костин Райю. «Если в 2017 году программы-вымогатели в основном просили маленький выкуп (от 100 до 300 долларов) и целями атакующих были частные пользователи и их персональные компьютеры, то примерно с конца 2017 года этот тренд изменился и атаки стали сложнее». Одним из трендов этого года эксперт назвал стремление хакеров публиковать предварительно зашифрованную информацию и шантажировать компании-жертвы: «Поэтому компании платят миллионы долларов, опасаясь репутационных потерь».

Райю также призвал всех, кто стал жертвой шифровальщиков, не вести переговоры с преступниками и не платить им выкуп за расшифровку данных, ведь нет никаких гарантий, что данные будут расшифрованы. Вместо этого он посоветовал обращаться на портал nomoreransom.org: это глобальный проект, в рамках которого исследователи помогают расшифровать зашифрованные данные бесплатно, в случае если для этого существует инструментарий. «Если инструментов нет сейчас, они могут появиться позже. И конечно, не забывайте архивировать свою информацию и хранить ее на недоступном офлайновом ресурсе», — добавил Райю.

«В 2020 году преступники, проникая на компьютеры с целью получения финансовой выгоды, уже не пытались высосать деньги сами, направив в свою сторону финансовую трубу, как было раньше, а шифровали данные и требовали от жертв заплатить выкуп в биткойнах», — отметил Сергей Голованов, ведущий антивирусный эксперт «Лаборатории Касперского». Говоря о трендах ИБ, помимо атак шифровальщиков, Сергей обратил внимание на использование уязвимостей в средствах удаленного доступа. Кроме того, в этом году злоумышленники нацелились на домашние компьютеры пользователей, через которые можно получить доступ в инфраструктуру компании.

Проблемы фальшивых голосов и лиц

Алгоритмы искусственного интеллекта сейчас применяют в своей работе как специалисты по информационной безопасности, так и злоумышленники. Вячеслав Гордеев, архитектор систем защиты информации из Fortinet, рассмотрел такие технологии, как машинное обучение, нейронные сети, глубокие нейронные сети. Они используются для фильтрации спама, пассивного анализа трафика, поиска

вредоносного ПО или защиты веб-приложений. Атакующие также берут на вооружение эти технологии для сбора информации для подделки биометрических данных (записей голоса, изображений лица), подбора паролей и поиска уязвимостей.

Разговор о фальшивой биометрии продолжили исследователи безопасности из компании BBVA Next Technologies Мигель Эрнандес Боса и Хосе Игнасио Эскрибано. Они продемонстрировали техники, алгоритмы и инструменты (большинство из них опенсорсные), которые используются для генерации и обнаружения фальшивых данных (аудио, текстов, изображений и видео). Сегодня существуют открытые инструменты, позволяющие клонировать голос на основе всего пяти секунд аудио, заменять лица на видео или создавать уникальные аватары. Их можно использовать для атак как на конкретных людей (с целью испортить их репутацию), так и на организации. Создание синтетических личностей становится все проще, а борьба с ними — сложнее. Эксперты в ходе доклада показали ограничения различных инструментов и техник создания синтетических данных; это поможет специалистам по безопасности в их обнаружении.

Об угрозах другой новой технологии — динамического рендеринга — рассказал исследователь ИБ из американского стартапа r2c Василий Ермилов. Обычно подобные инструменты используют, чтобы предоставлять краулерам (Google, Slack, Twitter-бот) предварительно обработанные страницы сайта, таким образом улучшая SEO. Но неверная настройка динамического рендеринга открывает злоумышленникам возможность для проведения SSRF-атак. Причем для этого им не нужно будет тратить серьезные усилия, а еще более усугубляет ситуацию тот факт, что динамический рендеринг всегда применяют для самых важных и популярных страниц сайтов. Василий описал свой опыт поиска уязвимостей в сервисе Rendertron, который позволил ему получить контроль над одним из непубличных приложений. Кроме того, эксперт рассказал о том, как использовать опенсорсные инструменты, чтобы ускорить процесс выявления уязвимостей.

Новые подходы к защите от Microsoft

Злоумышленники все чаще смещают свой фокус на уровень прошивки и пытаются скомпрометировать процедуру загрузки системы. Один из примеров — уязвимость BootHole. В 2018 году уязвимости в прошивке использовала группировка Strontium. Об аппаратных механизмах защиты Windows 10 рассказал Артем Синицын, руководитель программ ИБ Microsoft в Центральной и Восточной Европе. Инициатива Secured-core PCs (SecOps) поддерживает создание компьютеров на базе Windows 10, защищенных от внешних атак на уровне прошивки. Такие системы обеспечивают биометрическую идентификацию без риска утечки данных, безопасное хранилище информации о кредитных картах и других критически важных данных, безопасную загрузку, защиту от буткитов и т. п. Помимо Microsoft Surface, на рынке уже есть устройства, поддерживающие Secured-core PCs, таких производителей, как Dell, Dynabook, HP, Lenovo, Panasonic.

Синицын также рассказал о том, сколько у Microsoft различных программ bug bounty — с их помощью повышают защищенность направлений Identity, Windows,

Xbox, Azure, Dynamics и Microsoft Edge. Артем подробно описал условия работы по обнаружению и обнародованию потенциальных уязвимостей, а также рассказал, что́ нужно знать перед подачей заявки через Coordinated Vulnerability Disclosure.

Угрозы для разработчиков

Популярные продукты для проверки качества кода или оценки уровня безопасности сами по себе могут быть точкой входа для APT-группировок. Денис Макрушин, руководитель группы перспективных исследований безопасности компании Huawei, рассказал, в частности, о SonarQube — платформе с открытым исходным кодом для анализа качества и защищенности программного кода. С помощью простого запроса «port:9000 sonarqube» в Shodan можно обнаружить десятки и сотни инсталляций, доступных из интернета, у некоторых отсутствует какая-либо аутентификация. В результате у злоумышленника появляется простой доступ к программному коду, разрабатываемому или проходящему проверку в организации.

В некоторых случаях не надо использовать Shodan. Разработчики и QA-инженеры сами выкладывают множество скриптов с конфиденциальной информацией в публичные репозитории, в которых с помощью элементарного GitHub-scrapping по запросу, например, «product_name+pass» можно обнаружить учетные данные или приватные ключи и сертификаты («domain_name+private»). Можно взять и коммерческое решение из квадранта Gartner, такое как Checkmarx, инсталляции которого обнаруживаются по запросу вида «CxWebclient», — и они также часто открыты для всех желающих. Для мониторинга и удаления подобных утечек можно использовать решения secret-management, например Hashicorp Vault.

Про QA-инженеров в своем выступлении говорил и Сергей Горохов, архитектор решений компании EPAM. Он рассказал о важности безопасной разработки, залогом которой должно стать тесное взаимодействие подразделений AppSec и security testing: «При оценке рисков, составлении требований, моделировании угроз, выстраивании архитектуры тестировщики должны присутствовать наравне с разработчиками, помогая последним».

Актуальную для создателей ПО проблему затронул аналитик ВПО Станислав Раковский. Он рассказал, как злоумышленник может модифицировать файлы PyInstaller и добавить в них немного полезной нагрузки. Файлы PyInstaller используются, если разработчик планирует распространять файлы Python, независимые от пользовательского окружения и интерпретатора. Докладчик отметил, что помимо полезной нагрузки во встроенный интерпретатор можно добавить различные антиотладочные инструменты и проверки на антивирусные продукты, чтобы модифицированное ПО могло скрыться в окружении, которое не устраивает атакующего. А обнаружить такие изменения в интерпретаторе весьма сложно.

Поиск иголки в стоге сена

Зачем обогащать данными инциденты ИБ? Для корректной расстановки приоритетов, маршрутизации уведомлений и адекватного реагирования. Но при обогащении инцидентов как никогда актуальна фраза «мусор на входе — мусор на выходе». Александр Кузнецов, руководитель ключевых проектов компании «Ростелеком-Солар», отметил, что если оператор SOC получает некорректные или

неполные данные, то они поступают в карточку инцидента и серьезно затрудняют расследование. Лучшими источниками данных автор назвал продукт Kaspersky Security Center, IPAM (служба управления IP адресами), AD DS (Active Directory Domain Services), TIP (платформа анализа информации об угрозах), EDR (система обнаружения сложных угроз на конечных точках). Что касается CMDB (база данных управления конфигурации), то эти решения, по мнению спикера, пока не полностью готовы для рассматриваемых в докладе задач. Проблемой для обогащения инцидентов становится удаленная работа — сотрудники стремительно меняют локации, технику и используют динамические IP-адреса. Если ничего для обогащения инцидентов нет, то можно начать даже с таблиц в Excel, но в зрелой инфраструктуре лучше использовать системы класса IRP или SOAR.

«Хороший SOC правильно работает тогда, когда его сотрудники понимают, как их могут атаковать и какие тактики и техники атак на текущий момент используют хакеры, — отметил в своем выступлении на круглом столе, посвященном теме SOC, директор экспертного центра безопасности (PT Expert Security Center) Positive Technologies Алексей Новиков. — Сотрудник SOC должен самообразовываться, изучать новые материалы. Это постоянная тренировка мозгов и стремление быть лучшим в области мониторинга и расследования инцидентов».

В свою очередь Роман Ладутько, исследователь вредоносного ПО, рассказал о том, как его команда анализирует активность одного из крупнейших ботнетов, Dridex. Чтобы определить, где владельцы ботнета нанесут следующий удар, приходится анализировать зловредные документы, искать управляющие серверы и домены, отслеживать их связь с другими ботнетами и периоды их активности. Роман показал цифры, подтверждающие эффективность этого подхода, и объяснил, как специалисты по защищенности могут его применять.

«Киберполигон The Standoff вышел на тот уровень, когда десятки команд нападающих и защитников с горящими глазами говорят "Ребята, это похоже на правду!", — поделился впечатлениями Юрий Максимов, генеральный директор Positive Technologies. — Противостояние действительно получилось очень точной моделью реальной жизни. А это открывает нам совсем другие перспективы. Наши продукты для обнаружения, блокирования атак и расследования инцидентов впервые попали в столь агрессивную атакующую среду. Мы все получили уникальный опыт, который позволит сделать продукты для ИБ умнее. А умные продукты освобождают людям время для творческой работы».

The Standoff завершен…» ***(The Standoff завершен: атаки выдержали только морской порт и железнодорожная станция // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/the-standoff-zavershen-ataki-vyderzhali-tolko-morskoj-port-i-zheleznodorozhnaya-stanciya/). 18.11.2020).***

***

«Согласно отчету Skybox Security, 73% руководителей уверены, что существуют дополнительные риски для организаций со стороны удаленных работников.

В 2020 году наблюдается рост уязвимостей на 34%. Эксперты считают это предпосылкой для увеличения количества будущих атак.

В отчете подчеркнули, что многие организации халатно относятся к защите удаленных рабочих мест. Более 30% опрошенных снизили приоритет обновлений ПО и политики BYOD (bring-your-own-device) с момента начала пандемии.

Вдобавок, треть опрошенных не может точно сказать, действительно ли настройки конфигураций и сети подрывают уровень безопасности. 55% признали, что оценить риски было трудно.

Это все вопреки факту, что 70% руководителей IT-сферы предполагают, что треть сотрудников продолжит работать удаленно следующие 18 месяцев.

Исследователи также отметили, что многие опрошенные были довольно самоуверенны в отношении возможностей своих компаний в сфере информационной безопасности. Несмотря на то, что всего 11% респондентов уверены в своей способности поддерживать целостный подход к обеспечению безопасности, а 93% опрошенных считают, что принимают верные решения в области информационной безопасности». ***(¾ руководителей обеспокоены безопасностью работы на удаленке для компании // SecureNews (https://securenews.ru/%c2%be-executives-are-concerned-about-the-safety-of-telecommuting-for-the-company/). 18.11.2020).***

***

«Основными препятствиями к внедрению решений для защиты промышленных сред респонденты опроса «Лаборатории Касперского» назвали невозможность остановить производство (34%), бюрократию, в том числе слишком долгий процесс одобрения (31%) и задержки, связанные с тем, что за принятие решений ответственно слишком большое количество людей (23%).

Кибератаки продолжают оставаться актуальной проблемой для промышленных компаний и АСУ ТП, и пандемия усугубила положение дел. Индустриальные предприятия вынуждены адаптироваться к новым нормам, таким как дистанционный режим работы, повсеместная цифровизация и дополнительные меры гигиены, а также к изменившемуся ландшафту киберугроз, например, растущему числу фишинговых атак. Организациям следует убедиться, что имеющиеся средства защиты эффективны в сложившейся ситуации и что промышленные сети ограждены от вредоносных действий.

Большинство барьеров, о которых сообщили респонденты, носят скорее бюрократический, чем технический характер. Почти половина организаций (46%) столкнулась с бумажными проволочками при реализации проекта по промышленной кибербезопасности. Помимо долгого процесса одобрения и большого числа согласующих помехи создают затянутые процессы выбора поставщиков и закупок, а также препятствия со стороны других отделов.

По мнению почти половины организаций (46%), из-за пандемии приоритеты в промышленной безопасности станут другими. Им, по всей видимости, нужно будет на ходу менять стратегию киберзащиты и быстро внедрять новые практики. Это может быть непросто из-за специфических требований на подобных объектах, а барьеры, о которых шла речь выше, могут еще больше тормозить весь процесс.

Каждая четвертая организация (24%) сообщила о том, что ситуация осложняется сокращением бюджета на промышленную безопасность в результате пандемии.

«Обсуждая эти препятствия с представителями российских предприятий, мы выяснили, что последние даже чаще сталкиваются с помехами, о которых говорили респонденты по всему миру. В то же время сокращение бюджета на безопасность промышленных систем в меньшей степени коснулось российской промышленности. В целом инвестировать деньги и ресурсы в проекты без прозрачного расчета коэффициента возврата инвестиций, к которым часто относятся инициативы по кибербезопасности, всегда труднее. Решения для защиты промышленных сред появились не так давно, поэтому пока их внедрение связано с рядом сложностей. Мы как вендор должны помочь предприятиям упростить и ускорить этот процесс. Наша задача — сделать коэффициент возврата инвестиций более прозрачным и объяснить все риски, чтобы клиенты с самого начала понимали все преимущества таких технологий и могли при необходимости убедительно представлять их своему руководству», — сказал Георгий Шебулдаев, руководитель департамента развития новых продуктов «Лаборатории Касперского».

Чтобы помочь компаниям ускорить реализацию проектов в области промышленной кибербезопасности, «Лаборатория Касперского» рекомендует следующие шаги: если у организации недостаточно соответствующего опыта, лучше внедрять решения поэтапно — начать с выстраивания организационных процессов и внедрения базовых мер кибербезопасности, таких как защитные экраны и защита конечных устройств, затем перейти к более сложным проектам, таким как мониторинг сетей, решения для предотвращения вторжений и SIEM-системы. Кроме того, существуют промышленные стандарты — ISO/IEC руководства, которые помогают организовать и ускорить выполнение проекта; разрешать внедрение только тех операционных технологий, которые обладают встроенными средствами безопасности. Это поможет в дальнейшем упростить процесс внедрения защитных решений и даст экспертам по безопасности OT-систем возможность тестировать новые инструменты в этих сегментах инфраструктуры; обучать людей, в частности проводить тренинги по промышленной безопасности для сотрудников ИБ-отделов и операционных инженеров и по цифровой грамотности для всей компании. Такие тренинги учат оценивать риски и определять зоны ответственности каждого сотрудника, а также повышают степень осведомленности коллектива в области кибербезопасности; выбрать надежное защитное решение для OT-компонентов и сетей, а также доверенных партнеров для его внедрения. Kaspersky Industrial CyberSecurity обеспечивает защиту конечных устройств и мониторинг сети, кроме того, включает в себя экспертные сервисы, в том числе анализ защищенности, услуги по реагированию на киберинциденты и самые актуальные данные об угрозах и возможных мерах противодействия». ***(«Лаборатория Касперского» назвала бюрократию основным барьерьером для инициатив в области промышленной кибербезопасности // CNews (https://safe.cnews.ru/news/line/2020-11-24_laboratoriya_kasperskogo). 24.11.2020).***

***

«Технологические гиганты будут подчиняться новому режиму, чтобы предоставить потребителям больший выбор и контроль над своими данными, помочь малому бизнесу процветать и гарантировать, что новостные агентства не будут вытеснены их более крупными соперниками.

Специальное подразделение цифровых рынков, которое будет создано в Управлении по конкуренции и рынкам (CMA), будет тесно сотрудничать с регулирующими органами, включая Ofcom и Управление комиссара по информации, чтобы ввести и обеспечить соблюдение нового кодекса для управления поведением платформ, которые в настоящее время доминируют в мире. рынок, такой как Google и Facebook, чтобы гарантировать, что потребители и малый бизнес не окажутся в невыгодном положении.

Онлайн-платформы приносят огромную пользу бизнесу и обществу. Их услуги облегчают и ускоряют работу и помогают людям оставаться на связи друг с другом. Миллионы людей делятся творческим контентом или рекламируют товары своего малого бизнеса в Интернете.

Но в Великобритании и за рубежом растет консенсус в отношении того, что концентрация власти среди небольшого числа технологических компаний сдерживает рост технологического сектора, сокращает количество инноваций и потенциально оказывает негативное влияние на людей и предприятия, которые полагаются на них.

Новый кодекс установит четкие ожидания для платформ, которые обладают значительной рыночной властью - известной как стратегический рыночный статус - в отношении того, что представляет собой приемлемое поведение при взаимодействии с конкурентами и пользователями.

В соответствии с новым кодексом от платформ, в том числе финансируемых за счет цифровой рекламы, может потребоваться, чтобы они были более прозрачными в отношении предоставляемых ими услуг и того, как они используют данные потребителей, давали потребителям возможность выбора в отношении получения персонализированной рекламы и не допускали наложения ограничений на их клиентов, которые затрудняют им использование конкурирующих платформ.

Новое подразделение, которое начнет работу в апреле, может быть наделено полномочиями приостанавливать, блокировать и отменять решения технологических гигантов, приказывать им предпринимать определенные действия для достижения соответствия кодексу и налагать финансовые санкции за несоблюдение.

Бизнес-секретарь Алок Шарма сказал:

Цифровые платформы, такие как Google и Facebook, вносят значительный вклад в нашу экономику и играют огромную роль в нашей повседневной жизни - будь то помощь в поддержании связи с нашими близкими, обмен творческим контентом или доступ к последним новостям.

Но доминирование всего нескольких крупных технологических компаний ведет к меньшему количеству инноваций, более высоким ценам на рекламу и меньшему выбору и контролю со стороны потребителей.

Наш новый, ориентированный на конкуренцию режим цифровых рынков обеспечит потребителям выбор, а меньшие фирмы не вытеснят.

Секретарь по цифровым технологиям Оливер Дауден сказал:

Я беззастенчиво занимаюсь технологией, и услуги цифровых платформ позитивно трансформируют экономику, принося огромные выгоды для бизнеса, потребителей и общества.

Но в Великобритании и за рубежом растет консенсус в отношении того, что концентрация власти среди небольшого числа технологических компаний сдерживает рост сектора, сокращает количество инноваций и оказывает негативное влияние на людей и предприятия, которые полагаются на них. Пришло время заняться этим и начать новую эру технического роста.

Сегодняшние предложения также могут помочь предоставить малым предприятиям справедливый доступ к сервисам платформы, включая цифровую рекламу, что позволит им расширить присутствие своего бизнеса в Интернете. Код может использоваться, чтобы гарантировать, что платформы не применяют несправедливые условия или политику к определенным бизнес-клиентам, включая издателей новостей.

В настоящее время доминирующие онлайн-платформы могут навязывать издателям новостей условия, которые ограничивают их возможности монетизировать свой контент, что серьезно влияет на их способность процветать.

Новый кодекс будет регулировать коммерческие договоренности между издателями и платформами, чтобы помочь издателям вести бизнес, помогая повысить устойчивость высококачественной онлайн-журналистики и публикации новостей в Великобритании.

Это будет составлять основную часть работы правительства по поддержке устойчивости ведущего мирового новостного издательского сектора Великобритании и обеспечения того, чтобы по мере того, как новости становятся все более доступными в Интернете, издатели получают справедливые условия от платформ, на которые они полагаются.

Правительство изложило свои планы по развитию нового подразделения и кодекса поведения в своем ответе на исследование рынка, которое оно попросило CMA провести на онлайн-платформах и в цифровом маркетинге.

Подразделение будет проинформировано о работе Целевой группы по цифровым рынкам, которая была создана в начале этого года для предоставления правительству рекомендаций по потенциальной разработке и реализации мер, способствующих конкуренции, включая методологию, которая определит, какие компании должны быть определены. как имеющий стратегический рыночный статус и как режим будет работать на практике.

Цифровой сектор внес в экономику Великобритании почти 150 миллиардов фунтов стерлингов в 2018 году, открывая возможности, повышая продуктивность и творческий потенциал во всех уголках Великобритании.

В ходе своего исследования CMA обнаружило, что, среди прочего, отсутствие конкуренции на цифровых рынках препятствует разработке новых ценных услуг для потребителей и приводит к повышению цен для предприятий, использующих платформы, которые затем передаются потребителям.

Исследование рынка CMA было проведено по заказу правительства как часть ряда шагов по развитию конкуренции в этой области. В 2018 году правительство создало комиссию экспертов по цифровой конкуренции под председательством профессора Джейсона Фурмана, которая в своем заключительном отчете Furman Review предложила новый режим конкуренции для рынков цифровых платформ. Правительство приняло шесть стратегических рекомендаций Furman Review, включая создание нового подразделения цифровых рынков (DMU) в начале этого года.

Правительство проконсультируется о форме и функциях Группы цифровых рынков в начале 2021 года и примет законы, как только позволит парламентское время…» ***(New competition regime for tech giants to give consumers more choice and control over their data, and ensure businesses are fairly treated // Government Digital Service (https://www.gov.uk/government/news/new-competition-regime-for-tech-giants-to-give-consumers-more-choice-and-control-over-their-data-and-ensure-businesses-are-fairly-treated). 27.11.2020).***

***

Сполучені Штати Америки

«В паре твитов, опубликованных во вторник, президент США Дональд Трамп объявил, что он «уволил» Криса Кребса, директора Агентства по кибербезопасности и безопасности инфраструктуры (CISA), в связи с недавним заявлением, в котором он назвал недавние президентские выборы самыми безопасными в истории США.

Трамп заявил, что заявление было «крайне неточным», вместо этого сославшись на «массовые нарушения и фальсификации» на выборах, которые он проиграл кандидату от демократов Джо Байдену.

Представитель CISA не был доступен для комментариев; Однако Кребс подтвердил в твиттере из своего личного кабинета.

До своего увольнения сегодня Кребс занимал должность директора CISA ровно два года и один день, с 16 ноября 2018 года, когда агентство было официально основано.

Слухи о том, что Трамп намеревается уволить высокопоставленного должностного лица CISA, начали распространяться на прошлой неделе, когда Кребс заявил нескольким своим коллегам, что ожидает его увольнения после усилий агентства по борьбе с кампаниями дезинформации избирателей во время недавних выборов.

Согласно отчету Reuters, Кребс оказался на плохой стороне Трампа после создания и запуска Rumor Control, веб-страницы на сайте CISA, где эксперты CISA развенчали слухи о фальсификации выборов, многие из которых президент США активно продвигал во время и после выборов как факты. в его аккаунте в Twitter.

После сообщения Reuters несколько официальных представителей демократов и экспертов по кибербезопасности встали на защиту Кребса.

Cyberscoop сообщил, что, хотя несколько депутатов-республиканцев ранее хвалили работу Кребса в CISA в предыдущие месяцы, никто не встал на его защиту после того, как вызвал гнев Трампа.

«Крис Кребс - выдающийся государственный служащий и именно тот человек, которого американцы хотят для защиты безопасности наших выборов», - заявил в своем сегодняшнем заявлении сенатор США Марк Р. Уорнер (демократ от штата Вирджиния), заместитель председателя Специального комитета Сената по разведке.

«Это говорит о многом, что президент решил уволить его просто за то, что он сказал правду». ***(Catalin Cimpanu. Trump fires CISA Director Chris Krebs // ZDNet (https://www.zdnet.com/article/trump-fires-cisa-director-chris-krebs/). 18.11.2020).***

***

«Компания Twitter наняла в качестве директора по информационной безопасности одного из руководителей хакерского сообщества CultoftheDeadCow. Прежде он работал в DARPA и Google.

Хакер с госнаградами

Twitter нанял в качестве директора по информационной безопасности знаменитого хакера Пейтера Затко (Peiter Zatko), известного также под никнеймом Mudge.

Затко — человек с чрезвычайно яркой биографией: в девяностые годы он был членом хакерских сообществ L0pht и Cult of the Dead Cow. Именно члены L0pht сформировали культуру «этического хакинга» (или «ответственного раскрытия уязвимостей»). Затко лично в 1995 г. опубликовал одно из первых исследований переполнения буфера — одной из самых распространенных и часто эксплуатируемых ошибок в программном коде. Кроме того, он написал ряд популярных средств для тестирования безопасности. Одним из самых известных стал L0phtCrack, инструмент для проверки устойчивости паролей против различных видов атак.

Помимо этого, Затко был одним из первых независимых экспертов по кибербезопасности, начавших открыто сотрудничать с властями и представителями бизнеса. В 1998 г. он выступал перед комитетом в Сенате США по теме самых серьезных уязвимостей Всемирной сети, а в 2000 г. президент США Билл Клинтон пригласил Затко на специальный саммит по информационной безопасности, в котором участвовали члены правительства и руководители крупных корпораций. Этот саммит был связан в не последнюю очередь с первыми массированными DDoS-атаками.

С 2004 г. Затко работал в компании BBN Technologies, правительственном подрядчике. В 2010 г. его назначили в качестве управляющего проектом DARPA, посвященном кибербезопасности. Затем в 2013 г. его пригласили на работу в Google. В 2015 г. он присоединился к ИБ-проекту #CyberUL, созданному по запросу Белого Дома. Сейчас мы наблюдаем новый виток его карьеры.

Информационная безопасность и борьба с дезинформацией

На новом месте Затко, по его собственным словам, будет заниматься информационной и физической безопасностью, а также вопросами обеспечения

надежности сайта и платформы в целом и борьбой с распространением дезинформации.

И это, возможно, один из самых проблемных аспектов будущей работы Затко. В предвыборный период Twitter и ряд других медиакомпаний подверглись жесточайшей медийной атаке за свою политику борьбы с предполагаемой (или настоящей) дезинформацией. После того как Twitter временно заблокировал распространение статьи, компрометировавшей родственников кандидата (на тот момент) в президенты США Джо Байдена, на компанию посыпались обвинения в самоуправстве и цензурировании информации в интересах сторонников Демократической партии США.

В 2020 г. Twitter пал жертвой кибератаки, в результате которой злоумышленники получили доступ к множеству аккаунтов различных знаменитостей, включая Джо Байдена, Илона Маска, Джеффа Безоса, Билла Гейтса и др. Очевидно, что в задачу Затко также будет входить предотвращение подобных ситуаций в будущем.

«Обеспечение информационной безопасности Twitter имеет огромное значение уже просто в силу размеров аудитории сервиса и потенциального количества жертв серьёзного сбоя, — говорит Михаил Зайцев, эксперт по информационной безопасности компании SEC Consult Services. — Затко — один из самых компетентных профессионалов в этой сфере, и его послужной список тому очевидное свидетельство. Возможно он как раз один из тех немногочисленных специалистов, кому поставленные задачи будут по силам». ***(Главой инфобезопасности Twitter стал легендарный хакер // CNews (https://safe.cnews.ru/news/top/2020-11-18_twitter_naznachila_glavoj_sluzhby). 18.11.2020).***

***

«Затраты на программу по разработке современного истребителя F-35 существенно возросли после того, как КНР скомпрометировала производителя программного обеспечения в цепочке поставок Lockheed Martin, что привело к необходимости перезаписи с нуля потенциально уязвимой системы. Об этом заявил специалист Центра стратегических и международных исследований Джеймс Льюис (James Lewis) в ходе заседания по вопросам киберобороны британской армии.

По словам Льюиса, Китай скомпрометировал системы субподрядчика, участвующего в разработке F-35 и предположительно заразил программное обеспечение, предназначенное для истребителя. Специалист не уточнил, о каком именно ПО шла речь, и удалось ли предотвратить инфицирование.

«Lockheed Martin выполнила отличную работу по защите своих систем […], но если идти ниже по цепи, не все обеспечивают тот уровень безопасности, который вам нужен. Так что это утверждение - через субподрядчика Китай смог получить доступ [к системам]. Мы не знаем, что они могли сделать, уязвимость была закрыта, а программное обеспечение по большей части переписано с нуля», - цитирует The Register заявление Льюиса.

В прошлом Льюис говорил об этом инциденте как о слухе, частично поясняющем высокую стоимость F-35. Судя по всему, данная атака не имеет отношения к инциденту 2017 года, когда злоумышленники проникли в компьютерную сеть ВВС США и украли материалы, касающиеся F-35, в том числе несколько гигабайтов данных, относящихся к дизайну и электронным системам истребителя.

Ранее в этом году Управление эксплуатационных испытаний и оценки (DOTE) США выпустило доклад, в котором в том числе раскритиковало процесс разработки программного обеспечения для F-35. В частности, регулятор отметил, что использование методологии Agile представляет высокий риск, поскольку применение стратегии MVP (минимально жизнеспособный продукт) для разработки критически важных компонентов, таких как системы управления полетом и вооружением, нельзя считать допустимой моделью.

Минимально жизнеспособный продукт (minimum viable product, MVP) — продукт, обладающий минимальными, но достаточными для удовлетворения первых потребителей функциями. Основная задача - получение обратной связи для формирования гипотез дальнейшего развития продукта». ***(Китай обвинили в заражении ПО для истребителя F-35 // SecurityLab.ru (https://www.securitylab.ru/news/514065.php). 14.11.2020).***

***

«Отныне отчеты Пентагона об иностранных хакерах будут сопровождаться карикатурными иллюстрациями.

Мало кому понравятся уничижительные издевки в его адрес, в особенности киберпреступникам. Именно такую тактику решило применить Киберкомандование США к «русским хакерам» - публично высмеять их, выставив неуклюжими и безобидными мультяшками.

Как сообщает CyberScoop, Киберкомандование (подразделение Минобороны США) обратилось к компании, занимающейся графическим дизайном, с просьбой иллюстративно изобразить иностранных хакеров. Киберкомандование решило, что смешные иллюстрации помогут не только разнообразить их отчеты об операциях иностранных киберпреступников, но и раздосадовать самих хакеров, сообщил осведомленный источник.

Одними из хакеров, проиллюстрированных графическими дизайнерами, являются киберпреступники из России. По словам источника, они ненавидят, когда их изображают белыми и пушистыми, поэтому Киберкомандование попросило художников нарисовать их в виде милых и неуклюжих мишек.

Медведь был выбран не случайно, так как для группировок «русских хакеров» уже давно используются названия Cozy Bear («Уютный медведь») и Fancy Bear («Модный медведь»). Ранее сообщения об этих группировках сопровождались изображениями сильных и разъяренных хищников, но теперь Киберкомандование решило, что пришло время прекратить раздувать их самомнение.

«Нам не нужен логотип, который они смогли бы напечатать у себя на футболках. Мы хотим что-нибудь такое, что их босс увидит в PowerPoint и выйдет из себя», - сообщил источник.

Таким образом, 29 октября нынешнего года вышел отчет, проиллюстрированный мультяшным изображением мишки, запутавшегося в полах своего военного пальто и рассыпавшего конфеты, собранные на Хэллоуин.

Когда Киберкомандование заказало карикатуру на хакеров (китайских) в первый раз, художникам пришлось перерисовать свои наброски, так как они оказались недостаточно глупыми.

Попытки разозлить хакеров – это лишь новая глава в более масштабной кампании по подрыву кибероперацій иностранных правительств, проводимой Киберкомандованием». ***(Пентагон троллит русских хакеров с помощью мультяшек // SecurityLab.ru (https://www.securitylab.ru/news/514054.php). 13.11.2020).***

***

Країни ЄС

«Апостольская библиотека, сталкивающаяся со 100 угрозами в месяц, хочет, чтобы читатели могли доверять оцифрованным записям ее исторических сокровищ.

Древний интеллект теперь охраняется искусственным интеллектом, который предпринимает шаги по защите одной из самых выдающихся коллекций исторических рукописей и документов в мире от кибератак.

Ватикан Апостольская библиотеку, которая имеет 80.000 документов огромной важности и неизмеримую ценность, в том числе старейшей копии Библии и рисунков и сочинений от Микеланджело и Галилея, сотрудничают с кибером-безопасностью фирмой, чтобы защитить свой амбициозный проект оцифровывания против преступников.

По словам Манлио Мичели, директора по информационным технологиям, библиотека сталкивается в среднем с 100 угрозами в месяц с момента начала оцифровки своей коллекции исторических сокровищ в 2012 году.

«Мы не можем игнорировать то, что наша цифровая инфраструктура интересна хакерам. В случае успешной атаки коллекция может быть украдена, обработана или полностью удалена», - сказал Мичели в интервью Observer.

Он добавил, что кибератаки увеличиваются, а не замедляются. «Хакеры всегда будут пытаться проникнуть в организации, чтобы украсть информацию, заработать деньги или нанести ущерб».

Библиотека, основанная в 1451 году Папой Николаем V, является одним из самых важных исследовательских институтов в мире, содержащим одну из лучших коллекций рукописей, книг, изображений, монет и медалей в мире. Оцифровка 41 миллиона страниц призвана «сохранить содержание исторических сокровищ, не нанося ущерба хрупким оригиналам», - сказал Мичели.

Но он добавил: «Этот проект - гораздо больше, чем просто физическая сохранность. Части истории, ранее исследованные только историками в белых перчатках, теперь доступны любому, у кого есть подключение к Интернету. Это огромный шаг к равенству в образовании».

К настоящему времени оцифровано около 25% документов библиотеки. По словам Мичели, проект начался с «уникальных, самых известных и хрупких вещей». Они включают одну из старейших рукописей в мире, иллюстрированный фрагмент Энеиды Вергилия, возраст которой составляет 1600 лет. Коллекция также содержит иллюстрацию Сандро Боттичелли 1450 года к «Божественной комедии»; стихи, технические заметки и зарисовки Микеланджело; древние рукописи людей инков; и исторические договоры и письма.

Но, по словам Мичели, оцифровка означает, что «мы должны защищать нашу онлайн-коллекцию, чтобы читатели могли быть уверены, что записи являются точной и неизменной историей». Он добавил: «Хотя физический ущерб часто очевиден и незамедлительно, атака такого рода не будет иметь такой же физической видимости и, следовательно, может нанести длительный и потенциально непоправимый ущерб не только архиву, но и исторической части мира. объем памяти. В эпоху фейковых новостей эти коллекции играют важную роль в борьбе с дезинформацией, поэтому защита их от «атак на доверие» имеет решающее значение.

«Менее Голливудские, но все же вызывающие беспокойство, это атака программ-вымогателей на библиотеку - хорошо известная атака, которая незаметно проникает в компании, а затем невероятно быстро блокирует файлы, пока вы не заплатите огромную сумму. Сегодня программы-вымогатели движутся со скоростью машины, превосходя способность людей обнаруживать и останавливать атаку до ее эскалации.

«Эти атаки могут повлиять на репутацию библиотеки Ватикана, которую она поддерживала на протяжении сотен лет, и иметь серьезные финансовые последствия, которые могут повлиять на нашу способность оцифровывать оставшиеся рукописи».

Библиотека сотрудничает с Darktrace, компанией, основанной математиками Кембриджского университета, которая утверждает, что первой разработала систему искусственного интеллекта для кибербезопасности. Мичели сказал: «Вы не можете бросать людей на эту проблему - вам нужно дополнить людей технологиями, которые понимают оттенки серого в очень сложных системах и сопротивляются со скоростью машины».

ИИ «никогда не спит, не делает перерывов и может обнаружить и расследовать больше угроз, чем могла бы любая человеческая команда. Он за секунды принимает решения о том, что странно, но мягко и странно, но угрожающе» Но, добавил он, 100% гарантии от нападения нет. «Единственный способ сделать организацию полностью защищенной - это отключить ее от Интернета. Наша миссия - перенести библиотеку Ватикана в 21 век, поэтому мы не будем этим заниматься в ближайшее время»…». ***(Harriet Sherwood. Vatican enlists bots to protect library from onslaught of hackers // Guardian (https://www.theguardian.com/world/2020/nov/08/vatican-enlists-bots-to-protect-library-from-onslaught-of-hackers). 08.11.2020).***

***

«Как сообщает PwC, 22% компаний в Великобритании планируют сокращать команды, которые занимаются информационной безопасностью. Чтобы составить Стратегию Кибербезопасности 2021, PwC опросила 3249 компаний, среди которых 265 были из Великобритании.

96% опрошенных глобально отстают по нескольким фронтам, хотя изменили свою стратегию в отношении кибербезопасности из-за пандемии. Часть из них заявила, что сделает защиту информации неотъемлемой составляющей каждого бизнес-решения в компании.

Однако только 38% британских компаний были уверены, что затраты на кибербезопасность оправданы. 56% компаний заявили, что увеличат бюджет в следующем году, но лишь 36% видели смысл в своих тратах.

Глава кибербезопасности PwC утверждает, что бизнесам нужно понимать возможность угроз кибербезопасности так хорошо, чтобы это действительно стало частью каждого бизнес-решения.

Треть британских компаний собирается ускорить цифровизацию из-за пандемии. Большинство считает атаки на облачные сервисы, критические бизнес-сервисы и программы-вымогатели наиболее вероятными угрозами в будущем году». ***(Британские компании планируют сокращать команды по информационной безопасности // SecureNews (https://securenews.ru/british-companies-plan-to-cut-cyber-security-teams/). 11.11.2020).***

***

«На секретной видеоконференции присутствовали министры стран Евросоюза. Главной темой стало обсуждение документа, который длительное время подготавливался всеми разведслужбами ЕС. Он посвящён потенциальным угрозам странам Европы.

"Вы знаете, что вы попали на секретную конференцию?", - спросил журналиста глава дипломатии ЕС Жозеп Боррель под смех некоторых официальных лиц.

"Да, да. Мне жаль. Я журналист из Нидерландов. Простите, что прерываю вашу конференцию", - ответил улыбающийся Верлаан.

Оказалось, что этот молодой человек - нидерландский журналист Даниэль Верлаан из RTL Nieuws. Он объяснил своим случайным собеседникам, что ничего не взламывал. Журналисту тут же сообщили: его появление на секретной конференции тянет на уголовное преступление - и потребовали срочно отключиться. Дважды просить не пришлось.

Этот инцидент вызвал серьезные вопросы о безопасности конфиденциальных встреч ЕС. Как выяснили СМИ, нидерландский журналист получил доступ к конфиденциальной видеоконференции министров обороны стран ЕС благодаря информации, опубликованной в аккаунте министра обороны Нидерландов в Twitter. Позднее стало известно, что представитель ведомства случайно опубликовал в соцсети фотографию, содержащую секретную информацию.

Чиновники в ходе видеоконференции обсуждали секретный документ о потенциальных угрозах Евросоюзу. Сбором данных занимались все разведывательные службы ЕС. Планируется, что благодаря документу ЕС может

продвигаться в разработке ответов на угрозы. Противодействие будет сконцентрировано на четырех направлениях работы: обеспечение устойчивости в области безопасности, развитие потенциала реагирования на угрозы, партнерство, антикризисное управление. Для реализации всех составляющих проекта понадобится несколько лет». ***(Журналист подключился к секретной конференции министров стран Евросоюза // SecurityLab.ru (https://www.securitylab.ru/news/514224.php). 21.11.2020).***

***

«Уряд у Лондоні вважає, що може захиститися від кібератак завдяки усуненню Huawei від розбудови мереж 5G. Законопроєкт передбачає штрафи до 113 тисяч євро на день.

Уряд Великобританії планує відсторонити китайський концерн Huawei від розбудови інфраструктури для мобільних мереж 5G на території країни. Також урядовці збираються запровадити великі штрафи за порушення цієї заборони.

"Новий законопроєкт - один із найжорсткіших у світі законів про безпеку в сфері телекомунікацій, який дозволить Великобританії вжити заходів, необхідних для захисту наших мереж", - заявив міністр цифрових технологій Великобританії Олівер Дауд у вівторок, 24 листопада.

Відповідно до законопроєкту, за використання компонентів Huawei для мереж 5G передбачений штраф розміром до десяти відсотків обороту або 113 тисяч євро на день. В уряді вважають, що суворіші стандарти у сфері безпеки допоможуть захистити Великобританію від можливих кібератак.

Huawei розчарований рішенням Лондона

Huawei висловив розчарування діями британського уряду. "Це рішення політично мотивоване і не ґрунтується на справедливій оцінці ризиків", - заявив віцепрезидент китайського концерну Віктор Чжан. Він вважає, що ця заборона відсторонить Великобританію на "смугу повільного руху" у сфері цифровізації…». ***(Марія Думанська. Великобританія штрафуватиме за використання компонентів Huawei // Deutsche Welle (https://www.dw.com/uk/velykobrytaniia-shtrafuvatyme-za-vykorystannia-komponentiv-huawei/a-55708778?maca=ukr-rss-MetaUA-ukr-Business_Finansy-3053-xml-mrss). 24.11.2020).***

***

Російська Федерація та країни ЄАЕС

«Кабмин внёс в парламент законопроект о введении административной ответственности за нарушение требований по обеспечению безопасности КИИ РФ, а также за несвоевременное предоставление сведений отвечающим за ликвидацию кибератак органам.

Правительство РФ внесло в Госдуму законопроект №1048574-7 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической

информационной инфраструктуры (КИИ) Российской Федерации», которым вводятся крупные административные штрафы за неисполнение положений закона о КИИ.

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

Нарушение «порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак», согласно тексту законопроекта, будет грозить должностным лицам штрафом в размере от 10 тыс. до 50 тыс. рублей, а юридическим лицам — от 100 тыс. до 500 тыс. рублей. Также за нарушение порядка обмена данными об инцидентах между субъектами такой инфраструктуры, иностранными уполномоченными органами, международными организациями и НПО, работающими в сфере реагирования на киберугрозы, предусмотрены штрафы — для должностных лиц от 20 тыс. до 50 тыс. рублей, для юридических лиц — от 100 тыс. до 500 тыс. рублей.

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

Если уполномоченный орган исполнительной власти не будет уведомлен (уведомлен с опозданием) о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости, то штраф составит от 10 тыс. до 50 тыс. рублей для должностных лиц и от 50 тыс. до 100 тыс. рублей — для юридических лиц. Согласно пояснительной записке, «размеры предлагаемых штрафов учитывают размер средней заработной платы руководителей структурных подразделений по обеспечению информационной безопасности».

В качестве обоснования необходимости предложенных мер Правительство приводит масштабную атаку 2017 года с использованием вируса-шифровальщика WannaCry, который поразил большое количество вычислительной техники в ряде госкомпаний, на восстановление которой ушло от 1 до 3 суток. Причиной ущерба стало невыполнение установленных требований, включая требование о своевременном обновлении программного обеспечения.

Полномочиями по рассмотрению административных дел о правонарушениях по предложенным статьям предлагается наделить ФСТЭК и ФСБ. Положение о штрафах за нарушение порядка информирования о компьютерных инцидентах и принятия мер по их ликвидации должно вступить в силу с 1 сентября 2021 года…». ***(Критическую информационную инфраструктуру хотят защитить штрафами // РосКомСвобода (https://roskomsvoboda.org/65915/). 03.11.2020).***

***

«В 2020 г. пришло время переходить от обсуждений к практическим действиям в реализации требований безопасности КИИ. Комплексная система защиты значимых объектов КИИ минимизирует риски остановки производства из-за киберинцидентов и чрезвычайных ситуаций, а также позволяет обеспечить требования нормативно-правовых актов и избежать санкций от надзорных органов. О том, как обеспечить безопасность объектов КИИ и выполнить все требования законодательства, в своей статье для CNews рассказал Роман Жуков, директор центра компетенций «Гарда Технологии».

Текущая ситуация в области законодательства о БКИИ

Структура БКИИ (безопасности критической информационной инфраструктуры) — это три основных федеральных закона (187-ФЗ, 193-ФЗ и 194-ФЗ), приказы ФСТЭК (№227, 229, 235, 236, 239), приказы и рекомендации ФСБ (№366, 367, 358, 196, 281 и 282), а также ведомственные приказы и рекомендации Минпромсвязи, Минпромэнерго и Центрального банка.

Согласно письму ФСТЭК, на первом этапе госсектор должен был к 1 сентября 2020 г. завершить процедуру категорирования. Алгоритм действий данного этапа предполагает инвентаризацию (описание систем и процессов, привязку к объектам КИИ, оценку состояния ИБ и набора СЗИ), выбор способа защиты (оценка типовых объектов и процессов, влияющих на КИИ), категорирование (указание отраслевой специфики, проведение комиссии и составление актов), а также подачу перечня объектов во ФСТЭК.

Второй этап предполагает составление требований и апробацию решений для обеспечения ИБ, проектирование (проектные решения на продукты и решения, а также документация), внедрение решений и составление всей документации с оценкой эффективности последующей эксплуатации. Результатом второго этапа становится комплексное обеспечение БКИИ.

Говоря о законодательстве, нельзя не упомянуть о разработке нового ГОСТ по ГосСОПКА для субъектов КИИ. Он полезен тем, что в нем предусмотрена визуализация терминов и концепция процессов, структурированы данные для обучения, а также приведены в соответствие различные документы. В случае принятия нового ГОСТ можно будет обосновывать собственные проекты по построению SOC субъектов КИИ.

Помимо этого, достоянием общественности стал проект приказа ФСТЭК о подключении 30 объектов КИИ к интернету. Он будет действовать только для вновь создаваемых объектов и потребует согласования подключения объектов КИИ к сети связи общего пользования путем направления во ФСТЭК копии модели угроз, в том числе схемы организации связи, номеров сертификатов или протоколов оценки испытаний…

Судебная практика в области обеспечения безопасности КИИ

Еще до выхода новых статей КоАП РФ появились судебные дела по нарушениям защиты КИИ, касающиеся действующего законодательства.

5 августа 2020 г. прокуратура Приморского края утвердила обвинительное заключение по уголовному делу в отношении 21-летнего местного жителя. Он

обвиняется в совершении преступления, предусмотренного ч.2 ст. 274.1 УК РФ (неправомерный доступ к охраняемой компьютерной информации, относящейся к критической информационной инфраструктуре РФ, повлекшей причинение вреда информационной системе). При помощи двух подельников злоумышленник получал пароли доступа к личным кабинетам абонентов и активировал переадресацию входящих вызовов на свой номер. Это позволило ему получить доступ к аккаунтам соцсетей, к которым привязаны номера, чтобы в дальнейшем использовать страницы в корыстных целях. Персональные данные абонентов телекоммуникационной компании относятся к объектам КИИ.

Сотрудник отдела оператора связи отправил сведения расположения узлов связи (военных частей, ФСБ, УФСИН, МВД) на личный почтовый ящик. (ч.4 ст. 274.1 — с использованием служебного положения). Копия письма сохранилась на облачном узле компании Google, зарегистрированной в США. На этом основании причинен вред КИИ Российской Федерации.

Во Владивостоке вынесен приговор по делу в сфере компьютерной информации, согласно ч. 4 ст. 274.1 УК РФ. Сотрудница телекоммуникационной компании скопировала на флешку персональные данные абонентов и затем переслала их знакомому, тем самым причинив вред критической информационной инфраструктуре.

Группа мошенников незаконно осуществила неправомерный доступ к компьютерной информации компании «Восточная верфь», зашифровала данные и требовала выкуп за них в биткоинах. Это повлекло за собой нарушение производственного процесса и причинение имущественного вреда в размере 655 тыс. руб. Наказание для всех участников преступной группы последовало также по ч.4 ст. 274.1 УК РФ и составило 2 года лишения свободы условно и 2 года запрета доступа к объектам КИИ.

В институте вулканологии сотрудник сканировал в 2019 г. сайт Роскомнадзора на уязвимости. Его хотели привлечь по статье 274.1 УК РФ. Суд посчитал это незаконным доступом к КИИ, хотя категорирования еще не было.

Импортозамещение для объектов КИИ

Пока в приказах ФСТЭК нет четких требований о том, что все оборудование и ПО объектов КИИ должны быть исключительно российской разработки. Но на значимом объекте не допускается прямой удаленный доступ к программно-аппаратным средствам объектов КИИ, а также наличие локального бесконтрольного доступа. Средства должны быть размещены на территории РФ. Это не значит, что прямой доступ из-за рубежа запрещен, можно обойти. Поправки в приказ ФСТЭК № 239, касающиеся запрета доступа к объектам КИИ даже для технической поддержки из-за рубежа, не прошли, но можно сделать выводы о тенденциях в этом направлении и о намерениях регуляторов. Поэтому об импортозамещении стоит задуматься уже сейчас.

Практика защиты объектов КИИ

Законодательство о безопасности КИИ — один из первых шагов к внедрению процессного подхода. В приказе №235 и других есть такие понятия как «жизненный цикл информационной системы». Основной фокус делается на предотвращении неправомерного воздействия. Уголовная ответственность

наступает за конкретные последствия или причиненный ущерб. В нормативных актах фигурирует обнаружение, реагирование и расследование инцидентов. В отличие от нормативных документов по ПДн, здесь подробно описан процессный подход. Этим можно пользоваться для внедрения практической безопасности. «Гарда Технологии» как вендор выступает за практическую безопасность, чтобы защитить бизнес от шифровальщиков, других реальных атак и внутренних злоумышленников.

Актуальность проблемы обеспечения информационной безопасности доказывает международный опыт 2020 г. Например, в апреле датский производитель насосов стал жертвой кибератаки, следствием чего стало отключение всех компьютерных систем предприятия. В июне взламывали серверы АЗС, чтобы использовать бесплатное топливо. Целевым атакам подверглась израильская компания SCADA — производитель систем водоснабжения. Кроме того, на 2020 г., по данным Shudan, в свободном доступе благодаря уязвимости Blue Keep находится более 80 тыс. RDP-протоколов.

Что происходит с важными системами в организации?

Основа для информационных систем и приложений — это базы данных как источник корпоративной и технологической информации. Кроме владельцев, этой информацией интересуется множество злоумышленников — инсайдеров, хакеров. Защитить базы данных (в том числе на объектах КИИ) позволяет специализированная система «Гарда БД».

Применение «Гарда БД» на объектах КИИ

Аудит действий сетевых и БД администраторов КИИ;

Защита критичных БД КИИ;

Выявление «случайных» БД на объектах КИИ;

Детектирование специфичных инцидентов;

Фиксация и расследование инцидентов, связанных с доступом к КИИ.

В нормативных документах по КИИ и ГосСОПКа обозначено, что все факты об инцидентах должны фиксироваться и отправляться в ГосСОПКу. «Гарда БД» фиксирует все обращения к базам данных и веб-приложениям. Даже если инцидент пропустили, всю фактуру по нему можно собрать, скомпоновать и отправить в компетентные органы по запросу.

Что умеет система «Гарда БД»

предотвращать выгрузки и продажи данных клиентов, включая персональные данные и данные кредитных карт;

контролировать манипуляции с клиентскими базами, включая накрутку KPI (Key Performance Indicators ключевые показатели эффективности);

проверять БД на обезличенность при их передаче;

разграничивать доступ к СУБД для аттестации информационных систем;

выявлять не оптимально настроенные конфигурации СУБД с точки зрения стандартов и лучших практик по ИБ;

предотвращать мошенничество и прямые хищения денежных средств с использованием БД и бизнес-приложений компании;

выявлять несанкционированное разворачивание теневых неучтенных баз данных со стороны администраторов.

На практике уже реализовано несколько кейсов применения «Гарда БД» в качестве наложенного средства защиты информации (СЗИ) при аттестации информационных систем. Особенно, когда применяются несертифицированные СУБД или уровень сертификации для организации недостаточен.

С помощью «Гарда БД» как сертифицированного отечественного решения удается закрыть требования к разграничению доступа к информации. Например, в комплексной информационной системе, где объединен бухгалтерский, кадровый учет, ERP и другие системы.

Решение «Гарда Монитор» отвечает на вопрос «что происходит в сети компании». С точки зрения защиты КИИ — это главный вопрос. Поэтому решение становится инструментом для ежедневной работы сотрудников компании — как офицеров безопасности, так и руководителей ИБ, ИТ-специалистов и аналитиков SOC.

Практика применения

Майнинг на рабочем месте

На объектах, относящимся к КИИ, выявляется майнинг на рабочих местах, который опсен тем, что нецелевым образом используются ресурсы и время сотрудников, в сети появляются вирусы под видом майнер-клиентов и майнеры-вредоносы. Такой ущерб крайне сложно доказать без прямых фактов, которые предоставляет «Гарда Монитор».

Нелегальный удаленный доступ

Опасен потерей контроля доступа при подключении из любых локаций, риском появления вирусной активности и сложностью при расследовании, когда нет ясности, откуда кто подключается и чем пользуется.

Защита от заражения вредоносным ПО и от внешних атак

Применение «Гарда Монитор» на объектах КИИ обеспечит запись и хранение всего сетевого трафика, детектирование специфических угроз для АСУ ТП, распределенную установку, позволяющую контролировать SOC, а также пассивное внедрение без влияния на сеть.

Отдельно стоит остановиться на теме обеспечения информационной безопасности в технологическом сегменте (АСУ ТП). Такие факты, как появление новых устройств, использование неучтенных накопителей, обнаружение нетипичного трафика, выявление ошибок разграничения доступа или непроизводственная активность на подключенных к сети устройствах — уже сами по себе — индикаторы нарушения безопасности АСУ ТП. Чем раньше об указанных инцидентах станет известно службе безопасности (а «Гарда Монитор» работает в режиме реального времени), тем больше будет шансов предотвратить негативное развитие событий, например: заражение устройств и захват управления, нарушение технологического процесса, несанкционированная передача данных за периметр безопасности, проникновение в другие сетевые сегменты.

«Гарда Монитор» осуществляет контроль сетевых соединений на периметре (глубокий разбор содержимого пакетов и сигнатурный анализ) и позволяет обнаружить нелегитимный трафик (игровой, YouTube, BitTorent), несанкционированное подключение к SCADA-серверу из внешнего сегмента и изменение параметров работы технологического оборудования, сканирование

хостов технологического сегмента сети, подбор паролей, эксплуатацию уязвимостей в ПО устройств, ошибки в настройках межсетевых экранов и маршрутизаторов.

Оценка ситуации на рабочих устройствах

Рассмотрим пример работы DLP-системы «Гарда Предприятие» в контроле информационных потоков на сети и через агентов рабочих мест. Система позволяет гибко управлять процессами передачи данных и анализировать все данные для определения инцидентов, особенно при мониторинге сотрудников на удаленке. Применение на объектах КИИ включает установку легких агентов (в том числе на старые ОС), тотальную запись всех действий на АРМ, запрет носителей и приложений, выявление «теневых» ИТ в условиях запретов на АСУ ТП, фиксацию юридически значимых фактов.

Применение решений «Гарда Технологии» обеспечивает практическую безопасность объектов критической информационной инфраструры. Все продукты поддерживают гео-распределенную кластерную инсталляцию с возможностью управления каждым из них в режиме одного окна. Это значит, что можно мониторить и защищать объекты КИИ в филиалах из единого центра с настройкой ролевых моделей, хранением и обработкой больших объемов данных.

Соответствие нормативным требованиям

При выстраивании процессов организации ИБ объектов КИИ нужно провести ревизию процессов, согласовать обмен с ГосСОПКА, не забывать про реальную безопасность, согласовать с другими НПА, использовать выпущенные ОРД в своих целях.

Решения «Гарда Технологии» помогают закрыть отдельные требования приказа №239 ФСТЭК России по обеспечению безопасности объектов КИИ. «Гарда Предприятие» — некоторые меры из групп ОПС, ЗНИ, АУД, ОЦЛ, ЗИС, ИНЦ. «Гарда БД» — некоторые меры из групп ИАФ, УПД, АУД, ОЦЛ, ЗИС, ИНЦ. «Гарда Монитор» — некоторые меры из групп УПД, АУД, СОВ, ЗИС, ИНЦ, УКФ.

В рамках выполнения требований к техническим средствам ГосСОПКА, согласно приказу №196 ФСБ России, в качестве средств по обнаружению и предупреждению атак, а также средств поиска компьютерных атак в сетях электросвязи могут выступать «Гарда БД», «Гарда Предприятие», «Гарда Монитор». При этом продукты способны выявлять более 80% категорий инцидентов из тех, которые нужно фиксировать для отправки в НКЦКИ. Среди них: заражение вредоносным программным обеспечением, распространение вредоносного программного обеспечения, нарушение или замедление работы контролируемого информационного ресурса, несанкционированный доступ в систему, попытки несанкционированного доступа в систему или к информации, сбор сведений с использование ИКТ, нарушение безопасности информации, распространение информации с неприемлемым содержимым, мошенничество с использованием ИКТ, уязвимости.

Нередко для обеспечения безопасности достаточно поставить антивирус, межсетевой экран и IDS (Intrusion Detection System, системы обнаружения вторжений), но этого недостаточно, чтобы снизить риски инцидентов, в частности, несанкционированного доступа к системе. Решения «Гарда Технологии»

закрывают потребности в безопасности на всех информационных уровнях компании: на рабочих местах, в бизнес-приложениях, в сетевом трафике». ***(Роман Жуков. Безопасность КИИ: как перейти от нормативов к практическим внедрениям // CNews (https://safe.cnews.ru/articles/2020-11-23_bezopasnost_kii_kak_perejti_ot). 23.11.2020).***

***

«Банк России проведет реструктуризацию своего департамента информационной безопасности. ФинЦЕРТ, основное подразделение департамента, отвечающее за реагирование на компьютерные инциденты, будет расформировано, а его функции — надзор над деятельностью банков в сфере ИБ и мониторинг киберрисков — перейдут другим управлениям.

Центробанк реструктурирует службу безопасности

Банк России (Центробанк, ЦБ) приступил к капитальной реструктуризации своего департамента информационной безопасности (ДИБ). Скорее всего, как пишет «Коммерсант», это приведет к расформированию подразделения «ФинЦЕРТ» (CERT, computer mergency response team, группа реагирования на компьютерные инциденты), которое с 2018 г. имеет статус управления в структуре ДИБ.

Основная цель, которой может руководствоваться ЦБ, — попытка разнести функции надзора над деятельностью банков в сфере ИБ и функции мониторинга киберрисков по разным управлениям, чтобы банки, обращаясь за помощью, не получали наказание, как это происходит сейчас. В настоящее время обе эти функции выполняет «ФинЦЕРТ».

…в ЦБ подтвердили, что с 5 ноября 2020 г. поменялась структура ДИБ. «Изменения связаны с необходимостью усиления основных бизнес-процессов. От них зависит достижение целевых показателей, предусмотренных "Основными направлениями развития ИБ кредитно-финансовой сферы на период 2019–2021 гг."», — сообщили представители ЦБ. Среди таких процессов — обработка информации о противодействии операциям без согласия клиентов финансовых организаций, которая поступает в ЦБ от участников информационного обмена. Кроме того, усиливается направление риск-ориентированного надзора за обеспечением финансовыми организациями киберустойчивости и операционной надежности.

Пока неизвестно, как будет выглядеть новая структура, также, возможно, останется и название «ФинЦЕРТ», так как на раскрутку этого бренда ушло пять лет, однако функции будут переданы другим управлениям.

На сегодняшний день в системе информационного обмена «ФинЦЕРТа» участвуют более 800 организаций, в том числе все российские банки, а также правоохранительные органы, провайдеры, операторы связи, системные интеграторы, разработчики антивирусного ПО и другие компании, работающие в сфере ИБ. Подключиться к системе информационного обмена может любой участник финансового рынка или компания, работающая в области защиты информации в финансовой сфере.

Почему банки недовольны работой «ФинЦЕРТа»

Главная задача «ФинЦЕРТа» — обеспечивать ИБ кредитно-финансовых организаций путем взаимного информирования и оповещения участников финансового рынка об уязвимостях, угрозах и рисках, с которыми им приходится сталкиваться, и о методах их предотвращения. Проще говоря, «ФинЦЕРТ» собирает от банков информацию о кибератаках, анализирует ее и на этой основе информирует их об актуальных угрозах кибербезопасности, а также разрабатывает рекомендации по отражению хакерских атак. Также «ФинЦЕРТ» взаимодействует с правоохранительными органами и оперативными службами ФСБ. Оперативный обмен информацией о компьютерных атаках с банками ведется в том числе с помощью автоматизированной системы обработки инцидентов (АСОИ).

На сегодняшний день предоставление информации в «ФинЦЕРТ» не является для финансовых организаций обязательным и происходит на добровольной основе. Тем не менее статус «ФинЦЕРТа» был спорным, по мнению участников рынка, изначально, так как, обращаясь в «ФинЦЕРТ» с сообщением об инциденте, банк тем самым давал повод для проверки и наказания самого себя, пишет «Коммерсант». Поэтому о части инцидентов банки просто умалчивали.

Качество помощи тоже оставляет желать лучшего. Как предположил один из собеседников «Коммерсанта», последней каплей могла стать история с выводом средств через систему быстрых платежей в августе 2020 г. «ФинЦЕРТу» понадобилось около двух недель, чтобы предупредить рынок об этой уязвимости, а потом выяснилось, что обращения ряда банков об инцидентах с СБП, в том числе и за 2019 г., не были рассмотрены вообще.

Участники рынка надеются, что в новой структуре функции ДИБ будут разнесены по различным управлениям, а специализация работы позволит работать более оперативно. Однако, как пишет «Коммерсант», это может сыграть злую шутку, так как после реструктуризации проверки банков со стороны регулятора могут ужесточиться…». ***(Ирина Пешкова. Российские банки перестанут наказывать за атаки хакеров // CNews (https://safe.cnews.ru/news/top/2020-11-12_tsb_perestanet_nakazyvat). 12.11.2020).***

***

«Согласно отчету Check Point Software Technologies по вредоносным атакам в России за период с мая по октябрь 2020 года, за последние полгода компании в России подвергались кибератакам примерно 689 раз в неделю, в то время как по всему миру среднее число атак на организацию составило 503.

В среднем в неделю 11,5% компаний были атакованы ботнетами, 8,5% — криптомайнерами, 5,6% — банковскими вредоносными ПО, а 4,5 % — инфостилерами. Самые активные вредоносные ПО в России — банковский троян Trickbot и криптомайнер XMRig.

87% вредоносных файлов было отправлено по электронной почте. Наиболее распространенная уязвимость — удаленное выполнение кода, из-за которой были атакованы 59% компаний.

Ландшафт киберугроз. Двойное вымогательство. Создатели программ-вымогателей разработали новую стратегию. Мошенники не только лишают жертву

доступа к файлам, но и компрометируют ее обнародованием конфиденциальной информации, в случае отказа платить выкуп.

Кибервойны. Социальное дистанцирование осложнило доступ к разведданным традиционными методами. По этой причине участились случаи использования киберорружия в государственных интересах. Одной из целей подобных атак является получение новых сведений о коронавирусе.

Мобильные устройства. Хакеры ищут новые уязвимости мобильных устройств и непрерывно совершенствуют методы атак, чтобы обходить систему безопасности официальных магазинов приложений или компаний. В ходе недавней атаки на систему управления мобильными устройствами крупной международной компании, мошенникам удалось распространить вредоносное ПО на более чем 75% ее устройств.

Облачные технологии. В условиях удаленной работы компании стали активно использовать облачные платформы. Однако размытие периметра повысило риски информационной безопасности. Так, в системе платформы Microsoft Azure впервые были обнаружены уязвимости, которые могли позволить злоумышленникам получить доступ к данным других пользователей.

Киберландшафт в условиях пандемии. Во время пандемии появилось множество новых доменов, связанных с темой коронавируса, для осуществления фишинговых атак. Медицинские учреждения и исследовательские центры стали все чаще подвергаться атакам мошенников, в целях получения выкупа или ценной информации.

«За последние несколько месяцев периметр компаний значительно размылся. Работая удаленно, люди используют домашние сети, облака, а также персональные устройства для работы с конфиденциальными данными. — отметил Василий Дягилев, глава представительства Check Point Software Technologies в России и СНГ. — По этой причине защита компании должна быть построена по принципу «нулевого доверия». Сегодня это единственный эффективный способ обезопасить себя от самых изощренных атак хакеров».

Исследователи Check Point отметили, что пик появлений новых доменов, связанных с коронавирусном, пришелся на конец марта 2020 года, далее эта активность пошла на спад. За последние шесть месяцев мошенники все чаще стали имитировать приложения для видеоконференций, стриминговые сервисы, подделывать денежные переводы и кредиты, а также резюме для устройства на работу.

Однако хакеры продолжают использовать тему коронавируса для своих атак: вредоносные приложения и сайты с информацией о COVID-19, а также рассылки электронных писем, заголовки и содержимое которых касались темы пандемии.

Наиболее активные вредоносные программы в России в сентябре 2020 года. Самым распространенным вредоносным ПО стал модульный троян Emotet, атаковавший 13% организаций в России и в мире.

Emotet (13%) – продвинутый модульный троян. Когда-то Emotet был рядовым банковским трояном, но в последнее время он используется для дальнейшего распространения вредоносных программ и кампаний, а также может рассылать фишинговые письма, содержащие вредоносные вложения или ссылки.

Trickbot (9%) – один из доминирующих банковских троянов, который постоянно дополняется новыми возможностями, функциями и векторами распространения. Trickbot — гибкое и настраиваемое вредоносное ПО, которое может распространяться в рамках многоцелевых кампаний.

RigEK (7%) – Rig содержит эксплойты для Internet Explorer, Flash, Java и Silverlight. Заражение начинается с перенаправления на целевую страницу, содержащую Java-скрипт, который затем ищет уязвимые плагины и внедряет эксплойт.

Pykspa (6%) – червь, который распространяется через сообщения в Skype. Pykspa выгружает личные данные пользователя и взаимодействует с удаленными серверами, используя алгоритмы генерации доменов (DGA).

XMRig (5%) – криптомайнер, программное обеспечение с открытым исходным кодом, впервые обнаруженное в мае 2017 года. Используется для майнинга криптовалюты Monero». ***(Check Point представила отчет о киберугрозах в России // CNews (https://safe.cnews.ru/news/line/2020-11-17_check_point_predstavila_otchet). 17.11.2020).***

***

«Полномочный представитель президента РФ в Южном федеральном округе Владимир Устинов поручил устранить недостатки в сфере информационной безопасности в оккупированных Крыму и Севастополе.

На данный момент состояние технической защиты информации не соответствует требованиям, сообщили в пресс-службе аппарата совета безопасности РФ, пишет ТАСС.

«Управлением Федеральной службы по техническому и экспортному контролю по Южному и Северо-Кавказскому федеральным округам проведена проверка соблюдения требований нормативных правовых актов РФ в Республике Крым. Сделан вывод, что состояние технической защиты информации не в полной мере соответствует обязательным требованиям. <…> Необходимо срочно устранить недостатки не только в сфере технической защиты информации, но и по всем иным направлениям», - привела пресс-служба слова Устинова.

Проверка выявила низкий уровень обеспечения безопасности персональных данных при их обработке в информационных системах. Также полпред потребовал существенно повысить уровень технической оснащенности систем безопасности информации.

Ранее сообщалось, что секретарь Совета безопасности (СБ) РФ Николай Патрушев отметил значительный рост числа киберпреступлений в стране». ***(Оккупанты обеспокоены состоянием кибербезопасности в Крыму и Севастополе // Чорноморські новини (https://www.blackseanews.net/read/171005). 26.11.2020).***

***

«…Правительство Канады приняло закон, ужесточающий ответственность за нарушение прав граждан в киберпространстве. Теперь компаниям в случае неправильного обращения с персональными данными грозят штрафы в размере до 5% годового дохода или до 25 миллионов канадских долларов (19 миллионов американских долларов).

Закон также предоставляет интернет-пользователям больше контроля над использованием компаниями их данных и даёт гражданам право требовать уничтожения персональной информации о них.

«Поскольку канадцы всё больше полагаются на технологии, нам нужна система, которая позволяет знать, как используются наши данные, и даёт контроль над тем, как они обрабатываются. Для того чтобы Канада добилась успеха, а наши компании могли внедрять инновации, необходима система, основанная на доверии, с прозрачными правилами и правоприменением», — заявил министр инноваций Навдип Бейнс.

На сегодняшний Канада, как отметили в правительстве, ввела в области кибербезопасности самые суровые штрафы из стран «Большой семёрки» (международный клуб, объединяющий Канаду, США, Великобританию, Германию, Францию, Италию и Японию)». ***(Kait Bolongaro. Trudeau Privacy Law to Level Stiff Fines for Digital Breaches // Bloomberg (https://www.bloomberg.com/news/articles/2020-11-17/trudeau-privacy-law-to-level-stiff-fines-for-digital-breaches). 17.11.2020).***

***

«Канадский центр кибербезопасности (Киберцентр) опубликовал свою Национальную оценку киберугроз за 2020 год.

Этот публичный отчет, основанный как на секретных, так и на несекретных источниках, определяет текущие тенденции в среде киберугроз, вероятность возникновения этих киберугроз и то, как это может повлиять на канадцев.

Вторая итерация нашей несекретной оценки отмечает, что количество субъектов киберугроз растет, и они становятся все более изощренными, что киберпреступность почти наверняка будет оставаться той киберугрозой, которая с наибольшей вероятностью затронет канадцев, и что атаки программ-вымогателей почти наверняка продолжатся нацелены на крупные предприятия и поставщиков критически важной инфраструктуры.

Мы оценили, что спонсируемые государством субъекты почти наверняка продолжат попытки украсть канадскую интеллектуальную собственность и конфиденциальную информацию, особенно связанную с COVID-19.

Кроме того, в оценке уточняется, что участники, скорее всего, работают над развитием кибервозможностей, чтобы нарушить канадскую инфраструктуру, такую как электроснабжение, для достижения своих целей. Однако мы считаем, что в отсутствие международных боевых действий маловероятно, что спонсируемые государством субъекты намеренно нарушили бы критическую инфраструктуру Канады.

Котировки

«Кибербезопасность никогда не была так важна, поскольку все больше и больше нашей деловой и личной деятельности перемещается в онлайн. Как показывает этот отчет Канадского центра кибербезопасности, киберугрозы становятся все более изощренными и масштабными. политики, лидеры бизнеса и отдельные канадцы повышают свою онлайн-безопасность в условиях меняющегося ландшафта киберугроз».

- Достопочтенный Харджит Саджан, министр национальной обороны

«От киберпреступников, хранящих нашу личную информацию для выкупа, до спонсируемых государством субъектов, угрожающих нашей критически важной инфраструктуре, - киберугрозы, с которыми сталкиваются канадцы, становятся все более изощренными и серьезными. Вот почему подход Cyber Centre к обеспечению безопасности через сотрудничество важен как никогда. Выводы, сделанные в этом отчете, показывают, почему мы должны продолжать тесно сотрудничать с нашими союзниками и нашими партнерами в правительстве и промышленности, чтобы повысить киберустойчивость Канады».

- Скотт Джонс, руководитель Канадского центра кибербезопасности…» ***(Canadian Centre for Cyber Security Releases the Canadian National Cyber Threat Assessment 2020 // Canadian Centre for Cyber Security (https://cyber.gc.ca/en/news/canadian-centre-cyber-security-releases-canadian-national-cyber-threat-assessment-2020). 18.11.2020).***

«ЦРУ и немецкая разведка подорвали репутацию Швейцарии как исторически нейтрального государства, десятилетиями используя одну из ее компаний в качестве платформы для шпионских операций по всему миру. Об этом сообщается в новом отчете членов швейцарского парламента…

Проводившие расследование специалисты заключили, что правительство Швейцарии не только знало, но и участвовало (хотя и опосредованно) в шпионских операциях, проводимых швейцарской компанией Crypto AG.

Как ранее сообщал SecurityLab, в течение пятидесяти лет компанией тайно владело ЦРУ США. Совместно с федеральной разведслужбой ФРГ (Bundesnachrichtendienst, BND) ЦРУ на протяжении десятилетий перехватывало секретные сообщения официальных лиц по всему миру с помощью Crypto AG, продававшей уязвимые системы шифрования иностранным правительствам. Согласно отчету, с 1993 года спецслужбам Швейцарии было известно, что компания принадлежит ЦРУ и что управление эксплуатирует уязвимости в системах шифрования.

Опубликованный на этой неделе отчет швейцарского правительства является кульминацией расследования, инициированного швейцарскими властями в феврале нынешнего года, когда в СМИ появилась информация о шпионской деятельности Crypto AG. Расследование стало первым публичным отчетом иностранного правительства о шпионской операции ЦРУ, настолько успешной и масштабной, что в секретной истории управления она была названа «разведывательным захватом власти века». ЦРУ не ответило на запрос The Washington Post, а BND отказалась от комментариев.

Базирующаяся в швейцарском городе Цуг компания Crypto AG являлась одним из крупнейших в мире поставщиков систем шифрования, использовавшихся иностранными правительствами для защиты коммуникаций своих разведчиков, военнослужащих и дипломатов. Однако с 1970 года компанией владело ЦРУ и более того, с начала 1950-х годов она активно сотрудничала с Агентством национальной безопасности США. За это время компания продала уязвимые системы шифрования более 120 правительствам, в том числе Ирану, странам Южной Америки, Индии, Пакистану и даже Ватикану.

С помощью уязвимостей в шифровании американские и немецкие спецслужбы читали дипломатическую переписку не только своих противников, но и некоторых союзников. Операция получила название «Рубикон». Согласно полученной The Washington Post секретной истории ЦРУ, «иностранные правительства платили США и Западной Германии большие деньги за то, чтобы их самые секретные коммуникации читали как минимум два (а то и пять-шесть) иностранных государства». Скорее всего, полученными с устройств Crypto AG данными ЦРУ обменивалось со спецслужбами Великобритании.

Связь Crypto AG с ЦРУ мастерски скрывалась с помощью запутанных финансовых транзакций, которыми руководила юридическая фирма в Лихтенштейне. Согласно отчету, позволяя ЦРУ проводить операции с участием компании, правительство Швейцарии не нарушило законодательство своей страны. Однако, подобная тактика может причинить большой ущерб ее политической репутации, отметили авторы отчета». ***(Спецслужбы Швейцарии почти 30 лет знали о связи Crypto AG с ЦРУ // SecurityLab.ru (https://www.securitylab.ru/news/514053.php). 13.11.2020).***

***

Протидія зовнішній кібернетичній агресії

«США устроили хакерскую атаку на Россию с целью не допустить ее вмешательства в выборы главы государства. Аналогичные меры были предприняты и против Ирана. Российские власти неоднократно заявляли, что не влияют на демократические процессы в других странах. Кроме того, нет ни одного доказательства участия российских хакеров во взломе системы голосования США.

Лучшая защита – нападение

США провели «превентивные» кибератаки на Россию и Иран в стремлении помешать этим странам вмешаться в выборы Президента США. По данным телеканала NBC News, атаки были проведены в рамках наступательной операции против иранских и российских «киберструктур».

Телеканал, не раскрывая свои источники и детали кибероперации, заявил, что предпринятые американскими властями меры возымели действие. В результате атак на Россию и США и виртуальном пространстве. В сообщении говорится, что «было очень тихо», и что кибератак, направленных на вмешательство в президентские выборы, «было очень мало».

Власти США не подтвердили и не опровергли информацию о превентивных кибератаках против российских и иранских хакеров. Между тем, в основной день голосования (3 ноября 2020 г.) глава Министерства внутренней безопасности США Чак Вулф (Chuck Wolfe) отметил, что его ведомство не фиксировало попыток взлома.

Слова Вулфа подтвердил и глава Агентства по кибербезопасности и инфраструктурной безопасности США (CISA) Кристофер Кребс (Christopher Krebs). Он добавил также, что в на этот раз Штаты подготовились к выборам более тщательно, чем в 2016 г.

Новые президентские выборы

В борьбе за пост Президента США ведут действующий президент, республиканец Дональд Трамп (Donald Trump) и демократ Джозеф Байден (Joseph Biden). На момент публикации материала голосование было завершено, проводился подсчет голосов. В лидерах был Джозеф Байден – он набрал пока 264 голоса выборщиков, тогда как у Трампа было лишь 214. Для победы на выборах необходимо набрать 270 голосов выборщиков.

В случае победы Трампа это будет его второй срок – на выборах в 2016 г. он победил в борьбе за пост Президента, обойдя своего главного конкурента – Хиллари Клинтон (Hillary Clinton). Это жена экс-президента США Билла Клинтона (Bill Clinton).

Россия не взламывает американские выборы

Российские власти регулярно опровергают обвинения в попытках тем или иным способом повлиять на выборы в других странах. Глава МИД России Сергей Лавров прямо заявил, что нет ни одного факта, указывающего на вмешательства России в выборы в иностранных государствах.

Аналогичного мнения придерживается и пресс-секретарь Президента России Дмитрий Песков. По его словам, обвинения России в подобных деяниях «абсолютно голословны».

Тем временем, в начале сентября 2020 г. за два месяца до проведения в США президентских выборов на одном из российских хакерских форумов появились сообщения с раздачей баз данных об американских избирателях их ряда штатов, включая Мичиган и Коннектикут. Как сообщал CNews, эти базы содержали от 2 до почти 8 млн строк, и информация в них очень детализирована.

Информация в этих БД оказалась подлинной – она актуальна на март 2020 г. Ряд экспертов увидели в этой утечке подготовку к обвинению русских хакеров во вмешательстве в президентские выборы.

США подозревают Россию во вмешательстве в президентские выборы 2016 г., но у них пока нет прямых доказательств этого. Также Штаты в октябре 2020 г. обвинили Россию в кибератаке на Олимпийские игры в Корее, прошедшие в 2018 г.

Минюст США предъявило обвинение шести россиянам, попутно заявив, что они же «работали» и во время президентских выборов во Франции в 2017 г. Также их подозревают в кибератаках с использованием вируса NotPetya.

Шестеро обвиненных россиян – это Юрий Андриенко, Сергей Детистов, Павел Фролов, Анатолий Ковалев, Артем Очиченко и Петр Плискин. Американский Минюст утверждает, что все они – сотрудники российской

разведки». ***(Эльяс Касми. Хакеры США атаковали Россию, чтобы она не вмешивалась в президентские выборы // CNews (https://safe.cnews.ru/news/top/2020-11-05_hakery_ssha_atakovali_rossiyu). 05.11.2020).***

***

«Власти Ирана признали факт кибератаки на два госучреждения, отметив, что их ИТ-системы пришлось в профилактических целях отключить. Это далеко не первый подобный эпизод.

Существенные атаки в Иране

Иран объявил о том, что два государственных учреждения страны подверглись кибератакам. Их ИТ-системы пришлось отключить в порядке профилактики, что, вероятнее всего, указывает на использование хакеров шифровальщика-вымогателя.

Атаки названы «существенными»; власти страны ведут расследование случившегося. Кто мог стоять за атаками, государственные СМИ не сообщают.

Это далеко не первый случай, когда Иран объявляет о кибератаках на свою инфраструктуру. Так, в декабре 2019 г. министр телекоммуникаций страны Мухаммед Джавад Азари Джахроми (Mohammad Javad Azari Jahromi) дважды за одну неделю объявлял об отражении кибератак на инфраструктуру Ирана с помощью «национального цифрового щита». При этом в организации нападения Джахроми обвинил китайскую группировку APT27.

«Подобные атаки — лишь один из множества эпизодов холодной кибервойны всех со всеми, где в целом нет уже ни правых, ни виноватых, — полагает Анастасия Мельникова, эксперт по информационной безопасности компании SEC Consult Services. — Не приходится ожидать, что она в ближайшее время закончится, но так или иначе возможность любых кибератак обеспечивается либо программными уязвимостями, либо недостаточной подготовленностью жертв фишинга к противодействию. Нынешний инцидент, судя по всему, не исключение».

Перманентное обострение

Инцидент был достаточно неожиданным, учитывая, что в большей части случаев Иран обвиняет в попытках кибератак США. После возобновления санкций против Ирана со стороны США в 2018 г. отношения между странами в очередной раз обострились. США в 2019 г. обвиняли Иран в атаках на нефтяные танкеры и уничтожении беспилотника, а власти Ирана объявили, что «опасаются» кибератак со стороны США.

В январе 2020 г. американский беспилотник был использован для убийства в Багдаде иранского генерала Касима Сулеймани (Qasem Soleimani), приказ на ликвидацию которого отдал президент США Дональд Трамп. По утверждению последнего, Сулеймани готовил серию атак на американских военнослужащих в Ираке.

Также в январе Министерство внутренней безопасности США выпустило бюллетень, в котором утверждалось, что связанные с Ираном кибергруппировки готовятся нанести удар по инфраструктуре США.

Кто первый начал

Иран формально является первой в истории страной, ставшей жертвой применения кибероружия: в 2011 г. червь Stuxnet был использован для нанесения физического ущерба заводу по обогащению урана в Натанце. По мнению разведок США и Израиля, назначение завода было сугубо военным, хотя Иран это отрицал. Ущерб от Stuxnet оказался намного меньшим, чем ожидали его разработчики, кроме того, вопреки первоначальным планам, он распространился далеко за пределы инфраструктуры целевого предприятия и в итоге был перехвачен в Белоруссии.

В вышедшем в 2016 г. документальном фильме ZeroDays («Нулевые дни») утверждалось, что Stuxnet был лишь одной из составляющих более масштабной программы, предполагавшей вывод из строя военной и гражданской инфраструктуры Ирана в случае военного нападения на Израиль или других союзников США.

Вскоре после обнаружения Stuxnet, все государства с развитой цифровой инфраструктурой поспешно обзавелись наступательными средствами для противостояния в киберпространстве.

В 2015 г. «Лаборатория Касперского» объявила об обнаружении вредоносного ПО APT-группировки Equation, действовавшей, по меньшей мере, с 2001 г. (домены для некоторых командных серверов были зарегистрированы и вовсе в 1996 г.). В исследовании «Лаборатории» указывалось, что Equation взаимодействовала с операторами вредоносов Flame и разработчиками Stuxnet «каждый раз с позиции превосходства».

Equation и все-все-все

В дальнейшем Equation проассоциировали с Агентством национальной безопасности; в 2016 г. неизвестная группировка ShadowBrokers организовала «слив» значительной части инструментария, использовавшегося Equation. Названия некоторых инструментов оказались исследователям знакомыми: они фигурировали в документах, в 2013 г. опубликованных Эдвардом Сноуденом (Edward Snowden).

Слив ShadowBrokers имел катастрофические последствия: мировая эпидемия шифровальщика WannaCry и множественные атаки с помощью шифровальщика-вайпера NotPetya стали в принципе возможны благодаря использованию эксплойтов Equation, в первую очередь, EternalBlue. Некоторые другие эксплойты из этой группы также впоследствии использовались для совершения сугубо криминальных или кибершпионских атак.

В свою очередь, Ирану также приписываются многочисленные кибератаки на инфраструктуру и коммерческие компании других стран. В частности, печально знаменитый вайпер Shamoon, нанесший в 2012 г. ущерб нефтяной компании SaudiAramco, считается детищем кибершпионской группировки APT33, связанной с властями Ирана». ***(Роман Георгиев. Госорганы Ирана атакованы шифровальщиком-вымогателем // CNews (https://safe.cnews.ru/news/top/2020-10-19_gosorgany_irana_atakovany). 06.11.2020).***

***

«Канадское агентство по киберзащите заявляет, что враждующие государства, скорее всего, разрабатывают способы нарушить работу энергосистем страны.

В опубликованном в среду отчете Службы безопасности связи (CSE) говорится, что другие страны вряд ли намеренно нарушат критически важную инфраструктуру Канады, такую как электрические сети, в отсутствие прямых боевых действий.

Но шпионское агентство заявило, что враждебные страны постоянно исследуют критически важные инфраструктурные сети, чтобы «подготовить» себя к будущим атакам или в качестве формы устрашения.

«Мы полагаем, что спонсируемые государством субъекты, скорее всего, пытаются разработать дополнительные киберпотенциалы, необходимые для прекращения подачи электроэнергии в Канаду», - говорится в оценке угроз агентства к 2020 году.

CSE не привязывал эту деятельность к конкретным странам. Но в другом месте отчета Китай, Россия, Иран и Северная Корея называются «величайшими стратегическими угрозами» кибербезопасности Канады.

«В 2019 году связанные с Россией субъекты зондировали сети электроэнергетических компаний США и Канады. Иранские хакерские группы нацелены на (системы управления производством) в конкурирующих странах… Северокорейское вредоносное ПО было обнаружено в ИТ-сетях индийских электростанций, а работники коммунальных служб США стали жертвами киберугроз, спонсируемых Китаем», - сообщает агентство. цитируя публично опубликованные примеры.

Скотт Джонс, глава канадского центра кибербезопасности CSE, сказал, что объединенная электрическая инфраструктура Северной Америки является «одной из крупнейших машин в мире». Это затрудняет предотвращение отказов даже в результате природных явлений, таких как ледяные бури.

Но по мере того, как все больше и больше «операционных технологий», используемых для управления критически важной инфраструктурой, мигрируют в онлайн, это открывает возможности для кибератак.

«Это угроза, и мы наблюдаем активность в наших секторах в Канаде и США», - сказал Джонс репортерам во время телефонной конференции в среду.

«И на самом деле это активность, о которой мы довольно рано сообщили нашему электрическому сектору по всей Канаде, как только мы ее обнаружили».

Как и в ходе своей первой общественной оценки угроз в 2018 году, агентство пришло к выводу, что отдельные канадцы с гораздо большей вероятностью станут мишенью для киберпреступников более низкого уровня, чем для действий, спонсируемых государством.

В нем говорится, что они почти наверняка продолжат подвергаться мошенничеству по электронной почте и атакам программ-вымогателей, когда хакеры блокируют доступ человека или организации к их устройству или сети и требуют оплаты за расшифровку файлов в течение следующих двух лет.

Но в отчете агентства отмечается, что поддерживаемая государством кибернетическая деятельность является более сложной и может нанести больший

ущерб государственным и частным организациям, и предполагается, что характер этой деятельности меняется.

CSE, наряду с другими разведывательными и правительственными ведомствами, было поручено охранять федеральные выборы 2019 года от иностранного вмешательства по аналогии с поддерживаемой Россией деятельностью, наблюдаемой на президентских выборах в США в 2016 году.

В отчете в среду говорится, что иностранное вмешательство и кампании влияния являются «новой нормой» и будут сохраняться даже за пределами периода выборов, чтобы попытаться сформировать мнение Канады по ключевым вопросам.

«По нашим оценкам, по сравнению с некоторыми другими странами, канадцы являются менее приоритетными целями для онлайн-влияния», - говорится в отчете.

«Тем не менее, медиаэкосистема Канады тесно связана с экосистемой Соединенных Штатов и других союзников, а это означает, что, когда их население становится мишенью, канадцы становятся уязвимыми для онлайн-влияния в качестве побочного ущерба». ***(Alex Boutilier. Cyber defence agency says hostile states are developing ways to disrupt Canada's power grid // Toronto Star Newspapers Ltd (https://www.thestar.com/politics/federal/2020/11/18/cyber-defence-agency-says-hostile-states-are-developing-ways-to-disrupt-canadas-power-grid.html). 18.11.2020).***

***

«Эстонское представительство NATO проводит ряд экспериментов с применением обманной тактики, якобы позволяющей привлечь внимание российских хакеров.

Североатлантический альянс решил потренироваться в отражении атак пресловутых российских хакеров и устроил учения по кибербезопасности, в ходе которых военные хакеры NATO протестируют специально разработанную обманную тактику. По их замыслу, «молодые киберофицеры» российской армии, которые ищут способы проникновения в защищенные сети государств-участников NATO, должны попасть в ловушку.

После того, как российские хакеры определят человека, чьи учётные данные можно украсть для кибератаки, они попытаются отправить ему фишинговое письмо, считают в NATO. «Жертва» выполнит все необходимые действия, но в результате российские офицеры узнают, что «украденная» информация является бессмысленной. Более того, тем самым они раскроют свои собственные методы или инструменты, уверены натовцы.

В NATO считают, что при помощи данной тактики аналитики по кибербезопасности получат полную информацию о российских хакерах. На чём основана такая уверенность, остаётся загадкой. Некоторое время назад российских хакеров обвинили в срыве Олимпиады-2020: в Microsoft заявили, что связанная с российским правительством группа хакеров атаковала как минимум 16 национальных и международных спортивных и антидопинговых организаций…». ***(Александр Пономарёв. NATO потренируется обманывать российских хакеров // ООО «Фэшн Пресс» (https://www.popmech.ru/technologies/news-645683-nato-potreniruetsya-obmanyvat-rossiyskih-hakerov/). 23.11.2020).***

***

«Специалисты по анализу киберугроз (CTI) могут получить представление о действиях противника, отслеживая конфликты или геополитическую напряженность. Подобно подходу «следования за деньгами» в уголовных расследованиях, изучение зон конфликта может выявить кибер-возможности, развернутые как часть событий - либо сторонами конфликта, либо третьими сторонами, заинтересованными в мониторинге событий для своих собственных целей.

Вышеупомянутая теория подтверждается историческими инцидентами, связанными с геополитической напряженностью:

Вторжение России на территорию Украины привело, среди прочего, к инцидентам с подачей электроэнергии на Украине в 2015 и 2016 годах, событию NotPetya в 2017 году и продолжающимся операциям по настоящее время.

Напряженность в Аравийском / регионе Персидского залива, ведущие к нескольким раундам из стеклоочистителей вредоносных программ, а также обеспечивая возможную «крышку» для 2017 Triton / TRISIS инцидента.

Продолжающаяся напряженность на Корейском полуострове, обеспечивающая прикрытие для разрушительного нападения на Олимпийские игры в Пхенчхане в 2018 году (даже если нападавшим в этом случае была не Северная Корея).

Основываясь на прецеденте, аналитики могут определять развитие действий противника и технических возможностей, отслеживая идентификаторы, связанные с крупными событиями и зонами конфликтов. Определение возможностей, развернутых для использования таких элементов, может дать представление об основных методах и поведении злоумышленников, а также обеспечить защиту и реагирование на инциденты, которые могут ударить гораздо ближе к дому в более поздний период.

Первоначальное открытие: Кавказский конфликт

Принимая во внимание вышеуказанный тезис, исследователи DomainTools изучили технические артефакты, возникшие в связи с конфликтом 2020 года между Арменией и Азербайджаном в Кавказском регионе. В ходе расследования исследователи обнаружили следующий вредоносный файл документа в коммерческом сервисе с несколькими сканерами…

Под видом новостной статьи, освещающей детали конфликта на Кавказе, документ содержит ссылку на внешний сайт для загрузки дополнительных материалов на компьютер жертвы…

В этом конкретном случае документ пытается связаться с доменом «msofficeupdate [.] Org»…

В целом документ, похоже, сосредоточен на армяно-азербайджанском конфликте с выделенной сетевой инфраструктурой, обеспечивающей последовательность атак. Хотя мы могли остановиться и рассмотреть этот элемент отдельно, дальнейший анализ обнаруживает еще более интересные элементы.

Определение элементов для поворота

И документ, и домен содержат элементы, представляющие интерес для дальнейшего анализа и просмотра. Просматривая уроки из предыдущего блога DomainTools, мы можем изучить технические индикаторы, связанные с этой кампанией, как составные объекты с возможностью распознавать фундаментальное поведение противника.

Изучая документ, метаданные файла, показанные здесь с помощью ExifTool Фила Харви, указывают на наличие необычно длинной строки чисел в качестве объекта шаблона...

На основе объекта шаблона и жестко запрограммированного унифицированного указателя ресурса (URL) документ попытается связаться с доменом, указанным выше. Фактическая функциональность вредоносного документа зависит от сетевого взаимодействия с доменом злоумышленника с HTTP-запросом к ресурсу...

Все следующие функции зависят от ответа на этот запрос. В настоящее время DomainTools не имеет данных или другой информации о том, что может быть возвращено из этого ответа. В результате наш анализ ограничивается самим документом и идентифицированной сетевой инфраструктурой. Однако защитники могут найти значение в шаблоне URL-адреса в HTTP-запросе - словах, разделенных на отдельные числа - для разработки сигнатур системы обнаружения сетевых вторжений (NIDS).

Если не считать отсутствия представления о последующем выполнении, у нас есть строка поиска, которую можно использовать для отпечатков дополнительных образцов файлов или для размещения элементов, которые могут быть связаны с исходной кампанией в строке шаблона. В частности, для вредоносного документа элемент не содержит активного содержимого (объекты ActiveX или макросы Visual Basic для приложений [VBA]), что ограничивает нашу способность идентифицировать дополнительные элементы. Однако элемент шаблона выглядит достаточно уникальным, чтобы служить указателем для идентификации дополнительных образцов, построенных аналогичным образом.

Что касается инфраструктуры, у нас есть еще несколько потенциальных клиентов. Как ранее было описано в прошлых блогах по поиску и анализу инфраструктуры, у нас есть комбинация технических индикаторов, связанных с созданием домена и хостингом, а также тематических идентификаторов, связанных с самим доменным именем. Для рассматриваемого домена, как видно на предыдущем контрольном изображении DomainTools Iris выше, справедливы следующие наблюдения:

Утечка адреса электронной почты регистранта: «gjdodson [AT] protonmail [.] Com».

Служба регистрации доменов «PDR Ltd. d / b / a PublicDomainRegistry.com».

Авторитетный сервер имен, связанный с доменом «bitdomain [.] Biz».

Хостинг на выделенном сервере «46.30.188 [.] 236» через нидерландского провайдера «Web2objects Gmbh».

Сертификат SSL / TLS, полученный через Sectigo, с ограниченной идентифицирующей информацией.

Доменная «тема» имитации служб обновления Microsoft Office.

Хотя любой из вышеперечисленных элементов по отдельности может быть относительно ограничен для выявления тенденций противодействия или дополнительной инфраструктуры - либо будучи слишком общим, либо слишком конкретным - в сочетании, они могут дать шаблоны для дальнейшего анализа. Например, поиск комбинации ориентированных на конфиденциальность адресов электронной почты, регистрирующих домены через PublicDomainRegistry с использованием сервера имен bitdomain [.] Biz, размещенного в Европе с сертификатами Sectigo SSL / TLS, может дать набор результатов для дальнейшего анализа. Применение «тематического» поиска к результатам такого расследования, например поиск других тем Microsoft или Office в доменных именах, может выявить дополнительные элементы для анализа, связанные с этой кампанией.

Раскрытие дополнительной инфраструктуры

Основываясь на характеристиках, описанных в предыдущем разделе, исследователи DomainTools идентифицировали 35 доменов, соответствующих шаблонам, связанным с изначально наблюдаемым вредоносным доменом, с различными уровнями оценочной вероятности или уверенности. Как показано в следующей таблице, мы можем наблюдать дополнительные тенденции, такие как предпочтение нескольких сервисов электронной почты, ориентированных на конфиденциальность, во время регистрации и подавляющее внимание провайдеров европейских виртуальных частных серверов (VPS) для целей хостинга…

Хотя большинство элементов было создано в 2020 году, некоторые потенциально связанные сетевые наблюдаемые датируются еще 2016 годом. При сравнении с образцами вредоносных документов, рассмотренных в следующем разделе, мы начинаем видеть контуры постоянной, довольно продолжительной кампании. Несмотря на то, что они растянуты во времени, то же самое фундаментальное поведение сети отражается в наблюдаемых элементах в течение этого периода.

Визуально, например, в визуализации DomainTools Iris ниже, мы видим кластеры активности, разделенные между серверами имен, регистраторами и доменами верхнего уровня (TLD). С еще большей численностью населения мы могли бы начать выделять еще больше аспектов методов работы этого противника и потенциально разрабатывать алгоритмы прогнозирования для создания будущей инфраструктуры.

Поиск дополнительных образцов

В дополнение к выявлению дополнительной сетевой инфраструктуры, комбинация просмотра исходного документа и перехода от наблюдаемой сетевой инфраструктуры дает дополнительные образцы вредоносных документов. Прежде всего, уникальная строка чисел в шаблоне в сочетании с отношениями к доменам и темам документов позволяет обнаруживать дополнительные элементы. Как показано в следующей таблице, эти элементы связаны как через уникальную строку шаблона, так и через инфраструктуру связи, связанную с анализом, представленным выше для сетевых наблюдаемых…

Как более подробно описано в следующем разделе, эти материалы в основном посвящены темам, связанным с конфликтом на Кавказе или продолжающимся конфликтом на Украине. Кроме того, они продлятся с декабря

2019 года по ноябрь 2020 года, что означает, что эта деятельность продолжается без значительных изменений почти год.

В дополнение к этим элементам исследователи DomainTools также определили второй набор документов, все из Франции, с темой «тестирования», но соответствующие различным характеристикам вышеуказанных элементов, таким как уникальная строка шаблона..

Вышеуказанные элементы выделяются среди других документов по нескольким причинам:

Все они были отправлены в один и тот же сервис мультисканера в один и тот же день.

Элементы кажутся итеративными с учетом схемы именования файлов (testmw2, testmw3 и т. Д.).

Анализ файлов указывает на фаззинг или изменение возможностей среди них в соответствии с итеративным характером имен файлов.

Первоначальный вывод будет заключаться в том, что это «тестирование» вредоносного формата документа или шаблона, которые появятся в более поздних кампаниях. Однако время для этого вывода еще не пришло, поскольку «тестовые» элементы появляются в середине сентября, когда элементы, использующие один и тот же шаблон (функциональный и приманочный документ), впервые появляются в декабре 2019 года.

В целом, эта партия предметов остается загадкой, поскольку нет явных признаков, связывающих ее с другими кампаниями. Кроме того, некоторые из рассматриваемых элементов не работают или в них отсутствуют другие компоненты, связанные с действием в первом наборе документов, связанных с вероятной постоянной кампанией. В настоящее время DomainTools не обладает какой-либо дополнительной информацией для удаления этих элементов, поэтому они остаются в некоторой степени загадкой по сравнению с другими вредоносными документами, которые, как представляется, более явно предназначены для целей шпионажа.

Мотивы и атрибуция

Выявленные документы поступают из разных мест, но в основном касаются Азербайджана и Украины.

Еще более интересны темы, связанные с документами в их тексте и заголовках. В дополнение к документу, положившему начало этому расследованию, и его темам, сосредоточенным на недавнем конфликте на Кавказе, были определены следующие темы:

Ч.Байрамов.doc: ссылки на министра иностранных дел Азербайджана Джейхуна Байрамова.

Фадеев M1.doc: представляет собой рекламную кампанию по сбору средств для режиссера-документалиста, освещающего события в Донецкой области Украины, зоне конфликта.

О поставке зенитных ракетных систем С-400.doc: маскируется под репортаж о системе ПВО С-400, произведенной в России и проданной во многие страны.

Планируемые расходы на 2020 год (1) .doc: «Запланированные расходы на 2020 год», документ, который, по всей видимости, показывает расходы на персонал местного органа власти в Украине.

Стратегический обзор обороны и безопасности (2021 SDSR) .doc: документ стратегического оборонного планирования, предназначенный для министерства обороны Словении. Примечательно, что этот документ связан с фишинговым письмом, отправленным человеку, который, по всей видимости, является военным атташе Словении при посольстве страны в Российской Федерации.

Справочник АП_26.10.2020_.doc: плановый документ поддерживаемой Россией, но непризнанной сепаратистской Донецкой Народной Республики.

Новые поправки к Госпрограмме переселения в РФ (вст. В силу 01.07.2020) .doc: документ о внутреннем переселении в пределах Российской Федерации.

Минтруд госслужба.doc: документ из поддерживаемой Россией, но непризнанной самопровозглашенной Луганской Народной Республики.

В целом, документы связаны с политическими, военными и связанными с ними темами в основном в зонах конфликтов, таких как Кавказ и поддерживаемые Россией сепаратистские регионы востока Украины. Дополнительные элементы, такие как словенский защитный документ, который исследователи DomainTools смогли связать с фишинговым электронным письмом, явно подразумевают спонсируемые государством интересы в шпионаже или в аналогичных целях в качестве мотивации этой кампании.

В октябре 2020 года несколько исследователей заметили некоторые документы, указанные в этом отчете, и связали их с группой, называемой в публичных отчетах «Облачный атлас» или «Начало». Хотя имеющиеся в настоящее время данные не полностью соответствуют предыдущей деятельности Cloud Atlas, наблюдаются следующие общие черты:

Ориентация на регионы ближнего зарубежья России.

Использование шаблонных объектов для первоначальной активности через вредоносные документы.

Скорее всего, полагаться на сетевое взаимодействие для получения инструментов второго этапа для последующей деятельности.

Ответ на HTTP-запросы, отправленные документами, предположительно будет ключом для согласования вышеуказанных кампаний с субъектом Cloud Atlas, но при отсутствии этого доказательства DomainTools не может ни подтвердить, ни опровергнуть связь с этой группой в настоящее время.

Независимо от конкретной атрибуции, возможные связи с известным субъектом Advanced Persistent Threat (APT) (Cloud Atlas) в сочетании с темами кампании, которые носят весьма политический характер без очевидного механизма монетизации, делают обнаруженную кампанию, вероятно, спонсируемой государством или управляемой государством. шпионская кампания. Хотя таргетинг в этом случае может подразумевать интересы, связанные с Россией, важно отметить, что ранее деятельность Cloud Atlas также была нацелена на организации в Российской Федерации. Одна из возможных альтернативных гипотез, учитывая нацеленность в России, а также акцент на сепаратистские регионы на Украине, заключается в том, что эта деятельность представляет собой кибершпионаж,

спонсируемый Украиной. Хотя это интересно, в настоящее время опять же недостаточно доказательств, чтобы поддержать эту гипотезу.

Хотя описанная выше деятельность, безусловно, вызывает беспокойство, доступная информация на данный момент не поддерживает даже слабую атрибуцию какого-либо государственного интереса, имея только правдоподобные (но еще не доказанные) ссылки на объект Cloud Atlas. Хотя конкретная атрибуция может быть невозможной, мы, тем не менее, можем с большой уверенностью заключить, что эта деятельность представляет собой кибершпионаж, направляемый некоторым, пока неизвестным государственным субъектом.

Вывод

Отслеживание тем, связанных с геополитическими событиями, может быть весьма плодотворным для выявления активных кампаний, вероятно, связанных с интересами, спонсируемыми государством. В приведенном выше примере поиск предметов, связанных с армяно-азербайджанским конфликтом на Кавказе в конце 2020 года, дал вредоносный документ. Дальнейший анализ этого документа и связанной с ним инфраструктуры привел к обнаружению дополнительных элементов, описывающих всю кампанию, начиная с 2019 года.

Хотя жертвы этой кампании кажутся географически ограниченными, в основном сосредоточенными на Украине и Азербайджане, уроки, извлеченные из анализа как вредоносных документов, так и соответствующей сетевой инфраструктуры, могут быть использованы для дальнейшей защиты от атак аналогичного типа. Наблюдая за этими типами инцидентов, связанных с конкретными событиями, аналитики CTI могут получить представление о возникающих APT-действиях и развернуть защитные контрмеры вскоре после обнаружения.

Чтобы узнать, как выявлять и отслеживать операции злоумышленников в DomainTools Iris, посетите страницу нашего продукта». ***(Joe Slowik. Current Events to Widespread Campaigns: Pivoting from Samples to Identify Activity // DomainTools (https://www.domaintools.com/resources/blog/current-events-to-widespread-campaigns-pivoting-from-samples-to-identify#). 20.11.2020).***

***

Створення та функціонування кібервійськ

«Правительство Великобритании сообщило, что новая наступательная сила, состоящая из шпионов, киберэкспертов и военнослужащих, уже проводит кибероперации по пресечению действий враждебного государства, террористов и преступников.

Новая группа, известная как Национальные киберсилы, нацелена на борьбу с угрозами национальной безопасности Великобритании, такими как противодействие террористическим заговорам, а также поддержка военных операций Великобритании.

Премьер-министр Борис Джонсон сообщил парламенту, что новые силы уже созданы и действуют: «Я могу объявить, что мы создали Национальную киберсилу,

объединив наши спецслужбы и обслуживающий персонал, которые уже действуют в киберпространстве против терроризма, организованной преступности и враждебных сил. государственная деятельность», - сказал он.

SEE: Что такое кибервойна? Все, что вам нужно знать о пугающем будущем цифрового конфликта

Национальные киберсилы объединяют экспертов из разведывательного агентства GCHQ, Министерства обороны, Лаборатории оборонной науки и технологий и Секретной разведывательной службы - МИ-6, - которые поделятся своим «опытом в вербовке и управлении агентов, а также уникальной способностью доставлять секретные сообщения. эксплуатационная технология».

GCHQ заявило, что примеры кибероперацій могут включать вмешательство в работу мобильного телефона, чтобы террорист не мог общаться со своими контактами, помощь в предотвращении использования Интернета в качестве платформы для серьезных преступлений или обеспечение безопасности военных самолетов Великобритании от нападений. системами оружия противника.

NCF отделен от NCSC, другой части GCHQ, которая занимается кибербезопасностью Великобритании.

Директор GCHQ Джереми Флеминг сказал, что Национальные киберсилы «объединяют возможности разведки и обороны, чтобы преобразовать способность Великобритании бороться с противниками в киберпространстве, защищать страну, ее людей и наш образ жизни».

GCHQ заявило, что новые силы основаны на текущей Национальной наступательной киберпрограмме Великобритании, включая сотрудничество между GCHQ и военными для проведения кибероперацій. Национальные киберсилы уже в этом году несколько раз запускали правительство; еще в 2018 году сообщалось, что новое подразделение будет насчитывать 2000 человек и будет иметь бюджет в 250 миллионов фунтов стерлингов.

Великобритания уже использовала кибератаки или «наступательные кибероперации»: в 2016 году правительство заявило, что проводило кибероперации против Даиш, а в 2018 году выяснилось, что Великобритания использовала кибератаки против пропагандистских сетей ИГИЛ. Великобритания также предложила НАТО свои кибер-возможности.

По словам премьер-министра, новость о Национальных киберсилах была частью более широкого объявления об обзоре обороны, направленном на расширение использования технологий вооруженными силами, создание «единой сети» для преодоления врага.

"Солдат на враждебной территории будет предупрежден о далекой засаде с помощью датчиков спутников или беспилотных летательных аппаратов, мгновенно передавая предупреждение, используя искусственный интеллект для разработки оптимального ответа и предлагая множество вариантов, от вызова воздушного удара до приказа о создании роя. - атаковать с помощью дронов или парализовать врага кибероружием», - сказал Джонсон.

Однако такой упор на кибероперации не обходится без критики. Поскольку нет четких правил относительно того, что является надлежащим ответом на кибератаку, есть опасения, что более широкое использование возможностей

наступательной кибервойны может привести к быстрой и трудно поддающейся контролю эскалации во время конфликта, поскольку разные страны могут быть играя по разным правилам.

И хотя некоторые утверждают, что рекламные кибервозможности могут служить сдерживающим фактором для потенциальных злоумышленников, не все в этом уверены. В своем недавнем выступлении Киаран Мартин, до недавнего времени возглавлявший NCSC, сказал: «Из всего моего опыта работы я не видел абсолютно ничего, что указывало бы на то, что существование западных кибер-возможностей или наша готовность использовать их сдерживает злоумышленников.

«Мы рискуем согласиться с тем, что приобретение и использование высокотехнологичных кибер-возможностей являются приоритетом, не проверяя вопрос о том, что это означает для нашей собственной цифровой среды. У нас не было этих фундаментальных дебатов, потому что сообщество национальной безопасности и технологические общины на самом деле не разговаривают друг с другом», - сказал он». ***(Steve Ranger. The UK's new offensive cyber unit takes on organised crime and hostile states // ZDNet (https://www.zdnet.com/article/new-cyber-force-will-take-the-fight-to-organised-crime-and-hostile-states/). 19.11.2020).***

***

Кіберзахист критичної інфраструктури

«В результате хакерской атаки Комиссия по атомной энергии Японии временно отключила свою электронную почту. Хакеры охотились за данными о безопасности АЭС, но получить их не смогли.

Закрыли форточку

Комиссия по атомной энергии Японии в конце октября 2020 г. была вынуждена временно отключить свои системы электронной почты в связи с кибератакой.

Данная комиссия занимается вопросами безопасности АЭС на территории Японии, но не занимается их прямым управлением, так что кибератака никак не сказалась на деятельности атомных электростанций.

На сайте Комиссии указывается, что это учреждение не имело возможности принимать какие-либо заявки на участие в общественных слушаниях и других мероприятиях по электронной почте.

Японские СМИ указывают, что атаку произвели иностранные киберзлоумышленники, очевидно, пытавшиеся получить какие-либо важные сведения об атомных электростанциях Японии. Заместитель председателя Комиссии Кацуя Окада (KatsuyaOkada), однако, заявил, что ключевая информация о мерах безопасности на ядерных объектах страны хранится в отдельной, изолированной сети, получить доступ к которой извне невозможно.

Иностранная APT?

Ранее власти США выпустили предупреждение о северокорейской APT-группировке, которая зондирует госорганы США, Японии и Южной Кореи в

поисках информации, в том числе связанной с политикой в области атомной энергетики. Возможно, именно эта группировка и стоит за кибератакой.

«Подобные ситуации всегда вызывают повышенную тревогу: любые атаки на объекты, даже косвенно связанные с критической инфраструктурой, несут реальную угрозу жизни и здоровью людей, особенно если речь идет об атомной энергетике, — говорит Алексей Водясов, технический директор компании SECConsultServices. — Хотелось бы верить, что критические сведения действительно остались недоступными для злоумышленников на этот раз, хотя известны случаи, когда им удавалось скомпрометировать и изолированные сети».

Достоверно известен как минимум один подтвержденный случай прямых кибератак на АЭС. Осенью 2019 г. крупнейшая индийская атомная электростанция Куданкулам признала факт взлома своих ИТ-систем. Атака также приписывается северокорейским спецслужбам». ***(Роман Георгиев. Хакеры лишили электронной почты госуправление по ядерной энергетике // CNews (https://www.cnews.ru/news/top/2020-11-09_hakery_lishili_elektronnoj). 09.11.2020).***

***

Захист персональних даних

«Технологии и данные могут расширить возможности всего бизнеса. С другой стороны, они могут создавать риски. По мере роста использования данных все компании сталкиваются с риском утечки данных. Принимая во внимание усиление принудительных мер и принятие большего количества решений в пользу истцов, мы рассматриваем некоторые нормативные и правовые последствия, которые могут последовать за утечкой данных.

Большинство организаций в первую очередь озабочены принудительными мерами регулирования после инцидента, связанного с безопасностью данных. Хотя правоприменительные меры с большей вероятностью порождают гражданские иски, риск продолжения гражданских исков потерпевшими сторонами также реален. Кроме того, истцам не обязательно всегда ждать завершения исполнительных действий, чтобы подать собственный гражданский иск.

Согласно статистическим данным, опубликованным на сайте PDPC, количество жалоб, полученных PDPC, неуклонно растет; В период с октября по декабрь 2018 года было получено 600 жалоб по сравнению с 1700 жалобами в октябре-декабре 2019 года. Увеличение количества жалоб в регулирующие органы указывает на то, что люди с большей вероятностью будут подавать гражданские иски. Следующие факторы также могут способствовать увеличению воздействия на корпорации:

- Повышение осведомленности общественности о правах на данные;
- Повышенные ожидания потребителей, что компании должны поступать «правильно»;
- Повышенная правоприменительная деятельность по всему миру; принудительные действия регулирующего органа в одной юрисдикции могут

побудить регулирующие органы в других юрисдикциях действовать аналогичным образом; а также

- Более широкое внедрение цифровых платформ в ответ на пандемию.

Внутренние регуляторы регулирования все больше внимания уделяют вопросам кибербезопасности и конфиденциальности данных. В то время как местные регулирующие органы, возможно, ранее поощряли (хотя и довольно сильно) определенное поведение, в настоящее время такое поведение закреплено как формализованные требования.

Одним из примечательных примеров является введение режима обязательного уведомления о нарушениях посредством поправок к Закону о защите личных данных («PDPA»). С поправками, организации должны будут уведомлять затронутых лиц и Комиссию по защите личных данных («PDPC»), Когда утечка данных приводит или может привести к значительному ущербу. Хотя сроки уведомления затронутых лиц конкретно не указаны в днях или часах, PDC должен быть уведомлен в течение 3 календарных дней со дня проведения оценки.

Максимальный финансовый штраф по НДПА также будет увеличен. Это будет 10% от годового оборота организации или 1 миллион, в зависимости от того, что больше. В связи с опасениями, что пересмотренный максимальный штраф может быть неоправданно суровым, было указано, что PDPC будет гарантировать, что налагаемые финансовые штрафы будут соразмерны серьезности нарушения.

Ответственность перед частными лицами также может возникать в соответствии с местным законодательством. НДПА прямо предусматривает право иска о возмещении ущерба в рамках гражданского судопроизводства в отношении убытков или ущерба непосредственно в результате нарушения определенных положений НДПА.

Обязательства могут возникать и в соответствии с другими положениями. Например, хотя Закон о кибербезопасности в основном касается организаций, которые владеют или эксплуатируют критическую информационную инфраструктуру («CII»), Закон по-прежнему налагает обязательства на компании, которые не владеют и не управляют CII. Все организации обязаны сотрудничать с Уполномоченным в расследовании угроз и инцидентов кибербезопасности. Это включает в себя необходимость предоставить любую физическую или электронную запись или документ или такие меры по исправлению положения в соответствии с указаниями Уполномоченного.

Международное и экстерриториальное право Законы, имеющие экстерриториальное действие, также могут создавать потенциальную ответственность для корпорации-жертвы.

Растущее количество правил кибербезопасности и конфиденциальности данных во всем мире имеет экстерриториальный характер. Например, Общий регламент по защите данных может применяться к контроллерам данных, которые не имеют представительства в Европе, и при определенных обстоятельствах субъекты данных даже не обязаны проживать в Европе, чтобы иметь право на защиту.

Учитывая, что большинство крупных корпораций, как правило, работают в нескольких странах, инцидент, связанный с кибербезопасностью, может привести к

возникновению нормативных актов, касающихся конфиденциальности данных и кибербезопасности, в нескольких юрисдикциях. Это, в свою очередь, означает, что корпорация-жертва должна бороться с правилами (и регулирующими органами) в нескольких юрисдикциях. Это подчеркивает важность скоординированного подхода.

Прямая ответственность

Как указано выше, PDPA прямо предоставляет право на компенсацию людям, которые понесли ущерб в результате невыполнения организацией своих обязательств в отношении сбора, использования и раскрытия личных данных.

Раскрытие информации в нарушение доверительных отношений также может повлечь за собой ответственность. Как только будет установлено, что рассматриваемая информация имеет необходимое качество доверия и была передана в обстоятельствах, требующих соблюдения конфиденциальности, может возникнуть основание для иска о злоупотреблении доверием. Раскрытие информации не должно быть преднамеренным, чтобы корпорация могла нести ответственность.

Другие причины действий могут быть доступны, если раскрытие информации или утечка произошли в нарушение каких-либо договорных соглашений между скомпрометированной корпорацией и пострадавшей стороной. Примеры включают случаи, когда контрагент понес убытки в результате нарушения договора с клиентом или нарушения трудового договора, требующего обработки данных определенным образом.

Ответственность также может возникать из-за того, как организация и ее старшие должностные лица справляются с инцидентом кибербезопасности или утечкой данных. Обязанность директоров действовать в интересах компании может включать рассмотрение реакции, принятой после инцидента.

На практике часто можно указать несколько причин для иска, поскольку инцидент, связанный с кибербезопасностью, обычно включает в себя разные вещи, происходящие с разными данными.

Коллективные действия

Хотя индивидуальные претензии по поводу утечки данных или неправомерного использования обычно не влекут за собой серьезных убытков, совокупная сумма может быть весьма значительной.

В Соединенном Королевстве было несколько случаев, когда коллективные иски клиентов были разрешены. Отчасти это связано с тем, что истцы решили структурировать свои претензии грамотно.

Последнее решение Сингапура по этому вопросу также указывает на более либеральный подход к таким коллективным действиям, который разрешен в соответствии с правилами гражданского судопроизводства Сингапура в качестве представительного действия. Широкое толкование требования «одинаковой заинтересованности» (необходимого для продолжения представительного действия) было принято в различных юрисдикциях, и Апелляционный суд Сингапура принял такой подход.

Апелляционный суд Сингапура также применил широкий и гибкий подход к управлению представительскими исками и судебной защите, которая может быть предоставлена истцам.

Независимо от того, вынуждают ли они все более жесткое регулирование или угроза гражданской ответственности, корпорации и их высшее руководство столкнутся с более пристальным вниманием и давлением, чтобы усилить управление киберпространством / данными и их устойчивость. Если они этого не сделали, корпорации должны рассматривать этот период как возможность оценить и укрепить свою политику, процессы и структуру, чтобы снизить эти кибер-риски и риски, связанные с данными». ***(Lijun Chui. Singapore: Cyber and Data Breach Exposure // Bird & Bird (https://www.twobirds.com/en/news/articles/2020/singapore/singapore-cyber-and-data-breach-exposure). 10.11.2020).***

***

«В соответствии с международной практикой, проект Закона КНР о защите личной информации («Проект Закона о защите личных данных») содержит исчерпывающий набор индивидуальных прав. В части 3 нашей серии из четырех частей мы рассмотрим некоторые из этих прав и, где это уместно, сравним их с их аналогами в GDPR.

1. Право на получение информации (информационное сообщение)

Законопроект о защите личных данных предусматривает, что определенная информация должна быть предоставлена соответствующему лицу, прежде чем его личная информация может быть обработана. Обязательная информация включает:

- личность обработчика PI и его контактные данные
- цели обработки
- средства, на которых будет обрабатываться личная информация
- типы обрабатываемой личной информации
- срок хранения
- как могут быть реализованы права человека
- Процессор PI также необходим для предоставления дополнительной информации в определенных обстоятельствах:
- если личная информация будет предоставлена третьей стороне, информация в пунктах (a) - (d) выше в той мере, в какой она относится к передаче и третьей стороне-получателю; а также
- если передача необходима из-за слияния, личность и контактные данные получателя.

Для китайских предприятий, которые соблюдают требования, изложенные в Законе КНР о кибербезопасности и обновленном и пересмотренном Национальном стандарте PI по технологиям информационной безопасности - Спецификация безопасности личной информации (последняя версия вступила в силу 1 октября 2020 г., (" PI National Стандарт ")), а также отраслевые правила, их существующие политики конфиденциальности, вероятно, уже включают требуемую информацию. Поэтому здесь нет ничего удивительного.

Тем не менее, существуют определенные заметные различия между проектом закона о защите личных данных и, например, GDPR в отношении требований об уведомлении. Например, правовые основы для обработки личной информации, хотя и изложены в статье 13 проекта закона о защите личных данных, не обязательно должны быть прямо прописаны в политике конфиденциальности (в отличие от GDPR).

Другой пример: проект закона о защите PI требует, чтобы процессор PI явно указывал срок хранения. В отличие от статьи 13 (2) (a) GDPR, которая позволяет контроллеру данных указывать критерии, используемые для определения срока хранения, если невозможно заранее определить срок хранения, в проекте PI нет такого эквивалентного положения. Закон о защите. Как отмечалось в Части 2, проект Закона о защите персональных данных действительно содержит общий принцип защиты данных (статья 20), ограничивающий срок хранения до периода, необходимого для достижения цели, для которой собираются данные. Тем не менее, этот период хранения данных для защиты данных может быть отменен другими (чаще более длительными) установленными законом сроками хранения - это обязательство (или право) прямо сохраняется в проекте закона о защите PI.

2. Право на доступ, исправление и стирание

Хотя Закон КНР о кибербезопасности конкретно предоставляет определенные права доступа к данным, его положения краткие и не содержат подробностей, чтобы процессор PI мог должным образом облегчить такие права (см. Статью 43). Напротив, проект закона о защите личных данных содержит ряд более подробных требований:

Право на доступ (Статья 45)

Физическое лицо имеет право получать доступ и запрашивать копии своей личной информации у обработчика PI. В отличие от национального стандарта PI или GDPR, положения не содержат каких-либо дополнительных сведений о типе информации, которую процессор PI должен предоставить физическому лицу.

Право на исправление (статья 46)

Физическое лицо имеет право потребовать от обработчика PI исправить любую неточную личную информацию и дополнить неполную личную информацию, которая хранится у обработчика PI.

Право на удаление (статья 47)

Проект защиты PI определяет обстоятельства, при которых физическое лицо может потребовать у обработчика PI удаления его личной информации. Эти обстоятельства включают: (i) цели в отношении личной информации были достигнуты или согласованный период хранения истек; (ii) обработчик PI прекращает предоставление товаров и услуг; (iii) согласие было отозвано; и (iv) обработчик PI обрабатывает данные вопреки закону или согласованным целям. Существует также всеобъемлющее положение: другие обстоятельства, предусмотренные законами и постановлениями.

Однако обязательство по удалению не является абсолютным. Процессору PI не нужно стирать личную информацию, если это технически невозможно или если установленный законом срок хранения еще не истек. Однако процессор PI должен прекратить обработку личной информации.

Право на удаление также представлено в проекте закона о защите данных PI Data Protection как обязательство обработчика PI. Это означает, что при возникновении любого из упомянутых выше обстоятельств ожидается, что процессор PI удалит соответствующую личную информацию.

Хотя, похоже, нет отдельного права на возражение, как обсуждалось в Части 2, «право на возражение» встроено в обязанность обработчика PI получить согласие от отдельных лиц, причем согласие является ключевым правовым основанием для обработки личной информации. в Китае.

3. Право на автоматизированное принятие решений

Частному лицу предоставляется право возражать против использования автоматизированного принятия решений процессором PI при принятии решений, которые окажут значительное влияние на права и выгоды человека. Физическое лицо также имеет право потребовать от обработчика PI пояснений. Если для маркетинга используется автоматизированное принятие решений, проект закона о защите PI требует, чтобы обработчик PI предоставлял возможность выбора для проведения такого маркетинга без индивидуального профилирования. Право, относящееся к автоматизированному принятию решений в соответствии с проектом закона о защите персональных данных в этом отношении, не идентично праву, предусмотренному в GDPR.

4. Право на объяснение и объяснение

Законопроект о защите PI также устанавливает права физических лиц запрашивать объяснения от процессора PI по установленным им правилам обработки данных. Если процессор PI отклоняет любой запрос доступа от лица, это лицо также имеет право запросить объяснение.

Наблюдения

Одно личное право, которое заметно отсутствует в проекте закона о защите данных PI, - это право на переносимость данных, то есть право иметь свою личную информацию в формате, который может быть передан от одного процессора PI к другому. Это право в ограниченной форме можно найти в Национальном стандарте PI. параграф 8.6, который предусматривает, что, если физическое лицо этого требует и если это технически допустимо, контролер данных должен передать определенную личную информацию, запрошенную напрямую, третьей стороне, указанной таким лицом.

К другим заметным упущениям относятся: (i) подробные обязательства обработчика PI по способам реализации вышеуказанных прав (особенно всех новых прав доступа). Статья 49 проекта Закона о защите данных PI в настоящее время налагает только общие обязательства на процессор PI; и (ii) обстоятельства, при которых обработчик PI может на законных основаниях отказать в удовлетворении запросов физического лица. Сам национальный стандарт PI содержит довольно исчерпывающий набор положений (см. Параграф 8.7), охватывающий эти два упущения». ***(Michelle Chan, Clarice Yue, John Shi, Sven-Michael Werner. China Draft Personal Information Protection Law: Deep Dive (3): Individual Rights // Bird & Bird (https://www.twobirds.com/en/news/articles/2020/china/china-draft-personal-information-protection-law-deep-dive-3-individual-rights). 05.11.2020).***

***

«Комиссар по информации первоначально вручил Уведомление о намерении наложить штраф на Marriott на 99,2 миллиона фунтов стерлингов.

Окончательный штраф составил бы 28 миллионов фунтов стерлингов, но он был уменьшен на 20% до 22,4 миллиона фунтов стерлингов, чтобы учесть смягчающие факторы, включая усилия, предпринятые для работы с клиентами. Затем штраф был уменьшен до 18,4 миллиона фунтов стерлингов в свете поправок Комиссара к политике регулирующих действий, связанных с Covid-19. Хотя считается, что нарушение безопасности Marriott продолжалось с 2014 по 2018 год, штраф был определен в период после того, как GDPR стал полностью применяться, то есть с мая 2018 года по сентябрь 2018 года. Нарушение затронуло 30,1 миллиона записей EEA [1].

Контроллеры должны иметь программы для отслеживания нарушений, должны шифровать и должным образом защищать ключевые активы.

В 2014 году злоумышленник проник в системы отелей Starwood, которые были приобретены Marriott в 2016 году. Злоумышленник получил доступ к миллионам записей и всколыхнул их. Хотя записи кредитных карт были зашифрованы, подробные записи о бронировании, включая большое количество номеров паспортов, не были зашифрованы.

Комиссар пришел к выводу, что Marriott неадекватно отслеживает учетные записи пользователей и базы данных: хотя это не предотвратило бы атаку, но сделало бы более раннее обнаружение более вероятным. Комиссар также пришел к выводу, что Marriott не смогла развернуть достаточную безопасность своих ключевых систем - в частности, Комиссар пришел к выводу, что ему следовало развернуть «усиление защиты сервера» (то есть ограничение доступа к ключевым системам по указанным, утвержденным IP-адресам). Наконец, у Marriott были только зашифрованные данные кредитной карты. Комиссар выразил особую обеспокоенность тем, что номера паспортов не зашифрованы. Кроме того, похоже, что шифрование Marriott было взломано (детали этой части уведомления отредактированы).

Marriott сталкивается с групповым судебным разбирательством в связи с инцидентом, и обнаружение вины в уведомлении о денежном штрафе Уполномоченного будет полезно для заявителей.

Нарушение безопасности может повлечь за собой более высокий штраф в размере 4% - и мировой оборот, а не оборот в Великобритании, является ориентиром.

Читатели, которые знают свой GDPR наизусть, будут знать, что обязательство по внедрению соответствующих технических и организационных мер изложено в Ст. 32 GDPR - максимальный штраф составляет 2% от мирового оборота или 10 миллионов евро, в зависимости от того, что больше. Однако GDPR также ссылается на обязательство обеспечить надлежащую безопасность в статье 5 (1) (f) - среди принципов защиты данных, применимых к контроллерам, - для которых максимальный штраф составляет 4% или 20 миллионов евро.

ICO обнаружило, что Marriott нарушила статью 5 (1) (f), что позволило применить более высокий предел (хотя фактический штраф в любом случае не превышает более низкой суммы).

При рассмотрении этого вопроса ICO обращало внимание на оборот главного контролера, Marriott International Inc., а не на оборот, применимый к ЕЭЗ или британскому бизнесу.

Передача вашей информационной безопасности на аутсорсинг не означает, что вы избежите штрафа.

Marriott отметила, что она передала свою информационную безопасность на аутсорсинг Accenture. Комиссар по информации четко отметил, что, если организация признает, что это контролер, привлечение третьей стороны не может снизить ответственность контролера.

Marriott также привлекла третью сторону для проведения аудита PCI DSS. В отчетах аудита неверно утверждалось, что для этих систем применялась многофакторная аутентификация. ICO заявило, что для Marriott было разумно полагаться на эти заявления, даже если они были неверными.

В решении не комментируется разница в подходах Accenture и аудитора PCI. Разница может заключаться в том, что Marriott может ясно показать ошибку со стороны аудитора, тогда как в решении не упоминается о вине Accenture. Это может быть область, которая станет важной при принятии других решений.

Факторы, влияющие на установление и уменьшение штрафа

Уведомление об окончательном решении не объясняет, как комиссар пришел к цифре в 28 миллионов фунтов стерлингов. Он отмечает, что это было расценено как очень серьезное нарушение; что нарушение безопасности с мая по сентябрь 2018 года рассматривалось как значительный период и что количество людей, степень бедствия или ущерба (хотя не было доказательств финансовых потерь) и непринятие разумных мер для смягчения последствий нарушение - все соответствующие факторы, оправдывающие наложение (значительного) штрафа.

К смягчающим факторам относятся более поздние инвестиции в повышение безопасности, тот факт, что Marriott создал индивидуальный веб-сайт и имел колл-центр, работающий на нескольких языках, который обеспечивал веб-мониторинг и взаимодействовал с эмитентами карт.

Комиссар отвергла аргументы Marriott о том, что она слишком сильно полагалась на текучесть кадров, чтобы установить штраф; что это просто наказание организаций за их размер; и что вместо этого подход, предусматривающий установленный тариф для каждого типа нарушений, был бы более подходящим. Комиссар также отверг аргументы Marriott о том, что по сравнению со штрафами, налагаемыми другими органами ЕЭЗ, это было слишком много. Здесь комиссар отметила, что хотя GDPR должен привести к большей согласованности, на данный момент было слишком мало штрафов - и все они были конкретными, - так что ее это не убедило. Она также заявила, что тот факт, что наказание было передано в механизм согласованности в соответствии со статьей 60, означает, что оно должно соответствовать штрафам, применяемым в других случаях». ***(Ruth Boardman. Information Commissioner fines Marriott International Inc. £18.4 million in relation to its 2018 data breach // Bird & Bird***

(https://www.twobirds.com/en/news/articles/2020/global/information-commissioner-fines-marriott-international). 02.11.2020).

***

«После утечки данных в сентябре злоумышленник продает базу данных RedDoorz, содержащую 5,8 миллиона пользовательских записей, на хакерском форуме.

RedDoorz - это сингапурская платформа для управления и бронирования отелей с более чем 1000 отелями в Юго-Восточной Азии. Используя веб-сайт или мобильное приложение, пользователи могут зарегистрировать учетную запись, чтобы просматривать доступные бюджетные отели и бронировать места.

В конце сентября 2020 года RedDoorz сообщили, что они пострадали от взлома данных после того, как неавторизованный человек получил доступ к одной из их баз данных. Однако в то время ни финансовая информация, ни пароли RedDoorz не были раскрыты «насколько ей было известно».

5,8 миллиона записей пользователей RedDoorz продано онлайн

На этой неделе злоумышленник начал продавать базу данных, содержащую 5,8 миллиона пользовательских записей, которые были украдены во время утечки данных RedDoorz.

В рамках продажи злоумышленник поделился образцом базы данных, включая структуру таблицы и записи для 587 пользователей. Эти записи позволяют нам увидеть, что было раскрыто во время взлома RedDoorz.

Для каждой записи пользователя в базе данных отображается адрес электронной почты участника RedDoorz, хешированные пароли bcrypt, полное имя, пол, ссылка на фотографию профиля, номер телефона, дополнительный номер телефона, дату рождения и род занятий.

По многочисленным пользовательским записям в примерах BleepingComputer подтвердил, что указанные адреса электронной почты и номера телефонов верны для конкретного пользователя.

Хотя эта утечка данных выявила гораздо более конфиденциальные данные, чем первоначально было заявлено RedDoorz, она не содержит никакой финансовой информации.

Что делать пользователям RedDoorz?

На всякий случай, если вы являетесь пользователем RedDoorz, вам следует немедленно сменить пароль.

Если вы используете тот же пароль на других сайтах, вам также следует изменить пароль на этих сайтах на уникальный и надежный для этого сайта.

Использование уникальных паролей на каждом сайте, на котором у вас есть учетная запись, предотвращает нарушение данных на одном сайте от воздействия на вас других веб-сайтов, которые вы используете.

Рекомендуется использовать менеджер паролей, который поможет вам отслеживать уникальные и надежные пароли на каждом сайте». ***(Lawrence Abrams. 5.8 million RedDoorz user records for sale on hacking forum // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/58-million-reddoorz-user-records-for-sale-on-hacking-forum/). 10.11.2020).***

***

«На веб-сайте DontTouchTheGreenButton.com, только что запущенном кампанией Трампа в связи с недавно поданным в Аризоне иском об отклонении голосов, была обнаружена утечка данных избирателей.

Данные включали имя избирателя, адрес и уникальный идентификатор. Однако появились сообщения о пользователях, утверждающих, что на веб-сайте есть недостатки SQL-инъекции, которые позволяют собирать SSN избирателя и дату рождения.

«Наспех» запущен сайт утечки данных

В минувшие выходные кампания по переизбранию президента Трампа и Республиканский национальный комитет подали иск в Аризоне, утверждая, что сотрудники избирательных комиссий округа Марикопа неправильно отклонили личное голосование в день выборов, злоупотребив механической функцией (зеленой кнопкой) на пульте управления. машины для голосования.

«Сотрудники избирательных комиссий изо всех сил пытались использовать новые машины для голосования в округе Марикопа, и неправильно нажимали и просили избирателей нажать зеленую кнопку, чтобы исправить серьезные ошибки», - сказал Мэтт Морган, главный советник кампании Трампа 2020.

«В результате машины для голосования не учитывали голоса, отданные лично избирателями в день выборов в округе Марикопа», - заявил Морган.

Для сбора анекдотических свидетельств от избирателей, которые могли наблюдать такое поведение на избирательных участках, подтверждающих то, что утверждается в иске, кампания создала веб-сайт для сбора заявлений избирателей под присягой.

Веб-сайт DontTouchTheGreenButton.com запрашивает у избирателей личную информацию, такую как их имя и адрес, номер телефона, адрес электронной почты, дату рождения, последние 4 цифры номера социального страхования (SSN) и ответы на вопросы с несколькими вариантами ответов…

Учитывая, что данные об избирателях уже являются общедоступной информацией *, возможность для любого найти эту информацию не вызывает удивления, хотя это очевидная проблема конфиденциальности.

Однако на веб-сайте использовался API, позволяющий производить массовый сбор информации об избирателях.

При условии, что веб-сайт был запущен довольно быстро после подачи иска, некоторые пользователи называют его «поспешной настройкой» и изобилуют утечками данных и ошибками внедрения SQL.

BleepingComputer заметил, что данные извлекаются с сервера с помощью Algolia REST API.

Открытый ключ API и идентификатор приложения в запросе могут позволить любому пользователю программно запускать запросы для массового удаления данных избирателей из службы.

Данные JSON, возвращаемые REST API, по умолчанию содержат список из 5 имен и адресов избирателей, а также уникальные идентификаторы, основанные на поисковом запросе (например, первые несколько букв имени избирателя).

Теоретически можно было бы сделать автоматические запросы для загрузки информации об избирателе, изменив значение hitsPerPage, показанное выше, на более высокое значение, и делать это многократно для различных многобуквенных комбинаций, пока они не просканируют весь набор данных.

Этот API, используемый для получения информации об избирателях, был удален с сайта DontTouchTheGreenButton.com.

На Reddit некоторые пользователи также утверждали, что веб-сайт соответствует названию и адресу, представленным последним 4 цифрам SSN, введенным пользователем, и раскрывает частичный SSN.

Принимая во внимание, что другие пользователи упомянули, что можно выполнить атаку SQL-инъекции на веб-сайт, чтобы получить информацию SSN и дату рождения для избирателей…». ***(Ax Sharma. Trump lawsuit site to report 'rejected votes' leaked voter data // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/trump-lawsuit-site-to-report-rejected-votes-leaked-voter-data/). 08.11.2020).***

***

«Folksam, одна из крупнейших страховых компаний Швеции, сегодня раскрыла утечку данных, затронувшую около 1 миллиона шведов, после того, как они поделились личной информацией клиентов с несколькими технологическими гигантами.

По словам Йенса Викстрёма, руководителя отдела маркетинга и продаж Folksam, страховщик обнаружил утечку данных после внутреннего аудита и сообщил об инциденте в Шведский орган по защите данных (Datainspektionen).

«Компании, которые получили персональные данные от Folksam, - это, например, Facebook, Google, Microsoft, Linkedin и Adobe», - пояснил Викстрём. «Целью было, среди прочего, проанализировать, какую информацию вошедшие в систему клиенты и другие посетители искали на folksam.se».

Конфиденциальные личные данные, передаваемые Folksam, включают различные типы информации, такие как номера социального страхования или информацию о том, что отдельное лицо приобрело профсоюз или страховку на беременность.

Результаты анализа совместно используемых данных использовались технологическими гигантами для предоставления клиентам индивидуальных предложений через каналы связи Folksam и других компаний, сказал Викстрём.

Этого не должно произойти, и сейчас мы много работаем, чтобы этого больше никогда не повторилось. Мы отображаем, какие личные данные мы передаем нашим партнерам и как мы их передаем. Мы работаем параллельно, чтобы гарантировать наличие процедур и обновленных соглашений. - Йенс Викстрём

«Наша цель заключалась в том, чтобы проанализировать и предоставить нашим клиентам индивидуальные предложения, но, к сожалению, мы сделали это неправильно», - добавил Викстрём.

Обнаружив нарушение, Folksam немедленно прекратил делиться конфиденциальной информацией со своими цифровыми партнерами и потребовал удалить эту информацию от компаний, которые ее получили.

«Мы понимаем, что это может вызвать беспокойство у наших клиентов, и серьезно относимся к тому, что произошло», - сказал Викстрём. «Мы немедленно прекратили разглашать эту личную информацию и потребовали ее удаления».

Folksam заявляет, что на данный момент нет никаких доказательств того, что общие конфиденциальные данные использовались третьими лицами ненадлежащим образом…». ***(Sergiu Gatlan. Folksam data breach leaks info of 1M Swedes to Google, Facebook, more // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/folksam-data-breach-leaks-info-of-1m-swedes-to-google-facebook-more/). 03.11.2020).***

***

«Сайт сообщества производителей каннабиса невольно выложил в публичный доступ данные более 3,4 миллионов пользовательских записей, в том числе из стран, где выращивание данного растения незаконно, сообщают исследователи.

Незащищённую базу данных обнаружили 10 октября, хотя система индексировалась BinaryEdge ещё с 22 сентября. Принадлежала база сайту GrowDiaries, на котором пользователи делились информацией о своих растениях сорта каннабис.

Среди опубликованных данных обнаружили адреса электронной почты, IP-адреса, имена пользователей, а также их посты и хэшированные пароли». ***(Случайная утечка данных производителей каннабиса // SecureNews (https://securenews.ru/accidental-data-leak-of-cannabis-producers/). 05.11.2020).***

***

«Испанский разработчик Prestige Software по ошибке выложил базу данных своих пользователей в открытый доступ. Она содержала более 10 миллионов файлов с личной информацией.

Исследователь из Website Planet предупреждает, что утечка может быть более масштабной, так как некоторые файлы содержали информацию сразу нескольких человек.

Среди данных были обнаружены полные имена, электронные адреса, номера паспортов, телефонные номера и платежная информация посетителей отелей.

Полученными данными могли воспользоваться для организации фишинговых атак и манипуляций с деталями бронирования.

Однако на данный момент нет свидетельств того, что злоумышленники использовали эти данные». ***(Крупная утечка данных на платформе для бронирования отелей // SecureNews (https://securenews.ru/major-data-breach-on-hotel-booking-platform/). 09.11.2020).***

***

«На просторах даркнета неизвестный выложил на продажу доступ администратора к пакистанским авиалиниям. Это обнаружила команда киберразведывательной фирмы KELA.

По наблюдениям KELA, покупателей у злоумышленника много. «Люди, которые приобрели доступ к сети, впоследствии могут продвинуться дальше и атаковать компанию вирусом-вымогателем», — предсказывает представитель.

Неделю спустя киберпреступник опубликовал новое объявление о продаже всех баз данных авиакомпании. Для примера он выложил часть якобы украденной информации. Он уверял, что она содержит имена, фамилии и номера паспортов всех клиентов.

Если злоумышленник говорит правду, значит, преступление он совершил дважды: получив доступ к сети авиалиний и используя его, чтобы украсть базы данных.

KELA следила за угрозой с июля 2020 года. За это время киберпреступник продал доступ 38 раз на общую сумму, по крайней мере, в $118,700.

«Мы знаем, что у него доступ шире, чем он предлагает», — сообщает KELA». ***(Хакер продает доступ к сети авиалиний Пакистана // SecureNews (https://securenews.ru/hacker-sells-access-to-pakistan-airlines-network/). 11.11.2020).***

***

«Согласно Датскому агентству по защите данных, ни один контроллер данных не должен запрашивать у субъектов данных отправку конфиденциальных или конфиденциальных персональных данных через незашифрованное интернет-соединение.

Все контроллеры данных подчиняются принципу подотчетности в ст. 5 GDPR, который требует от них обеспечения обработки персональных данных способом, гарантирующим надлежащую безопасность.

На практике это означает, что контролер данных перед обработкой персональных данных должен провести оценку рисков и принять соответствующие меры безопасности, соответствующие идентифицированному риску (-ам).

В 2018 году датское агентство по защите данных Datatilsynet опубликовало заявление о требованиях к шифрованию (только на датском языке)., поскольку Datatilsynet придерживался мнения, что переписка по электронной почте, включающая секретную или конфиденциальную информацию, должна быть зашифрована, чтобы обеспечить надлежащую безопасность. В своем руководстве Datatilsynet перечислил различные подходящие методы шифрования и заявил: Когда электронное письмо отправляется от контроллера данных, контроллер данных отвечает за безопасную передачу на почтовый сервер получателя.

Datatilsynet опубликовал новое заявление (только на датском языке), в котором Datatilsynet поясняет, что обязательство (в качестве контроллера данных под датской юрисдикцией) обеспечить надлежащую безопасность повышается, если контроллер данных запросил у субъекта данных отправку информации. к контроллеру данных, то есть обязательство по обеспечению безопасности применяется не только с момента времени, когда контроллер данных получает

данные, но и с момента, когда субъект данных отправляет запрошенную информацию контроллеру.

Есть только два исключения из дополнительных мер безопасности; незапрошенные персональные данные, предоставленные субъектами данных, или в случае, если субъект данных активно решает не использовать решение для безопасной передачи.

Требование распространяется как на государственные органы, так и на частные предприятия, действующие в качестве контроллеров данных, которые в рамках задачи или услуги запрашивают субъектов данных, например клиентов / клиентов / пациентов, для отправки определенных типов личных данных. Кроме того, Datatilsynet, по крайней мере публично, не признал переходный период для контроллеров данных.

В заключение, это новое требование означает, что контроллеры данных, которые запрашивают у субъектов данных отправку конфиденциальных или конфиденциальных личных данных, теперь обязаны предоставить субъекту данных возможность использовать зашифрованный канал, например, достаточно безопасное решение для двусторонней передачи, позволяет контролеру данных и субъекту данных обмениваться конфиденциальными и конфиденциальными личными данными, относящимися к субъекту данных». ***(Michael Gorm Madsen, Laura Katarina Dollerup. Who is responsible when personal data is sent via un-encrypted connections? // Bird & Bird (https://www.twobirds.com/en/news/articles/2020/denmark/who-is-responsible-when-personal-data-is-sent-via-unencrypted-connections). 19.11.2020).***

***

«Сингапур расследует утверждения о том, что местное мобильное приложение Muslim Pro продавало «подробные данные о местоположении» военным США. Популярное приложение для отслеживания молитв, получившее более 98,5 миллионов загрузок по всему миру, опровергло обвинения, заявив, что делится со своими партнерами только анонимными данными.

Комиссия по защите персональных данных (PDPC) подтвердила, что инвестирует в обвинения, и запросила дополнительную информацию у разработчика Muslim Pro, Bitsmedia. Регулирующий орган сообщил местным СМИ: «Мы напоминаем пользователям, что они также должны помнить о типах разрешений и личных данных, которые они предоставляют, и о том, как они могут быть использованы. В случае сомнений пользователи не должны загружать или использовать какие-либо приложения».

Основанная в 2009 году сингапурская компания Bitsmedia имеет офисы в Малайзии и Индонезии. Его приложение Muslim Pro отслеживает время молитв и, среди прочего, показывает направление в Мекку. Согласно его веб-сайту, оно было загружено пользователями из 200 стран.

Ранее на этой неделе сообщалось, что приложение продавало подробные данные о местоположении X-Mode, стороннему агрегатору данных из США, который продает свои услуги клиентам, в том числе подрядчикам из США.

Американско-канадское новостное агентство Vice Media опубликовало эту новость в своем отчете, заявив, что Muslim Pro было среди других мобильных приложений, которые продавали данные военным США и включали временные метки, данные о модели телефона и название сети Wi-Fi. к которому был подключен телефон.

Bitsmedia опровергла обвинения, опубликовав два заявления во вторник и четверг и отклонив их как «неверные и не соответствующие действительности».

Отметив, что это соответствовало глобальным законам и положениям о конфиденциальности данных, таким как GDPR (Общее положение о защите данных) ЕС и Закон о конфиденциальности потребителей Калифорнии (CCPA), Bitsmedia заявила, что «собирает, обрабатывает и использует информацию», которую предоставляют ее пользователи. разработчику при доступе к его приложению, чтобы "улучшить наш сервис" и облегчить "исследования и разработки" (НИОКР) для своего приложения.

Он сказал, что это может включать анализ данных, чтобы лучше понять поведение пользователей, чтобы «улучшить общую функциональность» своего сервиса. Он добавил, что данные о местоположении использовались для расчета времени молитвы и облегчили функции планирования и проектирования, а также для улучшения общего пользовательского опыта.

Разработчик приложения также настаивал, что не разглашает конфиденциальную личную информацию, такую как имя, номер телефона и адрес электронной почты. «Любые данные, передаваемые партнерам, анонимны, что означает, что наши данные не относятся к каким-либо конкретным лицам», - говорится в сообщении.

«Мы применяем стандартные меры безопасности и защитные меры и выбираем ведущих технологических партнеров, чтобы обеспечить безопасность наших данных в нашей облачной инфраструктуре. Мы также были открыты и прозрачны в отношении личной информации, которую мы собираем, храним и обрабатываем».

Опровергнув утверждения Vice Media, Bitsmedia заявила, что прекратила все отношения со своими информационными партнерами, включая X-Mode, "вступив в силу немедленно".

Он сказал, что сотрудничал с «избранными технологическими партнерами», чтобы улучшить качество своего приложения, и обменивался данными со своими партнерами для «общих целей, таких как реклама», что, по его мнению, было его основным источником дохода. Он сказал, что сделал это «в полном соответствии» со всеми соответствующими законами и внедрил «строгую политику управления данными» для защиты данных своих пользователей.

По словам разработчика приложения, он работал с третьими сторонами, такими как социальные сети и компании, занимающиеся анализом данных, и обменивался данными с согласия своих пользователей.

Он также отметил, что, помимо раздела «Сообщество», функции, представленные в Muslim Pro, доступны без необходимости входа в приложение. «Это способствует анонимности данных, которые мы собираем и обрабатываем», - говорится в сообщении.

В случае нарушения Закона Сингапура о защите личных данных (PDPA) Bitsmedia может столкнуться с финансовыми штрафами в размере до 10% от годового оборота или 1 млн сингапурских долларов (735 490 долларов США), в зависимости от того, какая сумма больше.

Только в этом месяце Сингапур обновил законодательство о защите данных, чтобы позволить местным предприятиям использовать данные потребителей без предварительного согласия для некоторых целей, таких как улучшение бизнеса и исследования. Поправки также позволили наложить более суровые финансовые санкции за утечку данных сверх предыдущего предела в 1 миллион сингапурских долларов.

В своем выступлении, посвященном поправкам, министр связи и информации Сингапура С. Ишваран сказал, что данные являются ключевым экономическим активом в цифровой экономике, поскольку они предоставляют ценную информацию, которая информирует предприятия и способствует повышению эффективности. По словам Исварана, это также расширит возможности для инноваций и улучшит продукты и станет критически важным ресурсом для новых технологий, таких как искусственный интеллект (ИИ), которые обладают преобразующим потенциалом.

Среди ключевых изменений в PDPA - требование «исключения из согласия», которое теперь позволяет предприятиям использовать, собирать и раскрывать данные для «законных целей», улучшения бизнеса и более широкого объема исследований и разработок. В дополнение к существующим исключениям согласия, которые включают в себя цели расследований и реагирования на чрезвычайные ситуации, теперь они также включают усилия по борьбе с мошенничеством, совершенствованию продуктов и услуг и проведению маркетинговых исследований для понимания потенциальных сегментов клиентов.

Кроме того, дальнейшие поправки, определенные как «предполагаемое согласие» к PDPA, теперь позволят организациям обмениваться данными с внешними подрядчиками с целью выполнения контрактов с клиентами. Это обслуживает «современные коммерческие договоренности» и важные цели, включая безопасность.

Компании также смогут использовать данные без согласия для содействия исследованиям и разработкам, которые еще не были отмечены для выпуска продукции. Для всех других целей, кроме «предполагаемых» и «исключений» согласия, таких как сообщения прямого маркетинга, по-прежнему требуется предварительное согласие потребителей…». ***(Eileen Yu. Singapore investigating claims Muslim app developer sold user data to US military // ZDNet (https://www.zdnet.com/article/singapore-investigating-claims-muslim-app-developer-sold-user-data-to-us-military/). 20.11.2020).***

***

«Некоторым компаниям, вероятно, придется значительно изменить способы защиты данных, чтобы продолжить работу с европейскими резидентами, в соответствии с проектом руководящих принципов, выпущенным на прошлой неделе Европейским союзом, которые требуют

усиленных мер защиты конфиденциальности для информации, передаваемой за пределы блока.

Согласно проекту правил, компании будут вынуждены применять строгие методы шифрования и гарантировать, что личные данные европейцев не могут быть расшифрованы, если они будут перемещать эту информацию в США и другие страны за пределами ЕС.

Эксперты по конфиденциальности полагают, что эти рекомендации, вероятно, будут способствовать использованию новых методов шифрования данных.

Руководящие принципы представляют собой попытку отреагировать на значительную неопределенность, возникшую после июльского постановления верховного суда ЕС, в котором говорилось, что соглашение о защите конфиденциальности между ЕС и США является незаконным. Это соглашение было заключено в 2016 году и позволило осуществлять трансатлантическую коммерческую передачу данных, но суд заявил, что слежка правительства США представляет собой угрозу конфиденциальности, и что европейцы не имеют достаточных возможностей для возмещения ущерба в американской правовой системе.

Суд ЕС также постановил, что компании могут продолжать использовать отдельный, широко используемый международный метод передачи данных, известный как стандартные договорные положения, но только с дополнительными гарантиями, гарантирующими защиту данных от слежки.

Проект руководящих принципов регулирующих органов означает, что «передача данных в третьи страны строго ограничена», - сказал Лукаш Олейник, независимый исследователь и консультант по кибербезопасности из Брюсселя.

Кроме того, Европейская комиссия, исполнительный орган ЕС, на прошлой неделе опубликовала проект пересмотра своих стандартных договорных положений, которые представляют собой предварительно утвержденные контракты, определяющие, как компании могут передавать данные в страны, не входящие в блок. Новые статьи ужесточают требования для компаний, передающих данные деловым партнерам или дочерним компаниям за границу.

Проект руководящих принципов регулирующих органов будет применяться к странам, не входящим в союз из 27 членов, у которых нет так называемого решения о соответствии с блоком. Власти ЕС на данный момент предоставили 12 странам, включая Канаду и Новую Зеландию, заключение о достаточности, считая их законы о конфиденциальности достаточно строгими, чтобы компании могли перемещать туда личные данные европейцев без особых мер предосторожности.

Регулирующие органы перечислили несколько вариантов, которые компании могут использовать для продолжения передачи данных за границу без нарушения Общего регламента ЕС о конфиденциальности данных 2018 года. Руководящие принципы не требуют, чтобы компании применяли определенные меры, но оговаривают, что компании нарушают закон ЕС, когда они передают данные без столь же строгих мер защиты, как их рекомендации. Проект будет открыт для общественного обсуждения до 30 ноября.

Проект стандартных договорных положений Европейской комиссии также включает обновления в ответ на июльское решение суда. Согласно проекту, который будет открыт для комментариев до 10 декабря, фирмы за пределами ЕС должны будут информировать деловых партнеров, если какое-либо государственное учреждение или разведывательный орган подаст юридически обязательный запрос на доступ к данным европейцев. Комиссия предварительно одобряет эти положения о конфиденциальности.

Компаниям необходимо будет оценить, угрожают ли законы других стран конфиденциальности, а это означает, что им потребуется достаточная и точная информация об иностранном законодательстве, - сказал Анри Куяла, глобальный специалист по конфиденциальности в HERE Global BV, компании, предоставляющей услуги цифрового картографирования, контрольный пакет акций которой принадлежит Volkswagen. AG, Audi, BMW AG и Daimler AG. По его словам, оценка может стать более сложной, если в странах, где находятся поставщики компаний, изменятся законы.

По словам Куяла, нормативная поддержка таких методов, как гомоморфное шифрование и многосторонние вычисления, вероятно, расширит использование этих методов. Технология гомоморфного шифрования позволяет выполнять вычисления с зашифрованными данными без их дешифрования. Защита с помощью многосторонних вычислений разделяет данные между компьютерами, поэтому их нельзя использовать для идентификации человека без дополнительной информации.

«Это может существенно повлиять на подход компаний к шифрованию», - сказала Кейтлин Феннесси, директор по исследованиям торговой группы International Association of Privacy Professionals.

По словам Феннесси, для многих компаний соблюдение новых руководящих принципов по передаче данных будет означать, что команды по кибербезопасности и конфиденциальности будут более тесно сотрудничать. Вместе они должны будут разработать технические меры, такие как политика шифрования, сказала она. «Специалистам по конфиденциальности придется работать рука об руку с профессионалами в области безопасности больше, чем когда-либо в прошлом», - сказала она». ***(Catherine Stupp. EU Restrictions Could Force Companies to Change Data Transfer Practices // Dow Jones & Company (https://www.wsj.com/articles/eu-restrictions-could-force-companies-to-change-data-transfer-practices-11605609001?mod=tech_lead_pos10). 17.11.2020).***

***

«Налоговая служба США (IRS) объявила сегодня, что конфиденциальная информация будет замаскирована во всех налоговых декларациях предприятий, начиная со следующего месяца, чтобы защитить компании от кражи личных данных.

Кража бизнес-идентичности происходит, когда владельцы или сотрудники компании выдают себя за третьих лиц в процессе совершения мошенничества, такого как незаконное получение наличных денег, кредитов и займов, оставляя бизнесу заниматься возникающими долгами.

Этот тип кражи личных данных происходит после того, как мошенники получают доступ к банковским счетам и кредитным картам компании или после кражи конфиденциальной информации компании, включая, помимо прочего, идентификационные номера налогоплательщиков (ИНН) и личную информацию владельцев.

Новые меры защиты от кражи личных данных

«Стремясь защитить бизнес-налогоплательщиков от кражи личных данных, Налоговая служба сегодня объявила, что с 13 декабря она начнет маскировать конфиденциальные данные в расшифровках налоговых деклараций предприятий», - заявили в правительственном агентстве.

Как только конфиденциальные данные о налоговых декларациях предприятий начнут маскироваться, IRS сообщает, что в новых налоговых отчетах будет отображаться только следующая информация:

Последние четыре цифры любого идентификационного номера работодателя, указанного в расшифровке стенограммы: XX-XXX1234.

Последние четыре цифры любого номера социального страхования или индивидуального налогового идентификационного номера, указанного в расшифровке: XXX-XX-1234.

Последние четыре цифры любого счета или номера телефона

Первые четыре символа имени и фамилии любого человека (первые три символа, если имя состоит только из четырех букв)

Первые четыре символа любого имени в строке названия компании

Первые шесть символов почтового адреса, включая пробелы

Все денежные суммы, включая заработную плату и доход, причитающийся остаток, проценты и штрафы.

Новая налоговая выписка по-прежнему будет содержать дополнительный идентификатор, который соответствует налогоплательщику (юридическому или физическому лицу) в расшифровке.

30-дневное уведомление о внесении изменений

Это объявление предоставляет всем заинтересованным сторонам 30 дней на то, чтобы внести какие-либо изменения в свои процессы налоговой отчетности и анализа.

Налоговые специалисты были проинформированы IRS об этой мере по защите от кражи личных данных, которая началась этим летом в рамках Общенационального налогового форума.

Два года назад налоговое бюро министерства финансов начало маскировать всю конфиденциальную информацию, содержащуюся в индивидуальных налоговых декларациях.

В прошлом году IRS также опубликовало руководство, чтобы помочь налогоплательщикам защитить себя от попыток кражи личных данных при совершении покупок в Интернете.

Налоговое управление также дважды в этом году [1, 2] призывало налогоплательщиков включить многофакторную аутентификацию (MFA) в программном обеспечении для подготовки налоговых данных для защиты от кражи данных и попыток хакерского захвата». ***(Sergiu Gatlan. IRS announces move to***

protect businesses from identity theft // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/irs-announces-move-to-protect-businesses-from-identity-theft/). 13.11.2020).

***

«Хакер делится тем, что, по их словам, составляет 3,2 миллиона записей пользователей Pluto TV, которые были украдены во время утечки данных.

Pluto TV - это служба интернет-телевидения, которая позволяет транслировать бесплатные телешоу с рекламой. Сервис насчитывает более 28 миллионов пользователей, а его мобильные приложения были установлены более 10 миллионов раз.

База данных Pluto TV просочилась на хакерский форум

На прошлой неделе злоумышленники выпускали пользовательские базы данных для ужасных коммерческих веб-сайтов, которые были украдены во время утечки данных на хакерском форуме.

Сообщается, что все эти взломы были совершены злоумышленником по имени ShinyHunters, который в прошлом был ответственен за многочисленные утечки данных и взлом частного репозитория Microsoft GitHub. Однако за последние несколько месяцев ShinyHunters исчезли, и было зарегистрировано меньше утечек данных.

С момента повторного появления ShinyHunters были подтверждены многочисленные утечки данных, в том числе Animal Jam, 123RF, Geekie, Athletico, Wongnai, RedMart и многие другие.

В среду злоумышленник поделился так называемой пользовательской базой данных Pluto TV, содержащей 3,2 миллиона пользовательских записей. Это нарушение данных снова приписывается ShinyHunters…

Поскольку некоторые из раскрытых данных были подтверждены как точные, похоже, что достоверная информация была раскрыта.

Из осторожности рекомендуется, чтобы все пользователи Pluto TV немедленно изменили свои пароли.

Если вы используете тот же пароль Pluto TV на других сайтах, настоятельно рекомендуется изменить их и там. Вы можете использовать менеджер паролей, чтобы отслеживать уникальные пароли на каждом сайте». ***(Lawrence Abrams. Hacker shares 3.2 million Pluto TV accounts for free on forum // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hacker-shares-32-million-pluto-tv-accounts-for-free-on-forum/). 14.11.2020).***

***

«В результате утечки данных Luxottica была раскрыта личная и защищенная информация о здоровье 829 454 пациентов в LensCrafters, Target Optical, EyeMed и других офтальмологических учреждениях.

Luxottica - крупнейшая в мире компания по производству очков с портфелем известных брендов очков, включая Ray-Ban, Oakley, Oliver Peoples, Ferrari, Michael Kors, Bulgari, Armani, Prada, Chanel и Coach.

Помимо продажи очков, Luxottica также управляет компанией EyeMed vision и сотрудничает с офтальмологами в рамках своих торговых точек LensCrafters, Target Optical, EyeMed и Pearle Vision.

Эти партнеры получают доступ к веб-приложению для записи на прием, которое позволяет пациентам назначать приемы онлайн или по телефону.

Нарушение данных в системе записи на прием

В уведомлении «Об инциденте безопасности», опубликованном на этой неделе, Luxottica сообщила, что их приложение для записи на прием подверглось утечке данных после взлома 5 августа 2020 года.

Luxottica заявляет, что они впервые узнали об этой утечке 9 августа и после расследования атаки 28 августа определили, что злоумышленник получил доступ к личной информации пациентов.

«9 августа 2020 года Luxottica узнала об инциденте, сдержала его и немедленно начала расследование, чтобы определить масштаб инцидента. 28 августа 2020 года мы предварительно пришли к выводу, что злоумышленник мог получить доступ и получить информацию о пациентах», в уведомлении об утечке данных Luxottica.

Раскрытая информация включает личные данные (PII) и защищенную медицинскую информацию (PHI), включая медицинские данные и историю болезни.

"Личная информация, связанная с этим инцидентом, могла включать: полное имя, контактную информацию, дату и время встречи, номер страхового полиса, а также записи о враче или записи о приеме, которые могут содержать информацию, относящуюся к лечению глаз, например, рецепты, состояние здоровья или процедуры ", - предупредила Luxottica.

Для некоторых пациентов также были раскрыты номера кредитных карт и номера социального страхования.

Если у пациента была раскрыта его платежная информация и SSN, Luxottica предлагает бесплатную двухлетнюю услугу по мониторингу личности через Kroll.

Luxottica не осведомлена о неправомерном использовании полученных данных, но советует всем пациентам следить за уведомлениями от своих страховых компаний или поставщиков медицинских услуг и отслеживать свои кредитные отчеты и историю на предмет мошенничества.

"Мы рекомендуем всем потенциально затронутым людям принять меры для защиты себя, например, внимательно отслеживая уведомления вашей страховой компании и поставщиков медицинских услуг о неожиданных действиях. Если информация о вашей платежной карте и / или номер социального страхования были причастны к этому инциденту, это прямо указано в вашем письме "Luxottica сообщила на веб-сайте, созданном специально для этой утечки данных.

27 октября Luxottica начала рассылать уведомления пострадавшим. Они также начали публиковать пресс-релизы для местных газет на веб-сайтах, чтобы предупредить пациентов об утечке данных…» ***(Lawrence Abrams. Luxottica data breach exposes 820K EyeMed, LensCrafters patients // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/luxottica-data-breach-exposes-820k-eyemed-lenscrafters-patients/). 12.11.2020).***

***

«Офис Комиссара по информации Великобритании оштрафовал британскую компанию по продаже и распространению билетов на 1,25 млн фунтов стерлингов за утечку данных миллионов покупателей по всей Европе в 2018 году.

Об утечке сообщили в июне 2018 года после того, как сторонний провайдер Inbenta Technologies был заражен вредоносной программой. Но началась она в феврале того же года. Ее обнаружили после того, как покупатели Monzo Bank сообщили о мошеннических транзакциях.

Малварь украла информацию о пользователях и передала их неизвестному злоумышленнику. Данные включали имена, адреса, электронные адреса, телефонные номера, номера платежных карт, даты истечения, CCV-коды и детали регистрации на сайте Ticketmaster более чем 11 миллионов покупателей в Европе и Соединенном Королевстве.

Расследование показало, что Ticketmaster пренебрег Общим регламентом защиты персональных данных. Сайт не обеспечил адекватные меры безопасности, чтобы предотвратить кибератаки на чат-бот, установленный на странице сайта с оплатой.

Расследование также показало, что Ticketmaster начал мониторить свой сетевой трафик только через 9 недель после сообщения о возможных атаках.

Вследствие утечки злоумышленник воспользовался данными 60 000 платежных карт банка Barclays. Monzo Bank же заменил данные 6000 платежных карт пользователей Ticketmaster из-за мошеннического использования». ***(Ticketmaster оштрафовали на 1,25 млн фунтов стерлингов за утечку данных // SecureNews (https://securenews.ru/ticketmaster-fined-1-25m-for-data-breach/). 16.11.2020).***

***

«Киберпреступники оставили открытой базу данных ElasticSearch, раскрывая глобальную атаку, которая скомпрометировала учетные записи Facebook и использовала их для обмана других.

Исследователи обнаружили широкомасштабную глобальную аферу, нацеленную на пользователей Facebook, после обнаружения незащищенной базы данных, используемой мошенниками для хранения имен пользователей и паролей не менее 100 000 жертв.

Исследователи заявили, что киберпреступники, стоящие за мошенничеством, обманом заставляли жертв Facebook предоставить учетные данные для входа в свою учетную запись с помощью инструмента, который делал вид, что раскрывает, кто посещал их профили.

Затем мошенники «использовали украденные учетные данные для распространения спам-комментариев к сообщениям в Facebook через взломанную учетную запись жертв, направляя людей на их сеть мошеннических веб-сайтов», как сообщили в пятницу исследователи vpnMentor. «Все эти веб-сайты в конечном итоге привели к созданию поддельной торговой платформы биткойнов, которая

использовалась для обмана людей с «депозитами» на сумму не менее 250 евро [295 долларов]».

Исследователи заявили, что у них нет доказательств того, был ли доступ к данным или утечка каких-либо других злоумышленников.

Threatpost обратился к Facebook за дополнительными комментариями.

База данных

Размер незащищенной базы данных Elasticsearch составлял 5,5 гигабайт и содержал 13 521 774 записи не менее 100 000 пользователей Facebook. Он был открыт с июня по сентябрь этого года; он был обнаружен 21 сентября и закрыт 22 сентября.

Данные в открытой базе данных включали учетные данные и IP-адреса; текстовые наброски комментариев, которые мошенники оставляли на страницах Facebook (через взломанную учетную запись), которые направляли людей на подозрительные и мошеннические веб-сайты; а также данные, позволяющие установить личность (PII), такие как электронные письма, имена и номера телефонов жертв биткойн-мошенничества.

Исследователи заявили, что для подтверждения того, что база данных является действующей и реальной, они ввели поддельные учетные данные для входа на одну из мошеннических веб-страниц и подтвердили, что они были записаны.

На следующий день после того, как они обнаружили базу данных, исследователи полагают, что она подверглась продолжающейся широкомасштабной кибератаке Meow, в результате которой были полностью уничтожены все ее данные. Атака Meow - это продолжающиеся атаки, которые начались ранее в июле и привели к безвозвратному удалению 1000 незащищенных баз данных. По словам исследователя Боба Дьяченко, в результате атаки слово «мяу» стало его единственной визитной карточкой. Хакеры Meow также недавно атаковали сервер Mailfire, который был неправильно настроен и оставлен открытым.

«База данных отключилась в тот же день и больше не была доступна», - сказали исследователи. «Мы считаем, что мошенники сделали это после атаки Meow, но не можем подтвердить».

Мошенничество

Глобальная афера, нацеленная на пользователей Facebook, начинается с сети веб-сайтов, принадлежащих мошенникам, которые обманом заставляют пользователей Facebook предоставлять свои учетные данные, обещая, что они покажут цели список людей, которые недавно посещали их профили.

Неясно, как посетители попадали на эти сайты. Исследователи обнаружили 29 доменов, привязанных к этой сети; у веб-сайтов были такие имена, как: askviewer [.] com, capture-stalkers [.] com и followviewer [.] com.

Сайт сообщает жертвам: «За последние 2 дня на вашу страницу было 32 пользователя профиля! Продолжить просматривать свой список» и указывает им на кнопку с надписью «Открыть список!» Когда жертва нажимает кнопку, ее отправляют на поддельную страницу входа в Facebook, где ее просят ввести свои учетные данные. После этого появляется поддельная страница загрузки,

обещающая поделиться полным списком, и жертва перенаправляется на страницу Google Play для несвязанного аналитического приложения Facebook.

«В процессе мошенники сохранили имя пользователя и пароль жертвы Facebook в открытой базе данных для будущего использования в других своих преступных действиях», - заявили исследователи. «Они хранились в формате открытого текста, что позволяло любому, кто нашел базу данных, просмотреть, загрузить и украсть их».

Затем злоумышленники используют учетные данные жертв для следующего этапа атаки - захвата учетных записей и комментирования сообщений Facebook, опубликованных в сети жертв, со ссылками на другую сеть мошеннических веб-сайтов, принадлежащих мошенникам. Эти сайты относятся к схеме мошенничества с биткойнами. Когда друг жертвы в Facebook посещает один из сайтов, он получает указание зарегистрироваться для бесплатного торгового счета биткойнов и внести 295 долларов, чтобы начать торговлю.

«Включая ссылки на сайты с фальшивыми новостями, мошенники надеялись обойти и запутать инструменты Facebook для обнаружения мошенничества и ботов», - заявили исследователи. «Если бы взломанные учетные записи публиковали одни и те же ссылки на мошенничество с биткойнами снова и снова, они были бы быстро заблокированы социальной сетью».

Исследователи сказали пользователям Facebook, что если они считают, что стали жертвой мошенничества, немедленно изменить свои учетные данные.

«Кроме того, если вы повторно использовали свой пароль Facebook для любых других учетных записей, немедленно измените его, чтобы защитить их от взлома», - сказали исследователи. «Мы рекомендуем использовать генератор паролей для создания уникальных и надежных паролей для каждой вашей частной учетной записи и периодически их менять». ***(Lindsey O'Donnell. Exposed Database Reveals 100K+ Compromised Facebook Accounts // Threatpost (https://threatpost.com/exposed-database-100k-facebook-accounts/161247/). 16.11.2020).***

***

«Отчет о теневой экономике показывает, что злоумышленники предлагают облачные хранилища украденных данных, доступные с помощью удобных инструментов, позволяющих разрезать то, что предлагается.

Исследователи обнаружили, что киберпреступники используют облачные сервисы и технологии, чтобы ускорить свои атаки на организации и лучше монетизировать свои товары. Это в значительной степени обусловлено киберпреступниками, которые продают доступ к так называемым «облакам журналов», которые представляют собой кеши украденных учетных данных и других данных, размещенных в облаке.

Согласно Trend Micro, облачный подход делает информацию более доступной для заинтересованных покупателей, которые затем обращаются к ней и используют данные для проведения вторичных атак. Злоумышленники предлагают «облачные инструменты [покупателям] для анализа и извлечения данных, которые им необходимы для проведения [этих] дальнейших вредоносных действий», -

пояснила компания в опубликованном в понедельник сообщении, в котором разработка была охарактеризована как относительно новый подход.

Переход в облако для киберпреступников имеет то же главное преимущество, что и для законных организаций: скорость. Trend Micro заявила, что время между первоначальным кражей данных и использованием украденной информации против предприятия сократилось с недель до дней или даже часов, если применяется облачный подход.

«С внедрением облачных сервисов и технологий преступники могут гораздо быстрее воровать, покупать и использовать данные для проведения своих атак при нацеливании на организации», - говорят исследователи, используя аналогию со временем, которое нужно кому-то, чтобы купить их инструменты в гаражная распродажа по сравнению с покупкой их в интернет-магазине.

И с более быстрыми транзакциями в игре «организации не смогут предвидеть появление и быстрое выполнение таких атак - атак с использованием украденных данных и организованных преступниками за короткий промежуток времени, что оставляет им меньше времени для обнаружения и реагирования…»

Проблема больших данных

По словам исследователей, злоумышленники обращаются к облаку, чтобы более эффективно работать с огромным объемом данных, предлагаемых на подпольных форумах. По оценке Trend Micro, кеши представляют собой данные объемом в несколько терабайт.

«В последние годы наблюдается рост кражи учетных данных пользователей: злоумышленники собирают огромное количество учетных данных и связанных адресов электронной почты или доменных имен», - пояснили исследователи. «[Другие украденные данные] часто включают записанные нажатия клавиш, учетные данные для аутентификации на онлайн-порталах, онлайн-банках, аутентифицированные атрибуты сеанса, личную информацию (PII), сканированные документы, налоговые отчеты, счета-фактуры, платежные реквизиты банковского счета (например, кредитные карты), и больше."

Ситуацию усугубляет тот факт, что кража данных стала обязательной практикой практически для любого типа атак, включая программы-вымогатели, ботнеты, кейлоггеры, наборы эксплойтов и другие вредоносные компоненты.

«В дополнение к тому, что было упомянуто ранее, эта собранная информация может содержать историю просмотров, файлы cookie, нажатия клавиш, учетные данные пользователя, токены аутентификации, информацию о среде жертвы, которая может использоваться для обхода систем защиты от мошенничества, и многое другое», - сказали исследователи.

Все это означает, что у киберпреступников есть проблема с большими данными - опять же, как и у законных организаций. Трудно использовать весь потенциал такого колоссального количества данных без инструментов для их нарезки и нарезки кубиками.

Это проложило путь для бизнес-модели с оплатой за доступ, которая позволяет киберпреступникам лучше монетизировать свои незаконно полученные товары, позволяя другим злоумышленникам легко идентифицировать данные, которые им понадобятся, из облаков журналов продавцов для своих атак.

Плата за доступ в облачной экономике

По данным Trend Micro, клиенты платят за доступ к «облакам журналов» с помощью полезных облачных инструментов в различных ценовых диапазонах.

Пакеты, которые разрешают только ограниченный доступ и загрузки, стоят в пределах ста долларов. Также предлагаются ежемесячные тарифы на подписку, причем некоторые киберпреступники оценивают их в диапазоне от 300 до 1000 долларов в месяц.

«[Один актер] утверждает, что еженедельно обновляет свой набор данных, добавляя новые украденные аккаунты», - говорится в сообщении компании. «Услуга предлагает премиальную подписку за 300 долларов для первых четырех клиентов, а дополнительный доступ стоит 1000 долларов».

В другом случае реклама услуги гарантирует обновление новых пакетов данных в диапазоне от 20 000 до 30 000 журналов каждые одну-две недели. Ежемесячная подписка стоит 1000 долларов, а полугодовая подписка - 5000 долларов.

Данные могут быть разделены по стране или региону, типу данных, независимо от того, использовались ли журналы ранее в других кампаниях, названию или сектору организации-жертвы и другим параметрам.

«Преступникам нужно только искать те данные, которые им нужны, чтобы быстрее найти возможность совершить преступление; в конце концов, им больше не придется выполнять задачу по получению данных самостоятельно», - пояснили в компании.

По данным Trend Micro, преступники, покупающие доступ к этим наборам данных, также различаются по своей специализации.

«Некоторые из этих преступников в основном занимаются кардинговой деятельностью, в то время как другие специализируются на атаках на финансовые учреждения и поиске банковских реквизитов», - говорится в отчете. «Учетные данные для доступа к порталам облачной платформы также продаются тем преступникам, которые специализируются на продаже специализированных сервисов. Такие учетные данные могут быть использованы для создания экземпляров виртуальных машин, которые затем будут продаваться на подпольных рынках».

Как обсуждалось ранее, многие продавцы также ограничивают количество людей, которые могут получать доступ к журналам и покупать их. Они также применяют водяные знаки для данных и другие методы отслеживания для обеспечения соблюдения своих соглашений об уровне обслуживания (SLA).

«Среди этих ограничений - фиксированные расценки на общее количество объектов, к которым осуществляется доступ в день, ограничение на количество файлов, разрешенных для загрузки, или реализация политик формирования трафика», - сообщает Trend Micro. «Другие платформы также ограничивают доступ к облаку одним устройством для каждой учетной записи. Некоторым также требуются учетные данные частной VPN для инициирования доступа к услуге».

Будущее туманно

По мнению Trend Micro, с ростом бизнеса по продаже доступа к облакам журналов в будущем могут возникнуть различные схемы монетизации.

«Например, киберпреступники могут искать записи аутентифицированных пользовательских сеансов на облачных порталах», - пояснили в компании. «Если злоумышленник захватывает активный сеанс консоли у поставщика облачных услуг, он может получить полный контроль над облачными ресурсами жертвы. Это может означать получение доступа к существующим облачным системам и хранилищам. Затем актеры могли извлекать ценные данные из этих ресурсов, которые они, в свою очередь, могли извлечь и продать в подполье».

Исследователи также предполагают, что злоумышленники разработают инструменты на базе машинного обучения (ML) для ускорения процессов извлечения и анализа данных.

«Хотя на момент написания статьи мы видели только инструменты с ограниченными возможностями, мы считаем, что разработка инструментов на основе машинного обучения - тех, которые могут масштабировать гораздо большие наборы данных с более высокой скоростью - является следующим логическим шагом для преступников по мере развития рынка», отчет завершился». ***(Tara Seals. Cybercrime Moves to the Cloud to Accelerate Attacks Amid Data Glut // Threatpost (https://threatpost.com/cybercrime-cloud-accelerate-attacks-data-glut/161243/). 16.11.2020).***

***

«…The North Face сбросила пароли своих клиентов после того, как злоумышленники начали атаку с заполнением учетных данных на популярный веб-сайт внешнего поставщика оборудования.

В недавнем уведомлении об утечке данных компания сообщила клиентам, что 9 октября она была предупреждена о «необычной активности, связанной с ее веб-сайтом», thenorthface.com. Там клиенты могут покупать одежду и снаряжение в Интернете, создавать учетные записи и получать баллы лояльности. в рамках программы VIPeak Rewards. После дальнейшего расследования The North Face пришла к выводу, что злоумышленники предприняли атаку по подбору учетных данных на ее веб-сайт с 8 по 9 октября.

Заполнение учетных данных выполняется хакерами, которые используют людей, которые повторно используют одни и те же пароли для нескольких учетных записей в Интернете. Злоумышленники, заполняющие учетные данные, обычно используют идентификаторы и пароли, украденные из другого источника, например, взлома другой компании или веб-сайта, которые они затем пытаются использовать для входа в другие учетные записи, получая таким образом несанкционированный доступ. Этот процесс часто автоматизирован, и киберпреступники успешно использовали этот подход для кражи данных у различных популярных компаний, в том числе взломали магазин пончиков Dunkin ' (фактически два раза за три месяца).

«Основываясь на нашем расследовании, мы считаем, что злоумышленник ранее получил доступ к вашему адресу электронной почты и паролю из другого источника (не из The North Face) и впоследствии использовал те же учетные данные для доступа к вашей учетной записи на thenorthface.com», согласно данным уведомление о нарушении.

По данным StatSocial, North Face является лидером рынка верхней одежды и аксессуаров в США, получив в 2019 году более 2 миллиардов долларов из 4 миллиардов долларов годового дохода отрасли. The North Face не раскрывает, сколько клиентов пострадали от атаки., но он может быть значительным: по данным SimilarWeb, в октябре веб-сайт посетило 6,96 миллиона человек.

Threatpost обратился к The North Face за разъяснениями.

Помимо адресов электронной почты и паролей клиентов, киберпреступники могли получить доступ к информации, хранящейся в учетных записях клиентов на thenorthface.com. Сюда входят сведения о продуктах, которые были приобретены на веб-сайте компании, товарах, которые были сохранены в «избранном», а также платежные адреса клиентов, адреса доставки, общие баллы лояльности, настройки электронной почты, имя и фамилия, дни рождения и телефон. числа - все данные, готовые к злоупотреблениям, когда речь идет о разработке приемов социальной инженерии для фишинговых атак.

North Face не хранит копии данных платежных карт (включая кредитные, дебетовые карты или карты с сохраненной стоимостью) на thenorthface.com - это означает, что злоумышленники не могли просматривать номера платежных карт, даты истечения срока действия или CVV.

The North Face заявили, что, как только стало известно об инциденте, компания приняла меры, ограничивающие вход в учетную запись из подозрительных источников или из подозрительных шаблонов.

«В качестве дополнительной меры предосторожности мы отключили все пароли от учетных записей, к которым осуществлялся доступ во время атаки», - заявили в компании. «Мы также удалили все токены платежных карт со всех аккаунтов на thenorthface.com. Таким образом, вам нужно будет создать новый (уникальный) пароль и снова ввести данные своей платежной карты в следующий раз, когда вы будете делать покупки на thenorthface.com».

Поскольку многие потребители повторно используют свои пароли, атаки с заполнением учетных данных продолжают оставаться популярным способом доступа киберпреступников к учетным записям жертв. Например, в октябре посетители популярной сети закусочных Nando’s увидели, как с их банковских счетов были выведены сотни долларов после того, как киберпреступники смогли получить доступ к их учетным данным для заказа в ресторане. А ранее в феврале официальный аккаунт ФК Барселона в Твиттере был взломан в результате очевидной атаки с использованием учетных данных.

The North Face призвала клиентов использовать уникальные пароли и не повторять их вообще.

«Атаки с заполнением учетных данных могут происходить, когда люди используют одни и те же учетные данные для аутентификации на нескольких веб-сайтах, поэтому мы рекомендуем вам использовать уникальный пароль на thenorthface.com», - заявили в компании». ***(Lindsey O'Donnell. Credential-Stuffing Attack Hits The North Face // Threatpost (https://threatpost.com/credential-stuffing-attack-north-face/161190/). 13.11.2020).***

***

«Bleeping Computer сообщает, что в минувшие выходные на хакерском форуме выставили на продажу базу данных популярного фотобанка 123rf, содержащую около 8 300 000 записей. Продавец заявляет, что дамп был сделан в 2020 году.

Журналисты изучили опубликованный хакерами образец данных и пишут, что финансовой информации дамп не содержит, однако там можно найти полное имя пользователя, адрес электронной почты, хешированные пароли (MD5), название компании, номер телефона, адрес, привязанный к PayPal email-адрес (если используется), а также IP-адрес.

Еще в начале текущей недели журналисты уведомили о своей находке компанию Inmagine Group, которой принадлежит 123rf, и получили ответ, что сервер в центре обработки данных действительно был взломан, и хакеры успели похитить данные пользователей. Компания уже проводит расследование случившегося вместе со специалистами из правоохранительных органов.

При этом в Inmagine Group говорят, что выставленный на продажу дамп – это не новейшая копия базы клиентов за 2020 год. Похоже, это правда, так как самые свежие образцы, изученные Bleeping Computer, были датированы 27 октября 2019 года.

Хотя в компании заявили, что все пароли клиентов были зашифрованы, речь, очевидно, идет про MD5, то есть взлом таких паролей, к сожалению, не доставит злоумышленникам особенных проблем». ***(Мария Нефёдова. Крупный фотобанк 123rf пострадал от утечки данных. Хакеры продают информацию 8,3 млн пользователей // Xakep (https://xakep.ru/2020/11/13/123rf-hack/). 13.11.2020).***

***

«На этой неделе британский сервис потоковой передачи музыки Last.fm исправил проблему с утечкой учетных данных, из-за которой были обнаружены имя пользователя и пароль администратора.

Утечка произошла из-за неправильно настроенного приложения PHP Symfony, работающего в режиме «отладки» и открывающего журналы профилировщика.

С этими учетными данными злоумышленник мог получить доступ и изменить данные учетной записи пользователя Last.fm.

Веб-приложение Last.fm работало в режиме «отладки»

На прошлой неделе исследователи SecurityDiscovery.com Себастьян «Себ» Каул и Боб Дьяченко обнаружили веб-приложение, работающее в режиме «отладки».

Веб-приложение принадлежало Last.fm, принадлежащему CBS , бесплатному онлайн-сервису потоковой передачи музыки.

При работе в режиме отладки приложения предоставляют данные, которые должны оставаться скрытыми от общего просмотра, чтобы облегчить разработчикам устранение неполадок.

Дьяченко сказал, что неправильно сконфигурированное приложение Symfony, обнаруженное Каулом, открывало «страницу PHPinfo и журналы профилировщика с учетными данными».

В случае неправильного использования эти утекшие учетные данные позволили бы злоумышленникам запрашивать у каждого пользователя Last.fm важную информацию.

Присмотревшись к приложению, исследователи заметили, что журналы Symfony Profiler Last.fm раскрывают имена пользователей, пароли и секретные токены нескольких администраторов, как показано ниже на скриншоте, предоставленном BleepingComputer.

«Насколько мы поняли, это была часть административной панели, позволяющая [пользователям] просматривать и редактировать информацию и детали учетной записи пользователей Last.fm», - сказал Дьяченко BleepingComputer.

Во время нашего тестирования BleepingComputer обнаружил уязвимые конечные точки, и панель администратора больше не была доступна.

Исследователи обнаружили утечку через поисковую систему IoT

Кауль и Дьяченко заметили неверно настроенное веб-приложение Last.fm в ходе своих обычных исследований.

«Сейчас мы изучаем неправильно настроенные приложения Sympfony и снимаем с них отпечатки пальцев с помощью поисковых систем IoT. В ходе этого исследования были обнаружены экземпляры CBSi», - сказал Дьяченко BleepingComputer.

На прошлой неделе Дьяченко попросил всех помочь в определении ключевого человека в CBS Interactive, сообщившего об этой проблеме безопасности.

BleepingComputer обратился за комментариями к Last.fm и CBS Interactive, но мы еще не получили ответа.

Хотя теперь проблема, похоже, устранена, она создает прецедент для развертывания приложений в производственных средах.

Если не закрепить должным образом, поисковая система IoT может в конечном итоге проиндексировать уязвимые конечные точки для всеобщего обозрения.

Ранее в этом году хакеры, стоящие за атакой Meow, стерли почти 4000 баз данных MongoDB, обнаруженных через поисковые системы IoT.

Злоумышленники также угрожают вымогательством при обнаружении таким образом незащищенных систем.

В идеале при развертывании приложений в производственной среде следует отключить режим отладки, чтобы предотвратить любую потенциальную утечку конфиденциальных данных.

Кроме того, поиск в поисковых системах Интернета вещей для IP-адресов вашей компании может помочь выявить утечки, требующие срочного внимания». ***(Ax Sharma. CBS Last.fm fixes admin password leakage via Symfony profiler // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/cbs-lastfm-fixes-admin-password-leakage-via-symfony-profiler/). 27.11.2020).***

***

«Мошенники пытаются украсть учетные данные электронной почты у сотрудников, выдавая себя за отдел кадров своей организации в фишинговых письмах, замаскированных под внутренние служебные записки компании.

Согласно статистике, предоставленной исследователями компании Abnormal Security, занимающейся безопасностью электронной почты, которая обнаружила эту фишинговую кампанию, этим фишинговым сообщениям удалось попасть в почтовые ящики тысяч целевых лиц после обхода защиты электронной почты G Suite.

Существует высокая вероятность того, что некоторые из целей попадут на удары мошенников, учитывая, что во время пандемии COVID-19 в этом году большинство компаний регулярно отправляли своим сотрудникам по электронной почте обновления, касающиеся изменений политики удаленной работы.

Бланки соответствия кадровым требованиям

Фишинговые электронные письма, доставляемые в рамках этой кампании, подделывают почтовый сервис компании жертвы и выглядят как автоматические внутренние служебные записки с прикрепленными голосовыми сообщениями.

Эта тактика используется, чтобы убедить цель в том, что сообщения исходят от ее собственной компании, что повысит вероятность того, что они поделятся конфиденциальной информацией, когда ее спросят на более поздних этапах атаки.

К электронным письмам прилагаются пользовательские HTML-вложения с именами каждого сотрудника, метод, разработанный для того, чтобы убедить получателей в безопасности электронного письма, чтобы они открывали вложение, не задумываясь.

После открытия вложений целевые объекты отправляются в документ Sharepoint с подробностями об изменениях политики удаленной работы и ссылкой подтверждения внизу.

Щелчок по этой ссылке перенаправит их на фишинговую целевую страницу, замаскированную под уведомление о соответствии кадрового законодательства, требующее от целей ввести адрес электронной почты и пароль своей компании.

Дополнительная тактика, используемая для того, чтобы убедиться, что жертвы предоставят свои учетные данные электронной почты, - это добавление предупреждения под формой фишинга, в котором говорится, что они никогда не сообщают свои пароли людям, которым они не доверяют.

«Если получатели станут жертвами этой атаки, учетные данные для входа в их учетную запись электронной почты будут скомпрометированы, и злоумышленники получат доступ к конфиденциальной корпоративной и личной информации», - пояснил Abnormal Security.

«Эта атака отражает растущую озабоченность по поводу протоколов безопасности компании во время пандемии COVID-19», - добавили исследователи.

«Это электронное письмо устанавливает короткий срок, когда сотрудники должны подтвердить, что они получили это сообщение, и заполнить форму».

В ходе недавней фишинг-кампании, обнаруженной теми же исследователями в начале этого месяца, мошенники выдавали себя за Налоговую службу США (IRS), пытаясь обманом заставить жертв выплатить сфабрикованные

невыплаченные суммы, связанные с пропущенными или просроченными платежами.

Целям также пригрозили отчетами кредитного бюро и судебными исками, чтобы еще больше увеличить размер сдачи, которую они уступят и заплатят мошенникам.

В настоящее время проводится масштабная фишинговая кампания Zoom, нацеленная на встречи в День благодарения, что позволило злоумышленникам уже украсть учетные данные тысяч пользователей». ***(Sergiu Gatlan. Phishing lures employees with fake 'back to work' internal memos // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/phishing-lures-employees-with-fake-back-to-work-internal-memos/). 27.11.2020).***

***

«Довольно сложная фишинговая схема для кражи учетных данных Office 365 у малых и средних предприятий в США и Австралии объединяет облачные сервисы от Oracle и Amazon в свою инфраструктуру.

Кампания действует более полугода и использует сеть законных веб-сайтов, которые были скомпрометированы для работы в качестве прокси-цепочки.

Простая приманка

Операторы заманивают получателей поддельными уведомлениями о голосовых сообщениях и приглашениями Zoom, которые в конечном итоге приводят жертву на фишинговую страницу, собирающую учетные данные для входа.

Компания по кибербезопасности Mitiga заявляет, что, несмотря на простую приманку и цель, кампания выделяется столь же изощренной, как и путь к утечке через законные сервисы и веб-сайты.

Согласно их исследованию, злоумышленник отправляет фишинговые сообщения со скомпрометированных учетных записей электронной почты и использует Amazon Web Services (AWS) и Oracle Cloud в цепочке перенаправления…

Перенаправить поток

Затем жертвы перенаправляются на взломанный веб-сайт, который переводит их на поддельную страницу Office 365, размещенную в основном в сервисе Oracle Cloud Computing.

В некоторых случаях актер использовал Amazon Simple Storage Service (Amazon S3). Учетные данные, введенные на этой странице, автоматически доставляются на другой взломанный веб-сайт.

Mitiga говорит, что они выявили более 40 взломанных веб-сайтов, которые были частью этой фишинг-кампании Office 365.

Подсказки указывают на фишинг как на услугу

Подсказки, обнаруженные в HTML-коде поддельных страниц Office 365, позволяют предположить, что эта инфраструктура является частью бизнеса, предлагающего фишинг как услугу, арендуемого для нескольких клиентов.

Доказательством этого являются прокомментированные инструкции, такие как «// Установить ссылку здесь», и небольшие различия в переменных, именах

функций или взломанных сайтах, получивших украденные учетные данные, которые могут указывать на то, что несколько сторон используют одну и ту же инфраструктуру.

Исследователи также обнаружили ссылки на некоторые регионы Азии, такие как Гагал (Иран), Куранг (Индия) и Косонг (Северная Корея), а также индонезийские слова («томбол» - кнопка, «текан» - пресс, «колом»). - столбик, «кирим» - отправить).

Они могут намекать на операторов, занимающихся фишингом как услугу, или их клиентов. Однако это также могут быть ложные флаги, введенные в заблуждение исследователей.

Из проанализированных адресов электронной почты Митига определил, что целями этой фишинг-операции являются в основном руководители высшего звена малых и средних предприятий, а также крупных финансовых учреждений.

Mitiga дает следующие рекомендации, чтобы не стать жертвой этих атак:

Включить двухфакторную аутентификацию (2FA) для входа в Office 365

Принудительное обновление паролей Office 365

Изучите правила пересылки в учетных записях электронной почты

Поиск скрытых папок в почтовых ящиках и сообщениях в другом месте, чем обычно

Регистрировать изменения в логине и настройках почтового ящика и хранить данные не менее 90 дней.

Включите оповещения о подозрительной активности, такой как необычный вход в систему, и анализируйте журналы сервера на предмет аномального доступа к электронной почте.

Рассмотрите возможность моделирования аналогичного сценария атаки с помощью красной команды, чтобы проверить осведомленность организации о фишинге». ***(Ionut Ilascu. Office 365 phishing abuses Oracle and Amazon cloud services // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/office-365-phishing-abuses-oracle-and-amazon-cloud-services/). 27.11.2020).***

***

«Британская компания по кибербезопасности и оборудованию Sophos разослала по электронной почте небольшой группе клиентов, чтобы предупредить их о том, что их личная информация была раскрыта после нарушения безопасности, обнаруженного во вторник.

Раскрытые данные о клиентах были доступны неавторизованным сторонам из-за неправильно настроенного «инструмента», используемого компанией для хранения информации пользователями, которые обратились в службу поддержки компании.

Затронуто лишь небольшое количество клиентов

«24 ноября 2020 года Sophos была уведомлена о проблеме с разрешением доступа в инструменте, используемом для хранения информации о клиентах, которые обратились в службу поддержки Sophos», - говорится в сообщении компании.

«В результате были обнаружены некоторые данные от небольшой группы клиентов Sophos. Мы быстро исправили проблему».

Компания Sophos не предоставила никакой информации о том, кто обнаружил и раскрыл незащищенное хранилище, или о точном количестве клиентов, чьи личные данные были раскрыты из-за этого нарушения безопасности.

Доступные данные включают имена и фамилии клиентов, адреса электронной почты и их контактные номера телефонов, если они были предоставлены службе поддержки Sophos.

Компания также заявила, что информация о поддержке клиентов больше не предоставляется после принятия мер по исправлению положения, чтобы остановить раскрытие данных.

«В Sophos конфиденциальность и безопасность клиентов всегда являются нашим приоритетом», - добавила компания, занимающаяся кибербезопасностью. «Мы связываемся со всеми затронутыми клиентами».

«Кроме того, мы принимаем дополнительные меры для обеспечения постоянной безопасности настроек разрешений доступа»…». ***(Sergiu Gatlan. Sophos alerts customers of info exposure after security breach // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/sophos-alerts-customers-of-info-exposure-after-security-breach/). 26.11.2020).***

***

«Хакеры пытались получить доступ к учетным записям Spotify, используя базу данных из 380 миллионов записей с учетными данными и личной информацией, собранной из различных источников.

В течение многих лет пользователи жаловались, что их учетные записи Spotify были взломаны после смены паролей, в их профилях появлялись новые плейлисты или в их семейные учетные записи добавлялись незнакомцы из других стран.

Новый отчет, в котором подробно описывается, как база данных, содержащая более 380 миллионов записей, включая учетные данные, активно используется для взлома учетных записей Spotify, может пролить свет на эти взломы учетных записей.

300 миллионов записей с информацией о пользователях для взлома учетных записей Spotify

Распространенная атака, используемая для взлома учетных записей, называется атакой с заполнением учетных данных, когда злоумышленники используют большие коллекции комбинаций имени пользователя и пароля, которые были просочились в предыдущие нарушения безопасности, чтобы получить доступ к учетным записям пользователей на других онлайн-платформах.

Сегодня VPNMentor выпустил отчет о базе данных, размещенной в Интернете, которая содержала 300 миллионов комбинаций имен пользователей и паролей, используемых в атаках с заполнением учетных данных против Spotify.

Каждая запись в этой базе данных содержит имя для входа (адрес электронной почты), пароль и информацию о том, могут ли учетные данные успешно войти в учетную запись Spotify…

Неизвестно, как были собраны 300 миллионов записей, но, скорее всего, это связано с утечкой данных или большими «коллекциями» учетных данных, которые обычно бесплатно предоставляются злоумышленниками.

Исследователи считают, что 300 миллионов записей, перечисленных в базе данных, позволили злоумышленникам взломать от 300 000 до 350 000 учетных записей Spotify.

VPNMentor связался со Spotify 9 июля 2020 года по поводу обнаруженной базы данных и ее угрозы для учетных записей и получил ответ в тот же день.

«В ответ на наш запрос Spotify инициировал «непрерывный сброс» паролей для всех затронутых пользователей. В результате информация в базе данных будет аннулирована и станет бесполезной», - заявили исследователи.

Для тех пользователей, чьи учетные записи были скомпрометированы, Spotify выполнил сброс пароля в июле.

Spotify не поддерживает многофакторную аутентификацию, что значительно повысило бы безопасность учетных записей, даже если пользователи запрашивали ее в течение некоторого времени». ***(Lawrence Abrams. Over 300K Spotify accounts hacked in credential stuffing attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/over-300k-spotify-accounts-hacked-in-credential-stuffing-attack/). 23.11.2020).***

***

«Хакер просочил учетные данные почти 50 000 уязвимых VPN-сервисов Fortinet.

Как сообщает BleepingComputer, на выходных хакер опубликовал список однострочных эксплойтов для CVE-2018-13379 с целью кражи учетных данных VPN с этих устройств.

В списке уязвимых целей присутствуют IP-адреса крупных банков, телекоммуникационных компаний и государственных организаций со всего мира.

Просочившиеся файлы раскрывают имена пользователей, пароли, немаскированные IP-адреса

Использование критической уязвимости FortiOS CVE-2018-13379 позволяет злоумышленнику получить доступ к конфиденциальным файлам «sslvpn_websession» из VPN-сервисов Fortinet.

Эти файлы содержат информацию, относящуюся к сеансу, но, что наиболее важно, могут раскрывать имена и пароли пользователей Fortinet VPN в виде обычного текста.

Сегодня аналитик по анализу угроз Bank_Security нашел еще одну ветку на хакерском форуме, где злоумышленник поделился дампом данных, содержащим файлы «sslvpn_websession» для каждого IP-адреса, который был в списке.

По наблюдениям BleepingComputer, эти файлы раскрывают имена пользователей, пароли, уровни доступа (например, «полный доступ») и исходные немаскированные IP-адреса пользователей, подключенных к VPN.

Новый набор данных, размещенный на форуме, представляет собой просто архив RAR размером 36 МБ, но при распаковке он расширяется более чем на 7 ГБ на момент нашего тестирования.

Раскрытие паролей в этих файлах означает, что даже если уязвимые VPN Fortinet позже будут исправлены, эти учетные данные могут быть повторно использованы любым лицом, имеющим доступ к дампу в атаках с заполнением учетных данных, или для восстановления доступа к этим VPN.

Хотя мотивы злоумышленника для этой второй обширной утечки не ясны, BleepingComputer действительно заметил, что в недавно просочившемся архиве есть списки с пометкой pak, отделяющие пакистанские IP-адреса VPN и соответствующие файлы sslvpn_websession из большого набора данных из 49 000+ VPN.

Дополнительно прилагается файл изображения с названием «f ** k israel.jpg», который представляет собой плакат Адольфа Гитлера «Да, мы можем», созданный в стиле плаката президентской кампании Обамы 2008 года.

Что еще хуже, дамп учетных данных репостится на других форумах и в чатах.

Fortinet неоднократно пыталась предупредить клиентов

На этой неделе Fortinet сообщил BleepingComputer, что с момента публичного раскрытия критической уязвимости обхода пути (CVE-2018-13379) в прошлом году компания неоднократно предупреждала своих клиентов, призывая их исправить уязвимые экземпляры FortiOS.

«Безопасность наших клиентов - наш главный приоритет. В мае 2019 года Fortinet выпустила рекомендацию PSIRT относительно устраненной уязвимости SSL, а также напрямую связалась с клиентами и снова через сообщения в корпоративных блогах в августе 2019 и июле 2020 года, настоятельно рекомендуя обновление ", - сообщил BleepingComputer представитель Fortinet.

Несмотря на эти меры, критическая ошибка широко использовалась в дикой природе из-за отсутствия исправлений.

Как сообщает BleepingComputer, этот же недостаток был использован злоумышленниками для взлома системы поддержки выборов правительства США.

Ранее в этом году злоумышленники из национальных государств использовали эту уязвимость для взлома сетей и развертывания программ-вымогателей.

«На прошлой неделе мы связались со всеми клиентами, снова уведомив их об уязвимости и мерах по ее устранению. Хотя мы не можем подтвердить, что векторы атак для этой группы происходили через эту уязвимость, мы продолжаем призывать клиентов выполнить обновление и Чтобы получить дополнительную информацию, посетите наш обновленный блог и сразу же ознакомьтесь с рекомендациями [PSIRT] за май 2019 г. », - заключил Fortinet.

Поэтому сетевым администраторам и специалистам по безопасности рекомендуется немедленно исправить эту серьезную уязвимость.

В качестве меры предосторожности пользователи Fortinet VPN должны немедленно изменить свои пароли как на устройствах VPN, так и на любых других веб-сайтах, где использовались те же учетные данные». ***(Ax Sharma. Passwords exposed for almost 50,000 vulnerable Fortinet VPNs // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/passwords-exposed-for-almost-50-000-vulnerable-fortinet-vpns/). 25.11.2020).***

***

«Производитель сетевых устройств Belden подвергся кибератаке, которая позволила злоумышленникам украсть файлы, содержащие информацию о сотрудниках и деловых партнерах.

Belden - американский производитель устройств для подключения к сети, включая маршрутизаторы, межсетевые экраны, коммутаторы, кабели и соединители. Выручка Belden в 2019 году составила 2,5 миллиарда долларов, в компании работает около 9000 человек.

В раскрытии «инцидента с данными» Belden заявляет, что недавно они подверглись кибератаке, которая позволила хакерам украсть данные компании.

«Компания Belden Inc. (NYSE: BDC), ведущий мировой поставщик специализированных сетевых решений, объявила сегодня о принятии решительных мер по расследованию и устранению инцидентов с данными, связанных с несанкционированным доступом и копированием некоторых данных нынешних и бывших сотрудников, а также "Ограниченная информация компании относительно некоторых деловых партнеров", - объявил Белден.

Далее в заявлении говорится, что Belden подвергся «сложной атаке со стороны стороны, не входящей в Компанию, которая получила доступ к ограниченному количеству файловых серверов Компании».

Belden не предоставил подробностей о кибератаке, но фраза «изощренная атака» теперь обычно используется юристами для описания атаки вымогателя при составлении уведомлений о раскрытии информации…». ***(Lawrence Abrams. Belden networking giant's company data stolen in cyberattack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/belden-networking-giants-company-data-stolen-in-cyberattack/). 25.11.2020).***

***

«Приложение для проведения мероприятий Peatix на этой неделе обнаружило утечку данных после того, как, как сообщается, информация об учетной записи пользователя начала распространяться в Instagram и Telegram.

Приложение для обнаружения событий Peatix обнаружило утечку данных после того, как, как сообщается, в Instagram и Telegram распространялась реклама украденной информации об учетных записях пользователей.

В уведомлении об утечке данных для затронутых пользователей Peatix сообщила, что 9 ноября стало известно, что к данным учетной записи пользователя был произведен неправильный доступ. В ходе дальнейшего расследования компания обнаружила, что имена пользователей, адреса электронной почты, соленые и хешированные пароли, псевдонимы, предпочтительные языки, страны и часовые пояса были скомпрометированы.

«В рамках наших немедленных мер по восстановлению мы заблокировали несанкционированный доступ к базе данных и продолжаем расследование с

помощью внешних фирм по обеспечению безопасности», - говорится в уведомлении об утечке данных.

Peatix - это приложение для мероприятий, которое связывает людей с различными событиями и социальными сообществами. С момента своего первого запуска в 2011 году приложение выросло и обслуживает более 50 000 групп интересов по всему миру - с базой пользователей 5 миллионов. Неясно, сколько из этих пользователей пострадали от утечки данных или как изначально произошло нарушение; Threatpost обратился к Peatix за дополнительной информацией.

Хотя Peatix использует платежные процессоры, такие как PayPal и Stripe, для управления пользовательскими платежами, полные данные кредитной карты не хранятся в их базах данных, и Peatix сказал, что нет никаких доказательств того, что эта информация была скомпрометирована.

«Кроме того, на основании проведенного на сегодняшний день расследования у нас нет оснований полагать, что были получены какие-либо исторические данные о событиях, в которых участвовали пользователи, какие-либо данные, полученные с помощью нашей функции анкетирования, или адреса или номера телефонов пользователей», - говорится в сообщении службы безопасности. консультативный.

Хотя пароли были получены, компания подчеркнула, что использует систему зашифрованных паролей, в которой пароли пользователей хранятся в виде хеш-значений, а не паролей в виде простого текста. Тем не менее, Peatix призвал пользователей сбросить свои пароли «в качестве дополнительной меры предосторожности» и следить за подозрительной перепиской с запросом дополнительной личной информации.

Однако эксперты по безопасности, такие как Роберт Пригге, генеральный директор Jumio, не считают, что этого достаточно.

«Реакции Peatix на сброс паролей просто недостаточно, чтобы защитить их… учетные записи пользователей», - сказал Пригге в электронном письме. «Вместо этого онлайн-организации должны обратиться к более безопасной и безопасной альтернативе, такой как биометрическая аутентификация (использование уникальных человеческих качеств человека для проверки личности), которая подтвердит, что авторизованный пользователь входит в систему, обеспечивая защиту личных данных от киберпреступников и данных. брокеры-нарушители».

Компания предупредила, что злоумышленники могут использовать украденную информацию, чтобы связаться с затронутыми пользователями и попытаться собрать дополнительную личную или финансовую информацию с помощью фишинговых атак. Другие потенциальные векторы атак включают атаки с заполнением учетных данных и атаки с использованием пароля.

«Они могут утверждать, что они Peatix, или отправлять электронные письма, якобы от Peatix», - заявили в компании. «Они также могут попытаться получить доступ к вашей учетной записи Peatix или другим веб-сайтам и приложениям, на которых вы используете те же пароли».

По данным ZDNet, вскоре после того, как произошла утечка данных, скомпрометированные данные были обнаружены в рекламе, размещенной в историях Instagram, каналах Telegram и различных хакерских форумах.

«Обычно, когда мы слышим о хакерах, предлагающих украденные данные, это происходит на форумах или страницах в глубокой сети», - сказал по электронной почте Борис Сипот, старший инженер по продажам Synopsys Software Integrity Group. «Однако в этом случае мы также видим использование социальных сетей, таких как Instagram и приложение для обмена сообщениями Telegram, для продвижения украденных имен, имен пользователей, хешированных паролей и адресов электронной почты»…». ***(Lindsey O'Donnell. Post-Breach, Peatix Data Reportedly Found on Instagram, Telegram // Threatpost (https://threatpost.com/breach-peatix-data-instagram-telegram/161560/). 24.11.2020).***

***

«Популярный британский футбольный клуб подтвердил факт нападения, но сказал, что личные данные болельщиков остаются в безопасности.

Футбольный клуб «Манчестер Юнайтед» в Великобритании подтвердил, что команда стала жертвой кибератаки на его системы.

Man U., одна из самых популярных футбольных команд в мире, заявила, что она постоянно страдает от сбоев в работе ИТ. «Клуб принял быстрые меры по сдерживанию атаки и в настоящее время работает с экспертами-консультантами для расследования инцидента и минимизации продолжающихся сбоев в работе ИТ», - говорится в коротком заявлении, опубликованном в пятницу вечером. «У клуба есть обширные протоколы и процедуры для такого мероприятия, и он отрепетировал этот риск. Наша киберзащита определила атаку и отключила затронутые системы, чтобы ограничить ущерб и защитить данные».

Команда сообщила только, что атака была «изощренной операцией организованных киберпреступников», но другие детали скудны относительно того, в чем она участвовала - будь то программа-вымогатель или что-то еще. Футбольный джаггернаут действительно заявил, что личные данные, связанные с фанатами или клиентами, не были взломаны.

Он также сказал, что его общедоступные системы - веб-сайт клуба, мобильное приложение и каналы в социальных сетях - не пострадали, и что никаких перерывов в игре не ожидается.

«Все критически важные системы, необходимые для проведения матчей на «Олд Траффорд», остаются безопасными и работоспособными», - заявили в клубе. Субботний матч против «Вест Бромвич Альбион» прошел по плану.

«Кибератака на «Манчестер Юнайтед» вызывает тревогу, но определенно не будет последней в своем роде, - сказал Дэниел Норман, старший аналитик по решениям в Форуме информационной безопасности. «Многие хакеры рассматривают кибератаки как игру, целью которой являются организации. Родословная этого нападения не более известна, чем одно из самых громких имен в спорте. Неудивительно, что этот гигант спортивного мира стал мишенью».

Согласно заявлению Man U., его архитектура киберзащиты сработала, позволив ему предпринять согласованные действия, сказал Threatpost Дирк Шрейдер, глобальный вице-президент New Net Technologies (NNT). «Судя по тому, что известно до сих пор, это кажется быстрым и скоординированным ответом», -

сказал он. «Они обнаружили инцидент, у них были разработаны процедуры для такого типа инцидентов, которые охватывали не только технические меры, но также внутренние и внешние коммуникации и призыв к экспертам принять участие»…». ***(Tara Seals. Manchester United: IT Systems Disrupted in Cyberattack // Threatpost (https://threatpost.com/manchester-united-disrupted-cyberattack/161488/). 23.11.2020).***

***

«В настоящее время злоумышленник продает пароли для учетных записей электронной почты сотен руководителей высшего звена компаний по всему миру.

Данные продаются по замкнутому доступу подпольного форума для русскоязычных хакеров под названием Exploit.in…

Злоумышленник продает комбинации адресов электронной почты и паролей для учетных записей Office 365 и Microsoft, которые, как он утверждает, принадлежат руководителям высокого уровня, выполняющим такие функции, как:

CEO - генеральный директор

COO - главный операционный директор

Финансовый директор - финансовый директор или главный финансовый контролер

CMO - директор по маркетингу

CTOs - технический директор

Президент

Заместитель президента

Помощник руководителя

Финансовый менеджер

Бухгалтер

Директор

Финансовый директор

Финансовый контролер

Счета к оплате

Доступ к любой из этих учетных записей продается по цене от 100 до 1500 долларов, в зависимости от размера компании и роли пользователя.

Источник в сообществе кибербезопасности, согласившийся связаться с продавцом для получения образцов, подтвердил достоверность данных и получил действительные учетные данные для двух учетных записей, генерального директора американской компании по разработке программного обеспечения среднего размера и финансового директора одной из стран ЕС. сеть розничных магазинов.

Источник, который попросил ZDNet не использовать его имя, находится в процессе уведомления двух компаний, а также двух других компаний, для которых продавец опубликовал пароли учетных записей в качестве публичного доказательства того, что у них есть действительные данные для продажи.

Это были данные для входа в систему для руководителя британского консалтингового агентства по управлению бизнесом и президента американского производителя одежды и аксессуаров.

Продавец отказался сообщить, как он получил учетные данные для входа, но сказал, что у него есть еще сотни на продажу.

Согласно данным, предоставленным компанией KELA, занимающейся разведкой угроз, тот же злоумышленник ранее проявлял интерес к покупке «журналов Azor», термин, который относится к данным, собранным с компьютеров, зараженных троянской программой AzorUlt info- stealer.

Журналы Infostealer почти всегда содержат имена пользователей и пароли, которые троян извлекает из браузеров, установленных на зараженных хостах.

Эти данные часто собирают операторы инфостилеров, которые фильтруют и систематизируют их, а затем выставляют на продажу на специализированных рынках, таких как Genesis, на хакерских форумах или продают другим бандам киберпреступников.

«Взломанные учетные данные корпоративной электронной почты могут быть ценными для киберпреступников, поскольку их можно монетизировать разными способами», - сказал ZDNet менеджер по продукту KELA Равид Лаэб.

«Злоумышленники могут использовать их для внутренних коммуникаций в рамках« мошенничества с генеральным директором », когда преступники манипулируют сотрудниками, переводя им большие суммы денег; они могут использоваться для доступа к конфиденциальной информации в рамках схемы вымогательства; или эти учетные данные также могут быть использованы для получения доступа к другим внутренним системам, для которых требуется двухфакторная аутентификация на основе электронной почты, чтобы перемещаться в организации и осуществлять сетевое вторжение », - добавил Лаэб.

Но, скорее всего, скомпрометированные электронные письма будут куплены и использованы для мошенничества генерального директора, также известного как мошенничество BEC. Согласно отчету ФБР в этом году, мошенничество с BEC было, безусловно, самой популярной формой киберпреступности в 2019 году, составив половину потерь от киберпреступлений, зарегистрированных в прошлом году.

Самый простой способ предотвратить монетизацию хакерами украденных учетных данных любого типа - это использовать двухэтапную проверку (2SV) или двухфакторную аутентификацию (2FA) для ваших учетных записей в Интернете. Даже если хакерам удастся украсть данные для входа, они будут бесполезны без надлежащего дополнительного верификатора 2SV / 2FA». ***(Catalin Cimpanu. A hacker is selling access to the email accounts of hundreds of C-level executives // Zero Day (https://www.zdnet.com/article/a-hacker-is-selling-access-to-the-email-accounts-of-hundreds-of-c-level-executives/). 27.11.2020).***

***

«Комиссия по защите персональной информации Южной Кореи оштрафовала компания Facebook на 6,7 млрд южнокорейских вон ($6,06 млн)

и потребовала возбуждения уголовного дела за предоставление личной информации пользователей без их согласия другим операторам…

Как показали результаты расследования, личная информация по меньшей мере 3,3 млн пользователей Facebook в Корее была предоставлена другим компаниям в период с мая 2012 года по июнь 2018 года.

Как утверждается, были переданы имена людей, адреса, даты рождения, сведения об опыте работы и другие данные. По словам агентства, соцсеть могла поделиться этой информацией с «10 тыс. других компаний».

Комиссия также отдельно оштрафовала Facebook за отказ сотрудничать с властями. Как утверждает надзорный орган, компания передала недостоверные документы о своей работе. Сумма штрафа составила 66 млн вон ($59 тыс.).» ***(Власти Южной Кореи оштрафовали Facebook на $6 млн за разглашение информации // SecurityLab.ru (https://www.securitylab.ru/news/514353.php). 25.11.2020).***

***

«В приложениях Baidu Maps и Baidu Search Box обнаружена проблема, связанная со сбором конфиденциальных данных.

Как сообщили специалисты из американской фирмы Palo Alto Networks, приложения Baidu Maps и Baidu Search Box содержали код, собирающий информацию о пользователях. Код был обнаружен в Baidu Push SDK, который используется для отображения уведомлений в реальном времени внутри обоих приложений. Код позволял программах собирать информацию о модели телефона, MAC-адресе, операторе связи и номере IMSI (International Mobile Subscriber Identity).

По словам экспертов, хотя часть собранной информации была «довольно безвредной», некоторые данные, такие как IMSI-код, «могут использоваться для однозначной идентификации и отслеживания пользователя, даже если этот пользователь меняет телефон».

Представитель Baidu отметил, что хотя сбор данных и вызвал расследование со стороны команды Google, это не было причиной удаления приложений из магазина Google Play в октябре нынешнего года, поскольку китайская компания получила разрешение от пользователей собирать подобную информацию.

Тем не менее, исследователи безопасности также обнаружили и другие проблемы, над решением которых в настоящее время работает Baidu. Как заявили в компании, приложение Baidu Maps также вернется в магазин после того, как разработчики Baidu исправят обнаруженные проблемы.

Аналогичный код для сбора данных был обнаружен в ShareSDK, разработанном китайским гигантом рекламных технологий MobTech. SDK, используемый более чем 37 500 приложениями, также позволяет разработчикам приложений собирать такие данные, как информация о модели телефона, разрешении экрана, MAC-адресах, Android ID, рекламном идентификаторе, информацию об операторе связи, IMSI и IMEI-коды». ***(Приложения Baidu для Android собирают конфиденциальную информацию // SecurityLab.ru (https://www.securitylab.ru/news/514326.php). 25.11.2020).***

***

«Голландская полиция допросила исследователя безопасности, который сказал, что успешно вошел в аккаунт президента США в Twitter, угадав его пароль.

В прошлом месяце известный кибер-исследователь Виктор Геверс заявил, что получил доступ к аккаунту Дональда Трампа в Twitter с паролем «MAGA2020!».

Белый дом отрицал, что это произошло, а Twitter заявил, что у него нет доказательств взлома.

Но теперь г-н Геверс предоставил дополнительную информацию, подтверждающую его утверждения.

В ходе полицейского допроса г-н Геверс впервые показал, что у него есть значительно больше доказательств «взлома», чем он ранее опубликовал.

Он не раскрыл, какая именно информация у него была, но, войдя в чью-нибудь учетную запись Twitter, кто-то теоретически сможет:

просматривать и отправлять личные сообщения

просматривать твиты, которые пользователь добавил в закладки

доступ к информации, например, сколько людей заблокировал владелец аккаунта

Они даже смогут загрузить архив всех данных пользователя, включая фотографии и сообщения.

Представитель голландской прокуратуры подтвердил газете De Volkskrant: «В настоящее время мы расследуем, не произошло ли что-то криминальное».

Представитель заявил, что их расследование было «независимым голландским расследованием» и не основывалось на запросе США о правовой помощи.

Полиция сообщила Би-би-си, что г-н Геверс был допрошен в качестве свидетеля группой по преступлениям в сфере высоких технологий и еще не являлся подозреваемым.

Полиция должна сначала доказать, что взлом произошел. Если прокуратура сочтет действия г-на Геверса незаконными и выходящими за рамки исследования кибербезопасности, ему может грозить до четырех лет тюрьмы.

Геверс сообщил журналистам о своем взломе 22 октября. Об этом первым сообщил голландский новостной портал Vrij Nederland.

У аккаунта Дональда Трампа в Twitter около 89 миллионов подписчиков.

Скриншоты

Геверс говорит, что 16 октября он проводил полурегулярную проверку аккаунтов в Twitter высокопоставленных кандидатов на выборах в США, когда угадал пароль президента Трампа.

Он не публиковал никаких твитов и не менял никаких настроек, но сказал, что сделал скриншоты некоторых частей аккаунта президента.

Он сказал, что потратил несколько дней, пытаясь связаться с предвыборной кампанией Трампа, чтобы предупредить их об их безопасности, которой не хватало дополнительных мер безопасности, таких как двухфакторная аутентификация, прежде чем идти в прессу.

Двухфакторная аутентификация - это широко используемая система безопасности, которая связывает телефонное приложение или номер с учетной записью, чтобы добавить дополнительный шаг к процессу входа в систему.

Счет президента США теперь в безопасности.

Скептицизм

В то время Twitter сообщил: «Мы не увидели никаких доказательств, подтверждающих это утверждение. Мы активно внедрили меры безопасности для определенной группы высокопоставленных аккаунтов Twitter, связанных с выборами, в Соединенных Штатах, включая федеральные органы власти. "

Twitter отказался отвечать на какие-либо дополнительные вопросы о взломе, в том числе о том, постоянно ли применяются дополнительные меры безопасности и есть ли у компании доступ к учетной записи президента.

Рассказ г-на Геверса был встречен некоторыми в мире информационной безопасности скептически, поскольку его скриншоты могли быть подделаны.

Однако он утверждает, что у него гораздо больше данных. Он надеется, что ему не придется сообщать об этом в прокуратуру, но говорит, что готов к этому в случае необходимости.

Он сказал: «У меня есть доказательства, которые не были включены в ответственное раскрытие информации команде Трампа, потому что они ничего не добавили к предупреждению жертвы о риске.

«Я показал некоторые из них избранной группе журналистов. Полиция спросила меня, желаю ли я показать это, и я сказал нет. Только при наличии признаков правонарушения архивные материалы будут разблокированы».

BBC видела некоторые свидетельства, но не смогла проверить, все ли дополнительные материалы являются подлинными.

Но г-н Геверс говорит, что он придерживается своего отчета о событиях и надеется, что его действия будут признаны нормальной частью его работы как этичного хакера.

«У голландской национальной полиции, особенно группы отдела по борьбе с преступлениями в сфере высоких технологий, не должно быть причин сомневаться в моем заявлении. Они знают меня, они знают мою работу в Голландском институте раскрытия уязвимостей более 22 лет.

«Я не «взламывал» учетную запись Трампа, я не обходил никакую систему безопасности, поскольку не было адекватной защиты. Я просто угадал пароль, а затем попытался предупредить его команду о рисках и способах их устранения».

Ранее в этом году Геверс также утверждал, что в 2016 году успешно вошел в аккаунт Трампа в Twitter.

В этом логине он и другие исследователи безопасности использовали пароль, связанный с другой учетной записью Дональда Трампа в социальной сети, которая была обнаружена в результате предыдущей утечки данных.

В этом случае Геверс утверждает, что пароль был еще одной известной фразой звезды реалити-шоу и политика: «вы уволены». ***(Joe Tidy. Trump Twitter 'hack': Dutch police question researcher // BBC (https://www.bbc.com/news/technology-55019858). 20.11.2020).***

***

«…Gartner прогнозируют, что к концу 2025 г. более 3 млрд. пользователей будет охвачено, по крайней мере, одной коммерческой или государственной, программой «Интернета поведения» (IoB). В то же время половина крупных организаций внедрят новые алгоритмы обеспечения приватности для обработки данных в незащищенных и совместных (shared) средах.

И пользователи, и компании будут монетизировать свою приватность, только по разные стороны баррикад. Бизнес начнет платить или предоставлять свои услуги в обмен на возможность собирать и монетизировать данные пользователей. Люди же будут использовать различные программные комплексы для отслеживания и контроля персональной информации, и продавать ее. Высока вероятность, что корпорации в борьбе за право анализировать данные пользователей будут готовы платить дополнительную премию за эксклюзивный доступ к ним.

С другой стороны, все актуальнее становится вопрос цифровой национальной безопасности, контроль действий и информации со стороны силовых ведомств. Недавно очередной виток получил скандал с двойным бэкдором от «Агентства национальной безопасности США» и «неизвестного государства» в ОС сетевого оборудования Juniper.

Кроме того, на днях совет министров ЕС принял постановление, обязывающее производителей «мессенджеров», например, WhatsApp, Signal и т.д., предоставить мастер-ключи для мониторинга сообщений с E2E-шифрованием.

Это далеко не первая активность в данном направлении. Франция в течение всего года продвигала инициированные Великобританией действия против безопасного шифрования на таких платформах, как WhatsApp, на уровне ЕС. Основа для этого была подготовлена еще в 2015 г., как и история с Juniper, в виде целой серии инициатив Европола и ФБР.

Только в начале октября министры внутренних дел Великобритании, США, Австралии, Новой Зеландии и Канады, а позже Японии и Индии, снова обратились к интернет-провайдерам с просьбой оборудовать свои сети инструментами для сотрудников правоохранительных органов…» ***(Кирилл Гончарук. Приватность в digital-мире - миф или реальность? // Компьютерное Обозрение (https://ko.com.ua/privatnost_v_digital-mire_mif_ili_realnost_135418). 25.11.2020).***

***

«Компания «Elcore Украина», официальный дистрибьютор Micro Focus, сообщила о том, вендор анонсировал релиз 2.0 комплексного решения для аутентификации и безопасного доступа, NetIQ Risk Service.

Как отмечается, это обновление, уже предлагаемое заказчикам во всём мире, значительно улучшает адаптивное управление доступом: непрерывный анализ поведения, позволяет установить, когда защищённым ресурсам требуется более высокий уровень безопасности.

Используя неконтролируемое машинное обучение для определения поведенческих норм, NetIQ Risk Service предупреждает о значимых отклонениях от базовых показателей, при которых следует применить более строгие методы аутентификации, ограничение или завершение сессии либо комбинацию этих мер.

«Действительно, организации теперь могут использовать распознавание текущего поведения как фактор для оценки риска или принятия решения об аутентификации или авторизации, – отметил Ник Николс (Nick Nikols), вице-президент по стратегии Micro Focus. – Итеграция Risk Service с поведенческой аналитикой не требует обучения персонала и может быть мгновенно подключена к существующей защитной инфраструктуре, сводя к минимуму утечку ресурсов и повышая, в конечном итоге, устойчивость корпоративной кибербезопасности».

Главные усовершенствования и возможности Micro Focus NetIQ Risk Service:

• Готовая к использованию интеграция с облачной технологией машинного обучения Micro Focus Interset

• Специализированные поведенческие модели доступа, в которых для автоматического профилирования и измерения рисков применяется более 450 встроенных алгоритмов неконтролируемого машинного обучения.

• Компоновка в контейнерах Docker, обеспечивающая переносимость платформы, а также её управляемость с помощью Kubernetes.

• Спроектирован в качестве дополнения к широко распространённым политикам предопределённого реагирования на риски.

По мере того, как цифровая трансформация продолжает стимулировать стратегические изменения бизнеса, Micro Focus NetIQ Risk Service позволяет организациям осмысленно адаптироваться к текущим и будущим угрозам и является одним из многих способов, с помощью которых Micro Focus помогает клиентам вести, защищать и преобразовывать свой бизнес». ***(NetIQ Risk Services 2.0 использует машинное обучение для непрерывной авторизации // Компьютерное Обозрение (https://ko.com.ua/netiq_risk_services_2_0_ispolzuet_mashinnoe_obuchenie_dlya_nepreryvnoj_avtorizacii_135426). 26.11.2020).***

***

Кібербезпека Інтернету речей

«Использование умных и подключенных к Интернету устройств может существенно облегчить нашу жизнь, но также может дать их производителям больший контроль над ней.

По данным исследовательской компании Park Associates, каждое третье домашнее хозяйство в США с широкополосным подключением владеет как минимум одним устройством умного дома, а интерактивные системы безопасности, обеспечивающие удаленное подключение и возможности управления, установлены в 20% этих домашних хозяйств.

Некоторые компании, предлагающие интеллектуальные устройства, в том числе Google, Belkin и Best Buy, без предупреждения отказались от своих продуктовых линейок интеллектуальных устройств, оставив потребителей без поддержки.

Это приводит к тому, что Наташа Тусикова, доцент Йоркского университета Канады, называет «регулированием через стену». Это когда производители умышленно портят или уничтожают программное обеспечение «с намерением отрицательно повлиять на функциональность продукта».

Такое разрушение изменяет управление физическими продуктами, поскольку производители могут «произвольно и удаленно влиять на функциональность любого программного устройства и даже определять срок его службы», - говорит Тусикова.

Это также дает компаниям «несправедливую возможность навязывать свои предпочтительные политики в одностороннем, автоматическом и удаленном порядке. Благодаря их программному обеспечению продукты Интернета вещей остаются подключенными... к своим производителям, [что] позволяет компаниям... осуществлять значительный контроль над интегрированными в сеть вещами", говорит эксперт.

Любой выбор сложный

Например, в прошлом году Google закрыл свою программу Works with Nest, которая позволила сторонним производителям предлагать продукты, которые работали с его семейством подключенных устройств Nest. Это было прелюдией к запуску своей платформы на внутреннем рынке с помощью Google Assistant. Третьи стороны, по сути, должны были либо перевести свои продукты на работу с Google Assistant, либо перестать работать с Google.

Как рассказал Джейсон Перлоу в ZDNet, потребители, которые приобрели интеллектуальные или подключенные продукты, сделанные третьими сторонами, которые принадлежали программе Works with Nest, остались ни с чем.

«Есть довольно много продуктов, которые были разработаны для работы с Nest, в том числе интеллектуальные фонари Philips Hue, интеллектуальные гаражные ворота Chamberlain и интеллектуальные розетки Wemo - все они сейчас у меня дома», - написал Перлоу.

«Это также включает в себя Amazon Alexa, которая, похоже, получает особую привилегию, по крайней мере, на данный момент. Но да, Google может решить отключить ее в любое время, поскольку вместо этого у нее есть интеллектуальный динамик Google Home. "

По словам Тусиковой, компании могут дополнительно заставить клиентов принимать определенные характеристики продукта и определять, как они используются. Все это возможно в рамках лицензионных соглашений компаний с конечными пользователями, но люди «склонны не читать корпоративные политики и могут даже не знать о правилах, регулирующих использование ими продуктов IoT».

Кроме того, компании «имеют значительную свободу действий при разработке своей политики и оставляют за собой право изменять условия своих лицензионных соглашений без уведомления пользователя», - сказала она.

Последствия наблюдения и безопасности

По словам Тусиковой, видеонаблюдение «является бизнес-моделью и механизмом регулирования» для производителей устройств Интернета вещей. Эти устройства ежедневно обмениваются данными с серверами производителей или

даже несколько раз в день, собирая ошеломляющие объемы данных о своих владельцах.

Все более широкое использование таких технологий голосового помощника, как Google Voice, Apple Siri и Amazon Alexa на подключенных устройствах, еще больше расширяет их возможности наблюдения. Все три технологии всегда прослушиваются и могут быть легко активированы случайно с помощью случайных фраз.

«Потребители должны знать, что все, что подключено к Интернету, будет передавать часть или всю их информацию производителям для анализа, улучшений или других нужд», - говорит Джеймс Маккуигган, защитник осведомленности в обучающей компании по кибербезопасности KnowBe4.

«Угроза безопасности от этих постоянно прослушивающих устройств реальна», - предупредил генеральный директор Gurucul Сарью Найяр. «Существует множество потенциальных атак на эти системы, не говоря уже о серьезных последствиях для конфиденциальности». Однако для среднего потребителя риск невелик, потому что «ты просто не так важен».

На сегодняшний день большинство взломов подключенных устройств было относительно незначительным, хотя и пугающим для жертв фактом - например, взлом радионяни.

Тем не менее, «в мире, где люди постоянно находят уязвимости в продуктах, вам нужен поставщик, который бы реагировал на проблемы безопасности», - говорит Тайлер Регули, менеджер по исследованиям и разработкам в области безопасности в компании по кибербезопасности Tripwire.

Тем не менее, риск «определенно не больше, чем умные телевизоры, игровые приставки и множество других устройств, которые есть у нас дома».

Действительно ли производители заботятся о нас?

Линейки продуктов, которые планируется прекратить, действительно представляют угрозу безопасности для существующих пользователей, если в них обнаруживаются уязвимости до даты прекращения действия.

«Мы сообщили об уязвимостях в системе безопасности нескольким крупным производителям, и их окончательный ответ заключается в том, что они не собираются устранять проблемы, потому что планируют прекратить производство продукта», - говорит Ламар Бейли, старший директор по исследованиям безопасности Tripwire.

Неустанный марш технологий поставил потребителей в тупик. Технологии интеллектуальных устройств и подключенных устройств упрощают нашу жизнь, но цена за это до сих пор не определена». ***(Richard Adhikari. Smart Device Life Cycles Can Pull the Plug on Security // ECT News Network (https://www.technewsworld.com/story/Smart-Device-Life-Cycles-Can-Pull-the-Plug-on-Security-86928.html). 20.11.2020).***

***

«Законопроект, устанавливающий минимальный набор стандартов безопасности для IoT-устройств (Internet of Thing, Интернет вещей),

приобретаемых американским правительством, одобрен Сенатом США во вторник и будет направлен президенту…

Документ, напомним, был представлен в Сенате в августе 2017 года.

«В то время, когда всё больше продуктов, включая бытовую технику, работают на программном обеспечении и подключены к Интернету, очень немногие из них обладают хотя бы базовыми средствами защиты, что представляет риск для граждан и национальной безопасности, – заявил один из поддерживающих законопроект сенаторов. – Я призываю президента подписать этот документ без промедления».

В Сенате отмечают, что эксперты прогнозируют появление «десятков миллиардов» подключённых устройств в ближайшие годы, и указывают на опасности, которым подвергаются из-за этого IT-системы, в особенности – государственные.

В случае подписания президентом закон обяжет Национальный институт стандартов и технологий (National Institute of Standards and Technology, NIST) выпустить рекомендации по безопасной разработке, ремонту и конфигурированию устройств Интернета вещей, а также по управлению идентификацией пользователей. Административно-бюджетное управление Белого дома (Office of Management and Budget, OMB) должно будет представить руководства для федеральных агентств, согласованные с рекомендациями NIST.

Также NIST совместно с министерством внутренней безопасности (Department of Homeland Security, DHS) и сторонними экспертами придётся «публиковать руководства по раскрытию уязвимостей и ликвидации аварий и их последствий в федеральных информационных системах»…». ***(Вика Рябова. Сенат США одобрил законопроект о кибербезопасности IoT-устройств // Экспертный центр электронного государства (https://d-russia.ru/senat-ssha-odobril-zakonoproekt-o-kiberbezopasnosti-iot-ustrojstv.html). 19.11.2020).***

***

Кіберзлочинність та кібертерроризм

«Служба внутрішньої безпеки та боротьби з корупцією при Міністерстві внутрішніх справ Молдови зафіксували кібератаку проти міністра внутрішніх справ Павла Войку. Також кібератаки було здійснено й на інших співробітників міністерства…

Атака відбувалася у вигляді надмірних телефонних дзвінків з декількох номерів. Метою кібератаки було блокування мережі абонента.

Оператор мобільної мережі підтвердив, що кібератака на співробітників міністерства відбувалася з-за кордону.

Тепер правоохоронні органи планують порушити справу за несанкціонований доступ до телекомунікаційних мереж та послуг. Хакерам загрожує покарання у вигляді позбавлення волі до 5 років…». ***(У Молдові сталася кібератака на співробітників МВС // Рубрика (https://rubryka.com/2020/11/01/u-moldovi-stalasya-kiberataka-na-spivrobitnykiv-mvs/). 01.11.2020).***

***

«В Бразилии из-за мощной хакерской атаки парализована работа Верховного суда (STJ). Из-за действий злоумышленников была заблокирована база данных текущих судебных процессов…

Главе STJ Умберто Мартинсу пришлось подписать распоряжение о приостановке работы органа по меньшей мере до 9 ноября.

Как отмечает издание, члены STJ считают ситуацию «крайне серьезной», ведь была нарушена даже работа внутриведомственного почтового сервера.

Все заседания ВС Бразилии, которые проходили в формате видеоконференции, также были приостановлены. По данным суда, рассматриваются только срочные дела, в то время как целевая группа по восстановлению продолжает работу, и ожидается, что системы будут запущены 10 ноября.

Расследованием киберинцидента занялась Федеральная полиция страны.

…кибератака на STJ последовала вслед за новостью о «несанкционированном доступе» к серверам Национального совета правосудия Бразилии». ***(Верховный суд Бразилии приостановил свою работу из-за мощной хакерской атаки // Судово-юридична газета (https://sud.ua/ru/news/abroad/184566-verkhovnyy-sud-brazilii-priostanovil-svoyu-rabotu-iz-za-moschnoy-khakerskoy-ataki). 09.11.2020).***

***

«Компания Group-IB, специализирующаяся на предотвращении кибератак, обнаружила новую мошенническую схему с использованием популярной стриминговой платформы Twitch. Злоумышленники копируют стримы популярных геймеров, добавляют в них баннеры с обещанием легкого заработка, откуда пользователи попадают на мошеннические ресурсы, где теряют деньги и данные банковские карт.

В период пандемии популярность стриминговых платформ стремительно выросла: на самоизоляции люди стали больше смотреть онлайн-трансляций. В свою очередь Twitch в III квартале заняла 91% рынка стриминга во всем мире по количеству транслированных часов: за этот период пользователи посмотрели 4,7 млрд. часов видео на Twitch (данные Streamlabs и Stream Hatchet). Всего на платформу было выгружено рекордные 206 млн. часов видеоконтента, а среднее количество одновременных посетителей платформы составляет 1,5 млн человек. Сами стримеры, по некоторым данным, в среднем зарабатывают 2-10 тыс. долл. в месяц.

Суть новой мошеннической схемы, которую обнаружили аналитики CERT-GIB, в следующем. Злоумышленники находят каналы популярных стримеров и создают похожие по названию и оформлению аккаунты-клоны.

На них мошенники запускают записи стримов с оригинальных каналов, например, недельной давности, «вклеивая» в трансляцию баннер с обещанием легкого заработка, чаще всего с розыгрышем призов. Злоумышленники также публикуют в чате стрима специальную команду (!inst в данном случае), и пользователи, кликнувшие на баннер, отправляются на мошеннический ресурс.

Далее онлайн-афера развивается по классической схеме – жертве предлагается выплата до 5 тыс. долл. за небольшую «комиссию» по оформлению и переводу. В результате пользователь вводит на мошенническом ресурсе данные своего «пластика» (номер, имя владельца, срок действия, CVV-код). Таким образом, со счета жертвы списывается небольшая сумма, а все реквизиты карты остаются у злоумышленников.

Чтобы потенциальные жертвы гарантированно попадали на канал-клон, злоумышленники выводили его в топ поиска стримов, используя сервисы накрутки. Для большей убедительности мошенники размещали фейковые отзывы «счастливчиков», сколько денег им удалось получить, обсуждали процесс зачисления выигрыша, советовали, какими банками лучше пользоваться для более удобного вывода денег. Кроме того, использовались комментарии с настоящего стрима с обсуждением актуальных тем». ***(Мошенники охотятся на пользователей стриминговой платформы Twitch // Компьютерное Обозрение (https://ko.com.ua/moshenniki_ohotyatsya_na_polzovatelej_strimingovoj_platformy_twitch_135242). 12.11.2020).***

***

«Capcom подтвердил факт кибератаки и предупредил, что она вызвала проблемы с электронной почтой. Возможно, речь идет об атаке, анонсированной группировкой REvil.

Бизнес-процессы под угрозой

Японская компания Capcom, знаменитый во всем мире разработчик видеоигр (Resident Evil, Devil May Cry и др.), стала жертвой массивной кибератаки, которая затронула бизнес-процессы фирмы.

В пресс-релизе компании указывается, что атака произошла 2 ноября 2020 г., и что злоумышленники смогли получить доступ к системам организации, что вынудило ее администраторов отключить часть сети Capcom. В частности, пришлось остановить получение и отправку электронной почты.

К настоящему времени невозможно сказать определенно, были ли украдены пользовательские данные; в Capcom заявляют, что признаков кражи корпоративной информации пока нет, что, впрочем, ничего не значит.

Онлайн-игры Capcom продолжали функционировать, проблем с доступом к сайтам компании также не наблюдалось.

Ранее анонсированная атака?

В октябре 2020 г. операторы шифровальщика-вымогателя Egregor опубликовали данные, украденные у двух других игровых компаний — Ubisoft и Crytek. В частности, злоумышленники заявили, что угнали у Ubisoft исходные коды еще не вышедшей на тот момент игры Watch Dogs: Legion (хотя игра вышла 29 октября, как и планировалось), в то время как атакованные ресурсы Crytek были, по утверждению хакеров, «полностью зашифрованы».

В свою очередь, предполагаемый лидер группировки REvil недавно дал интервью каналу Russian OSINT, анонсировав серьезную атаку, которая, дескать, затронет очень крупного разработчика видеоигр. Не исключено, что речь шла как раз об атаке на Capcom.

Между тем, источники издания Bleeping Computer сообщают, что еще в августе 2020 г. в системы Capcom просочился троянец TrickBot. За этим часто следуют атаки посредством шифровальщиков Ryuk или Conti.

Так или иначе, чем именно атакован Capcom, пока неизвестно. Если речь шла о шифровальщике и успешном выводе данных, то, скорее всего, украденные данные вскоре всплывут на форумах даркнета.

«Крупные производители и издатели видеоигр обычно не бедствуют и вдобавок работают с огромным количеством персональных данных, что делает их привлекательной мишенью для киберпреступников, — указывает Анастасия Мельникова, эксперт по информационной безопасности компании SEC Consult Services. — И если безопасность не выстроена должным образом, крупномасштабный взлом — лишь вопрос времени». ***(Роман Георгиев. Знаменитый разработчик игр Resident Evil и Devil May Cry взломан хакерами // CNews (https://safe.cnews.ru/news/top/2020-11-06_znamenityj_razrabotchik_igr). 06.11.2020).***

***

«Агрессивные мошенники выдают себя за Налоговую службу США (IRS) в электронных письмах, предназначенных для того, чтобы обманом заставить потенциальных жертв выплатить сфабрикованные невыплаченные суммы, связанные с пропущенными или просроченными платежами.

Фишинговые электронные письма нацелены на пользователей платформы Microsoft Office 365 и, по оценкам исследователей из компании Abnormal Security, занимающейся безопасностью электронной почты, на сегодняшний день достигло примерно 70 000 почтовых ящиков.

Существует высокая вероятность того, что по крайней мере некоторые из целей сдадутся и заплатят мошенникам, видя, что мошенники угрожают им отчетами кредитного бюро и судебными исками.

Поддельные электронные письма IRS

«Злоумышленник выдает себя за IRS, создавая, казалось бы, заслуживающее доверия электронное письмо с угрозой предъявить юридические обвинения, если получатель не погасит непогашенный остаток на счете», - сообщили исследователи Abnormal Security.

Чтобы сделать его максимально убедительным, мошенники подделывают адрес электронной почты, с которого, по-видимому, исходят мошеннические сообщения, чтобы он выглядел так, как будто они были отправлены с support@irs.gov.

Они также используют идентификационные номера дел, номера досье и идентификаторы ордеров во всех электронных письмах, а также то, что при беглом просмотре выглядит как практически безошибочный английский контент, чтобы добавить к иллюзии легитимности.

Несмотря на это, было бы очевидно, что это афера для всех, кто просматривает заголовки писем и видит, что реальный домен отправителя на самом деле - shoesbagsall.com.

Кроме того, поле для ответа является явным признаком того, что что-то не так, поскольку оно перенаправляет ответы на legal.cc@outlook.com вместо почтового адреса службы поддержки IRS.

Судебные обвинения, ордера на арест и последние предупреждения

Чтобы еще больше запугать и отправить своих жертв в режим паники, мошенники прибегают к юридическим угрозам и даже добавляют возможность возможного ареста с самого начала электронных писем, заголовки которых включают предупреждение «ордер на ваш арест».

Для дополнительного эффекта получателям также сообщают, что электронные письма также будут пересылаться их работодателю, чтобы их причитающиеся суммы были законно удержаны из их заработной платы.

«Мы отправили вам это предупреждение о судебном разбирательстве в мае 2019 года. Но вы не ответили вовремя», - говорится в сообщениях. «На этот раз, если вы не ответите, мы зарегистрируем это дело в суде. Считайте это последним предупреждением».

«Пожалуйста, дайте нам знать, каковы ваши намерения к сегодняшнему дню, чтобы мы могли приостановить дело, иначе мы отправим документы в местный шериф, и вам будет вручена повестка в суд прямо у порога».

Электронные письма также инструктируют цели немедленно ответить с деталями платежа, чтобы избежать разорения их кредита.

«Имитация электронной почты IRS широко распространена во всех отраслях», - заключили исследователи. «Эти атаки различаются по масштабу и жертвам, нацелены как на отдельных лиц, так и на компании в целом».

«Эта конкретная атака следует за растущей тенденцией использования стратегий социальной инженерии для злонамеренного взаимодействия, позволяя злоумышленникам более легко обходить решения для защиты электронной почты, которые в основном сосредоточены на очевидных векторах угроз, таких как ссылки или вложения». ***(Sergiu Gatlan. Scammers impersonating the IRS threaten victims with legal action // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/scammers-impersonating-the-irs-threaten-victims-with-legal-action/). 10.11.2020).***

***

«Усовершенствованная афера с налоговыми льготами HM Revenue and Customs (HMRC) нацелена на жителей Великобритании на этой неделе с помощью текстовых сообщений (SMS).

Кампания smishing вызывает беспокойство, поскольку в ней используются несколько фишинговых доменов HMRC и тактика, при этом новые домены добавляются каждый день, так как старые помечаются спам-фильтрами.

Мало того, что фишинговые страницы тщательно имитируют веб-интерфейс HMRC, в них также встроены целые рабочие процессы онлайн-банкинга, в зависимости от того, кто ваш поставщик банковских услуг.

Начинается с SMS с текстом скидки

Как отмечает BleepingComputer, мошенничество начинается с текстового сообщения, информирующего получателя о том, что он имеет право на налоговую скидку, поскольку в этом году они заплатили «чрезвычайный налог».

Можно подумать, что пользователю лучше не нажимать на домен .com для доступа к государственным услугам. Однако некоторые правительственные услуги Великобритании предлагаются общественности через домены .com.

Одним из таких примеров является homeresponse.com, который настолько хорошо имитирует цветовую схему и пользовательский интерфейс GOV.UK, что однажды меня обманули, если это был фишинговый домен.

Тем не менее, homeresponse.com - это полностью законный веб-сайт, используемый правительством Великобритании для сбора обновленной информации об избирателях домашних хозяйств от жителей…

Таргетинг на клиентов онлайн-банкинга на основе кода сортировки

При нажатии на ссылку в сообщении пользователь попадает на сайт, похожий на сайт GOV.UK.

Но это не ваша основная одностраничная форма для фишинга. Обширный рабочий процесс, используемый в этой кампании, включает несколько этапов и страниц.

Он начинается с простой формы заявки на возврат налога, в которой запрашивается имя пользователя и почтовый индекс.

На следующем шаге форма показывает случайно выбранную сумму возмещения от 200 до 400 фунтов стерлингов, которую налогоплательщик имеет право требовать.

При нажатии кнопки «Пуск» последующие страницы собирают значительный объем информации от ничего не подозревающего пользователя.

Детали, собранные в рамках этой кампании, включают, помимо прочего, следующее, в зависимости от того, на каком фишинговом домене вы находитесь.

ФИО

Дата рождения

домашний адрес

телефонный номер

адрес электронной почты и пароли

Информация о кредитной карте

информация о банковском счете: код сортировки и номер счета

учетные данные онлайн-банкинга

Номер государственного страхования (NINo)

Номер паспорта

Номер водительского удостоверения

запоминающиеся слова и / или ответы на контрольные вопросы, например, девичья фамилия матери

Двухфакторные коды, генерируемые аппаратными устройствами онлайн-банкинга (токены безопасности и устройства чтения карт)

Фишинговые страницы также имеют встроенные проверки, поэтому ввод недопустимых значений для определенных полей может вызвать ошибки. Эта

проверка ошибок может еще больше заставить пользователя поверить в то, что веб-страница является законной.

Самое интересное начинается после того, как некоторая часть этой информации была отправлена пользователем.

Показана промежуточная страница "обработки", на которой проверяются некоторые поля, собранные на данный момент.

В тестах BleepingComputer рабочий процесс завершился на этом этапе, и пользователь был перенаправлен на настоящий веб-сайт HMRC.

Однако в других тестах, где вводился реальный код сортировки отделения банка, и предоставленные тестовые данные казались «достаточно реальными» для машины, мы наблюдали, что перенаправление приведет к фишинговым страницам онлайн-банкинга, размещенным в том же фишинговом домене.

BleepingComputer проверила фишинговые страницы с реальными кодами сортировки отделений банков Halifax и NatWest, что подтвердило наши подозрения.

Эти двойники онлайн-банкинга дополнительно собирают банковские данные пользователя, запоминающиеся слова, двухфакторные коды и т. Д.

BleepingComputer обнаружил, что в кампании есть целые наборы фишинговых сайтов, дублирующих реальные сайты известных британских крупных банков, для нацеливания на своих клиентов.

В список входят Barclays, Clydesdale, Halifax, NatWest, HSBC UK, Metro Bank, Nationwide, Citi, Lloyd's, TSB, Co-op, Royal Bank of Scotland (RBS), Santander, Tesco Bank и Yorkshire Bank.

Несмотря на тщательность тех, кто стоит за этой кампанией, они не проделали великолепную работу по защите собранных данных - вряд ли их забота, что делает эту кампанию еще более опасной.

В одном фишинговом домене, используемом в кампании, произошла утечка журналов посетителей с более чем 4500 записями. Домен, в котором произошла утечка этих журналов, больше не доступен.

При анализе журналов BleepingComputer обнаружил, что более 1000 уникальных IP-адресов получили доступ к этой фишинговой кампании…» ***(Ax Sharma. HMRC smishing tax scam targets UK banking customers // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/hmrc-smishing-tax-scam-targets-uk-banking-customers/). 08.11.2020).***

***

«По информации экспертов, британская общественная телерадиовещательная организация страдает от более чем 250.000 вредоносных электронных писем в день. среднее их число составило 283.597 писем за сутки.

В месяц BBC получает более 6,5 миллионов электронных писем, которые классифицируются как спам или скам, а также почти 19 тысяч содержат в себе вредоносные программы. В период с января по август 2020 года всего было заблокировано почти 52 миллиона вредоносных электронных писем.

Эксперты из Barracuda Networks отмечают, что из-за пандемии количество фишинговых писем увеличилось на 667%. Злоумышленники в основном играют на таких чувствах жертв, как вызванные кризисной ситуацией страх и неопределённость.

Телерадиовещательная компания подвергалась кибератакам и в прошлом. Например, в 2013 году сторонники президента Сирии Башара Асада получили контроль над некоторыми твиттер-аккаунтами BBC, с помощью которых была устроена фишинговая рассылка по сотрудникам». ***(BBC атакуют более 250.000 раз в день // SecureNews (https://securenews.ru/the-bbc-is-attacked-more-than-250000-times-a-day/). 03.11.2020).***

***

«Казначейство Соединённых Штатов Америки ввело санкции против одного из научно-исследовательских институтов России после того, как одного из его профессоров связали с малварью под названием TRITON в октябре 2018 года.

Также вредоносная программа известна под такими названиями, как TRISIS и HatMan. По результатам расследования, она была использована против нефтехимического предприятия в Саудовской Аравии в августе 2017 года.

Обвинённый профессор работал в Центральном научно-исследовательском институте химии и механики, который располагается в Москве. Это привело к введению санкций против института.

По заявлению Казначейства США, в институте разработали инструменты, с помощью которых была проведена кибератака. Также было заявлено, что в 2019 году злоумышленники просканировали не менее 20 электросетей в США на предмет уязвимостей.

Введённые 23 октября 2020 года санкции не позволят резидентам США сотрудничать с данным институтом». ***(США вводит санкции против российского института, связанного с кибератакой // SecureNews (https://securenews.ru/us-imposes-sanctions-on-russian-institution-linked-to-cyber-attack/). 02.11.2020).***

***

«Сеть здравоохранения Университета Вермонта (UVM) изо всех сил пытается восстановить свои системы после кибератаки, которая привела к широко распространенным задержкам в назначении пациентов, в том числе при химиотерапии, а также маммографии и биопсии.

Сеть UVM Health Network - это система из шести больниц, домашнего медицинского обслуживания и хосписа, в которую входят более 1000 врачей, 2000 медсестер и других врачей в Вермонте и северном Нью-Йорке. Кибератака была впервые начата на неделе 25 октября, при этом, согласно местным сообщениям, больше всего пострадал Медицинский центр UVM. В сообщениях говорилось, что атака прошла через главный компьютерный сервер больницы и затронула всю ее систему.

С тех пор ФБР и Национальная гвардия Вермонта были привлечены для проверки тысяч компьютеров и устройств конечных пользователей, чтобы

убедиться, что они не содержат вредоносных программ. В обновленной информации, опубликованной в субботу, сеть здравоохранения UVM сообщила, что «за ночь добилась значительного прогресса в восстановлении скрытых компонентов, которые помогут в восстановлении дополнительных систем, ориентированных на пациента».

«Наша ИТ-команда теперь получила доступ к расписаниям пациентов для всех сетевых больниц на следующие выходные», - говорится в субботнем обновлении. «Это повысит нашу эффективность и общий опыт для пациентов, поскольку мы продолжаем восстанавливать системы после кибератаки на прошлой неделе».

Threatpost обратился к представителю ФБР Саре Руан по поводу атаки, в том числе по поводу того, к какому типу данных был осуществлен доступ, как изначально произошла атака, использовались ли вредоносные программы или программы-вымогатели и многое другое. Эта статья будет обновлена соответствующим образом, когда пресс-секретарь ответит.

«Во время пандемии системы здравоохранения, больницы и фармацевтические компании подвергались более целенаправленным кибератакам, - сказал Threatpost Хэнк Шлесс, старший менеджер по решениям безопасности в Lookout. «Субъекты угроз знают, что эти организации находятся под сильным давлением, чтобы заботиться о большом количестве пациентов и помогать в открытии вакцины в дополнение к своим обычным обязанностям».

Влияние

В то время как сеть здравоохранения UVM была нечеткой в отношении того, к каким данным был получен доступ, согласно отчетам, это повлияло на планирование назначений пациентов, что повлияло на важные проверки пациентов и их назначения.

Перед атакой от 45 до 60 пациентов могли записаться на прием к химиотерапевту в медицинском центре UVM, однако после кибератаки это число снизилось до 15, что привело к увеличению количества людей, нуждающихся в помощи.

Сеть больниц заявила, что разработала планы по обеспечению пациентам необходимого лечения рака в течение следующих нескольких дней.

«Пациенты проходят лечение, и мы срочно работаем над расширением наших возможностей по предоставлению химиотерапии в медицинском центре UVM до семи дней в неделю и трех вечеров в неделю», - сказали они. «Между тем, мы также планируем лечение некоторых пациентов в Центральном медицинском центре Вермонта, больнице врачей долины Шамплейн и других учреждениях, когда это необходимо».

Сеть здравоохранения UVM также сообщила, что смогла восстановить некоторые графики встреч для остальной части своей сети. Однако сеть сообщила, что в понедельник в медицинском центре UVM не может провести визуализацию груди, включая маммографию, ультразвуковое исследование груди и биопсию.

«Наши специалисты по визуализации груди имеют ограниченный доступ к данным пациентов и поэтому не смогут заранее сообщить всем пациентам об

отмене их приема», - говорится в сообщении об утечке данных. «Мы приносим глубокие извинения за неудобства, которые могут возникнуть у пациентов».

Согласно сообщениям, сотрудники больниц также пострадали в результате кибератаки, в результате которой некоторые сотрудники не смогли выполнять свою обычную работу. По словам президента и главного операционного директора Стивена Леффлера, доктора медицины, на пресс-конференции в пятницу, до 300 сотрудников больницы медицинского центра UVM были переведены или уволены.

Киберпреступники атакуют больницы

За последние несколько месяцев больницы и здравоохранение столкнулись с шквалом кибератак. Например, в сентябре в результате атаки вымогателей была остановлена компания Universal Health Services, которая входит в список Fortune-500 и владеет общенациональной сетью больниц. В октябре атакам программ-вымогателей подверглись несколько больниц, в том числе Кламат-Фолс, медицинский центр Sky Lakes в штате Орегон и система здравоохранения Святого Лаврентия в Нью-Йорке.

«Отрасль здравоохранения останется мишенью для программ-вымогателей высокого уровня, особенно с учетом того, что продолжающееся тестирование увеличивает объем данных или информации о пациентах или будущих пациентах», - сказала Threatpost Хизер Паунет, вице-президент по управлению продуктами в Untangle. «ИТ-отделы должны быть более осведомлены, чем когда-либо прежде, о том, как защитить свою сеть, своих сотрудников и своих пациентов».

Мохит Тивари, соучредитель и генеральный директор Symmetry Systems, сказал Threatpost, что больницы оказываются в «очень сложной ситуации», когда дело касается безопасности.

«Им необходимо уделять первоочередное внимание ежедневной борьбе с рядом проблем, связанных со здравоохранением, а также необходимости работать с программным и аппаратным обеспечением, на сертификацию безопасности которого уходят годы, - сказал Тивари. «К сожалению, это означает, что вычислительная инфраструктура отстает как по коммерческим, так и по техническим причинам».

Дирк Шрадер, глобальный вице-президент New Net Technologies (NNT), в ходе предыдущего исследования обнаружил, что незащищенные медицинские устройства без исправлений, подключенные к Интернету (связанные с архивами изображений и системами электронных медицинских записей), показывают, что сектор здравоохранения по-прежнему остается несложным цель - и, скорее всего, так и останется в обозримом будущем.

Он сказал, что сектору необходимо изменить свой подход от небрежного отношения к кибербезопасности к интегрированному, устойчивому к киберпространству обращению с медицинскими устройствами, включенными в больничные процессы.

«Похоже, что группы вредоносных программ решили, что это конец закрытого сезона для больниц и других поставщиков медицинских услуг», - сказал Шрейдер Threatpost. «В начале пандемии большинство пообещали уклоняться от этой группы целей, однако недавнее предупреждение, выпущенное CISA, ФБР и HHS, указывает на то, что этого больше не ожидается». ***(Lindsey O'Donnell.***

Cyberattack on UVM Health Network Impedes Chemotherapy Appointments // Threatpost (https://threatpost.com/cyberattack-uvm-health-network/161059/). 09.11.2020).

***

«Два невиданных ранее бэкдора Powershell были обнаружены после того, как исследователи недавно обнаружили атаку на серверы Microsoft Exchange в организации в Кувейте.

Эта деятельность связана с известной группой угроз xHunt, которая была впервые обнаружена в 2018 году и ранее уже проводила ряд атак, направленных на правительство Кувейта, а также на судоходные и транспортные организации.

Однако недавно наблюдаемая атака - 22 августа 2019 г. или ранее на основании отметок времени создания запланированных задач, связанных с нарушением, - показывает, что злоумышленники обновили свой арсенал инструментов.

Атака использовала два недавно обнаруженных бэкдора: один, который исследователи назвали «TriFive», а другой, вариант ранее обнаруженного бэкдора на основе PowerShell (получившего название CASHY200), который они назвали «Snugy».

«Оба бэкдора, установленные на скомпрометированном сервере Exchange правительственной организации Кувейта, использовали скрытые каналы для связи C2, в частности туннелирование DNS и канал на основе электронной почты с использованием черновиков в папке «Удаленные» скомпрометированной учетной записи электронной почты», - заявили исследователи из Palo Команда Alto's Unit 42, понедельник.

Атака

Исследователи заявили, что им еще не известно, как участники получили доступ к серверу Exchange. Впервые они узнали об атаке в сентябре, когда их уведомили о том, что злоумышленники взломали организацию в Кувейте. Подозрительные команды на рассматриваемом сервере Exchange выполнялись через процесс w3wp.exe служб IIS.

После исследования сервера «мы обнаружили две запланированные задачи, созданные злоумышленником задолго до даты сбора журналов, обе из которых будут запускать вредоносные сценарии PowerShell», - заявили исследователи. «Мы не можем подтвердить, что субъекты использовали любой из этих сценариев PowerShell для установки веб-оболочки, но мы полагаем, что субъекты угроз уже имели доступ к серверу до записи журналов».

Речь идет о двух задачах: «ResolutionHosts» и «ResolutionsHosts». Оба они были созданы в папке c: \ Windows \ System32 \ Tasks \ Microsoft \ Windows \ WDI.

Исследователи полагают, что злоумышленники использовали эти две запланированные задачи в качестве метода сохранения, поскольку они запускали два сценария PowerShell повторно (один каждые 30 минут, а другой каждые пять минут). Команды, выполняемые двумя задачами, пытаются запустить «splwow64.ps1» и «OfficeIntegrator.ps1», которые являются двумя бэкдорами.

«Скрипты хранились в двух отдельных папках в системе, что, вероятно, является попыткой избежать обнаружения и удаления обоих бэкдоров», - заявили исследователи.

Бэкдор TriFive

По словам исследователей, первый бэкдор, TriFive, обеспечивает бэкдор-доступ к серверу Exchange путем входа в почтовый ящик легитимного пользователя и получения сценария PowerShell из черновика электронной почты в папке удаленных писем. Они отметили, что эта тактика ранее использовалась злоумышленником в качестве способа связи с вредоносным сервером управления и контроля (C2) в кампании сентября 2019 года.

«В образце TriFive использовалось законное имя учетной записи и учетные данные целевой организации», - заявили исследователи. «Это говорит о том, что злоумышленник украл учетные данные до установки бэкдора TriFive».

Во-первых, чтобы отдавать команды бэкдору, субъект должен входить в ту же законную учетную запись электронной почты и создавать черновик электронной почты с темой «555», включая команду в зашифрованном и закодированном в base64 формате.

На стороне бэкдора сценарий PowerShell затем входит в законную учетную запись электронной почты на скомпрометированном сервере Exchange и проверяет папку «Удаленные» на наличие писем с темой «555». Сценарий выполнит команду, указанную в электронном письме, через PowerShell. Наконец, они затем отправляли результаты команды обратно злоумышленнику, задав зашифрованный зашифрованный текст как тело сообщения черновика электронной почты и снова сохраняя электронное письмо в папке «Удаленные» с темой «555s».

Snugy

Другой бэкдор на основе PowerShell, Snugy, использует канал туннелирования DNS для выполнения команд на взломанном сервере. DNS-туннелирование позволяет злоумышленникам обмениваться данными с использованием протокола DNS, который можно использовать для автоматического извлечения данных или для установления канала связи с внешним вредоносным сервером.

Злоумышленники использовали бэкдор Snugy для получения имени хоста системы, выполнения команд и извлечения результатов. Исследователи смогли получить домены, запрошенные через запросы ping, отправленные со взломанного сервера.

«Основываясь на данных, полученных из поддоменов, мы смогли определить, кто запускал ipconfig / all и dir», - сказали они. «К сожалению, у нас было только подмножество запросов, поэтому извлеченные данные были усечены, что также предполагает, что субъекты, вероятно, выполняли другие команды, которые мы не наблюдали».

Исследователи наблюдали различные совпадения кода между Snugy и ранее обнаруженным бэкдором CASHY200, включая аналогичные функции, используемые для преобразования строк в шестнадцатеричное представление и генерации строки случайных символов верхнего и нижнего регистра; а также

обработчики команд, использующие первый октет IP-адреса для определения команды для запуска и получения имени хоста и выполнения команды.

По словам исследователей, кампания xHunt продолжается, поскольку злоумышленники совершают атаки на кувейтские организации.

Основываясь на этих последних обнаруженных бэкдорах, движение вперед «похоже, что эта группа начинает использовать канал связи на основе электронной почты, когда у них уже есть доступ к скомпрометированному серверу Exchange в организации», - заявили они». ***(Lindsey O'Donnell. Microsoft Exchange Attack Exposes New xHunt Backdoors // Threatpost (https://threatpost.com/microsoft-exchange-attack-xhunt-backdoors/161041/). 09.11.2020).***

***

«Ранее известная группа угроз, именуемая UNC1945, взламывала телекоммуникационные компании и нацеливалась на финансовые и профессиональные консалтинговые отрасли, используя брешь в безопасности в операционной системе Oracle Solaris.

Исследователи заявили, что группа использовала ошибку, когда был «нулевой день», задолго до того, как появился патч.

Ошибка, CVE-2020-14871, был недавно рассмотрен в Oracle в октябре 2020 Critical Patch Update. Уязвимость существует в подключаемом модуле аутентификации Oracle Solaris (PAM) и позволяет неаутентифицированному злоумышленнику, имеющему доступ к сети через несколько протоколов, использовать и компрометировать операционную систему. Злоумышленники использовали инструмент удаленной эксплуатации, который исследователи называют «EVILSUN», чтобы использовать уязвимость.

«В середине 2020 года мы наблюдали, как UNC1945 развернул EVILSUN - инструмент удаленной эксплуатации, содержащий эксплойт нулевого дня для CVE-2020-14871 - на сервере Solaris 9», - сказали исследователи из FireEye в понедельник. «В то время соединения с сервера на IP-адрес злоумышленника наблюдались через порт 8080».

Исследователи впервые заметили, что злоумышленники получили доступ к серверу Solaris и установили бэкдор (отслеживаемый как SLAPSTICK) в конце 2018 года. Днем позже злоумышленник запустил специальный бэкдор Linux (исследователи называли LEMONSTICK) на рабочей станции. Возможности этого бэкдора включают выполнение команд, передачу и выполнение файлов, а также возможность устанавливать туннельные соединения, что позволяет злоумышленникам захватывать детали соединения и учетные данные для облегчения дальнейшего взлома.

После 519-дневного периода ожидания, в течение которого, по словам исследователей, было «недостаточно доступных доказательств» для отслеживания группы, следующий показатель активности был в середине 2020 года. По словам исследователей, в это время к инфраструктуре злоумышленника подключался другой сервер Solaris.

Исследователи также заметили апрельский пост на черном рынке, рекламирующий «Oracle Solaris SSHD Remote Root Exploit» стоимостью около 3000 долларов, который, по их словам, может быть идентифицирован как EVILSUN.

Детали атаки

После первоначального заражения UNC1945 наблюдал сбрасывание пользовательской виртуальной машины QEMU (ВМ) на нескольких хостах. Это было выполнено в системах Linux путем запуска сценария start.sh, который содержал настройки пересылки TCP. Эти настройки «могут использоваться злоумышленником вместе с туннелями SSH, чтобы предоставить прямой доступ от виртуальной машины злоумышленника к серверу управления и контроля, чтобы скрыть взаимодействие с инфраструктурой клиента», - заявили исследователи.

Виртуальная машина также содержала различные инструменты, такие как сетевые сканеры, эксплойты и инструменты разведки. Предварительно загруженные инструменты Tiny Core Linux включали Mimikatz, Powersploit, Responder, Procdump, CrackMapExec, PoshC2, Medusa, JBoss Vulnerability Scanner и другие.

Злоумышленник также использовал различные средства защиты от обнаружения и методы защиты от криминалистики.

Например, он поместил свой инструмент и выходные файлы во временные точки монтирования файловой системы, которые хранились в энергозависимой памяти, использовал встроенные утилиты и общедоступные инструменты, такие как команды Linux, для изменения временных меток и использовал LOGBLEACH для очистки журналов, чтобы помешать криминалистическому анализу. LOGBLEACH - это служебная программа ELF с функцией удаления записей журнала из указанного файла журнала на основе фильтра, предоставляемого через командную строку.

«Для дальнейшего сокрытия активности в памяти системы Solaris был запущен упаковщик ELF Linux под названием STEELCORGI», - заявили исследователи. «Вредоносная программа содержит различные методы антианализа, включая защиту от отладки, отслеживания и обфускации строк. Он использует переменные среды как ключ для распаковки окончательной полезной нагрузки».

Установив точку опоры, UNC1945 собрал учетные данные с помощью SLAPSTICK и инструментов с открытым исходным кодом, таких как Mimikatz. Затем он повысил привилегии и успешно продвинулся по нескольким сетям.

UNC1945 также загрузил различные инструменты для постэксплуатации, такие как PUPYRAT, кроссплатформенный многофункциональный инструмент удаленного администрирования и постэксплуатации с открытым исходным кодом, в основном написанный на Python; а также инструмент сканирования BlueKeep. BlueKeep (CVE-2019-0708) - это уязвимость системы безопасности, которая была обнаружена в реализации протокола удаленного рабочего стола (RDP) от Microsoft, которая допускает возможность удаленного выполнения кода.

Несмотря на многоступенчатую операцию, исследователи заявили, что не наблюдали доказательств кражи данных и не смогли определить миссию UNC1945 для большинства исследованных вторжений.

«UNC1945 был нацелен на операционные системы Oracle Solaris, использовал несколько инструментов и утилит против операционных систем Windows и Linux, загружал и управлял пользовательскими виртуальными машинами, а также использовал методы, позволяющие избежать обнаружения», - заявили исследователи. «UNC1945 продемонстрировал доступ к эксплойтам, инструментам и вредоносным программам для нескольких операционных систем, дисциплинированный интерес к прикрытию или манипулированию их деятельностью, а также продемонстрировал передовые технические возможности во время интерактивных операций». ***(Lindsey O'Donnell. Oracle Solaris Zero-Day Attack Revealed // Threatpost (https://threatpost.com/oracle-solaris-zero-day-attack/160929/). 03.11.2020).***

***

«Согласно новой информации, представленной Комиссией по ценным бумагам и биржам США, в результате недавней кибератаки глобальные операции производителя офисной мебели Steelcase Inc. были закрыты на две недели.

Последняя форма 8-K Steelcase, поданная сегодня, подчеркивает разрушения, которые последовали после того, как компания сообщила об атаке 22 октября. В этой первоначальной документации Steelcase заявила, что «хотя кибератаки могут быть непредсказуемыми, Steelcase в настоящее время не ожидает этот инцидент окажет существенное влияние на его бизнес-операции или финансовые результаты».

Сегодняшняя документация рисует иную картину. В нем Steeclase сообщила, что отключила большую часть своих глобальных систем управления заказами, производства и распределения на две недели после атаки. На данный момент работа вернулась в нормальный режим.

«(Steelcase) возобновила нормальную работу и работает над отгрузкой заказов, задержанных из-за останова, и возвращением к нормальным срокам выполнения заказов», - говорится в документации. «В связи с остановкой производства, которая охватила начало ноября, (Steelcase) ожидает, что некоторые поставки, которые первоначально были запланированы на третий квартал компании, не будут отправлены до четвертого квартала».

В заявлении говорится, что Steelcase понес дополнительные расходы на сверхурочную работу и ускорил фрахт, поскольку он работает через накопившиеся заказы. Steelcase также понес расходы, связанные с ремонтом, восстановлением и укреплением своих систем.

Steelcase также заявил, что нет никаких доказательств того, что конфиденциальные бизнес-данные, включая интеллектуальную собственность и данные клиентов, поставщиков и сотрудников, были извлечены из системы…». ***(JAYSON BUSSA. Cyberattack caused global shutdowns for Steelcase, potential for delayed shipments // MiBiz (https://mibiz.com/sections/manufacturing/cyberattack-caused-global-shutdowns-for-steelcase-potential-for-delayed-shipments). 12.11.2020).***

***

«Федеральное бюро расследований разослало предупреждение о том, что злоумышленники злоупотребляют неправильно настроенными приложениями SonarQube для доступа и кражи репозиториев исходного кода у правительственных агентств США и частных компаний.

Вторжения имели место по крайней мере с апреля 2020 года, говорится в сообщении ФБР, разосланном в прошлом месяце и обнародованном на этой неделе на его веб-сайте.

Предупреждение специально предупреждает владельцев SonarQube, веб-приложения, которое компании интегрируют в свои цепочки сборки программного обеспечения для тестирования исходного кода и обнаружения недостатков безопасности перед развертыванием кода и приложений в производственных средах.

Приложения SonarQube устанавливаются на веб-серверы и подключаются к системам размещения исходного кода, таким как учетные записи BitBucket, GitHub или GitLab, или к системам Azure DevOps.

Но ФБР сообщает, что некоторые компании оставили эти системы незащищенными, запустив их в конфигурации по умолчанию (на порту 9000) с учетными данными администратора по умолчанию (admin / admin).

Представители ФБР заявляют, что злоумышленники злоупотребляли этими неправильными конфигурациями для доступа к экземплярам SonarQube, перехода к подключенным репозиториям исходного кода, а затем доступа и кражи проприетарных или частных / конфиденциальных приложений.

Официальные лица привели два примера прошлых инцидентов:

«В августе 2020 года неизвестные злоумышленники осуществили утечку внутренних данных из двух организаций через общедоступный репозиторий жизненного цикла. Похищенные данные были получены из экземпляров SonarQube, которые использовали настройки порта по умолчанию и учетные данные администратора, работающие в сетях затронутых организаций.

«Эта деятельность аналогична предыдущей утечке данных в июле 2020 года, когда идентифицированный кибер-актор извлек проприетарный исходный код с предприятий через плохо защищенные экземпляры SonarQube и опубликовал извлеченный исходный код в собственном публичном репозитории».

ЗАБЫТАЯ ПРОБЛЕМА СНОВА ПОЯВИТСЯ В 2020 ГОДУ

Предупреждение ФБР затрагивает малоизвестную проблему среди разработчиков программного обеспечения и исследователей безопасности.

В то время как индустрия кибербезопасности часто предупреждала об опасности оставлять базы данных MongoDB или Elasticsearch открытыми в Интернете без паролей, SonarQube ускользнул от проблем.

Однако некоторые исследователи безопасности предупреждали об опасности оставлять приложения SonarQube открытыми в сети с учетными данными по умолчанию еще с мая 2018 года.

В то время охотник за утечками данных Боб Дьяченко предупредил, что от 30% до 40% всех ~ 3000 экземпляров SonarQube, доступных в то время в сети, не имели пароля или механизма аутентификации.

В этом году швейцарский исследователь безопасности по имени Тилль Коттманн также поднял ту же проблему о неправильно настроенных экземплярах SonarQube. В течение года Коттманн собрал исходный код десятков технологических компаний на общедоступном портале, и многие из них были получены из приложений SonarQube.

«Большинство людей, кажется, не меняют абсолютно ни одной из настроек, которые на самом деле должным образом объяснены в руководстве по установке от SonarQube», - сказал Коттманн ZDNet.

«Я не знаю текущего количества открытых экземпляров SonarQube, но сомневаюсь, что оно сильно изменилось. Я предполагаю, что по-прежнему гораздо больше 1000 серверов (которые индексируются Shodan), которые являются «уязвимыми», поскольку либо не требуют авторизации, либо оставляют значение по умолчанию. спасибо, - сказал он

Чтобы предотвратить подобные утечки, в предупреждении ФБР перечислен ряд шагов, которые компании могут предпринять для защиты своих серверов SonarQube, начиная с изменения конфигурации и учетных данных приложения по умолчанию, а затем с использованием брандмауэров для предотвращения несанкционированного доступа к приложению со стороны неавторизованных пользователей». ***(Catalin Cimpanu. FBI: Hackers stole source code from US government agencies and private companies // ZDNet (https://www.zdnet.com/article/fbi-hackers-stole-source-code-from-us-government-agencies-and-private-companies/). 07.11.2020).***

***

«Не обращая на себя особого внимания, несколько злоумышленников в течение последних двух-трех лет проводили массовое сканирование Интернета на предмет наличия файлов ENV, которые были случайно загружены и оставлены открытыми на веб-серверах.

Файлы ENV или файлы среды - это тип файлов конфигурации, которые обычно используются инструментами разработки.

Такие платформы, как Docker, Node.js, Symfony и Django, используют файлы ENV для хранения переменных среды, таких как токены API, пароли и логины для входа в базу данных.

Из-за характера данных, которые они хранят, файлы ENV всегда должны храниться в защищенных папках.

«Я предполагаю, что ботнет сканирует эти файлы, чтобы найти сохраненные учетные данные, которые позволят злоумышленнику взаимодействовать с базами данных, такими как Firebase, экземпляры AWS и т. Д.» , - сказал ZDNet Дэниел Банс, главный аналитик безопасности SecurityJoes.

«Если злоумышленник может получить доступ к закрытым ключам API, он может злоупотребить программным обеспечением», - добавил Банс.

ТОЛЬКО В ЭТОМ МЕСЯЦЕ АКТИВНЫ БОЛЕЕ 1100 СКАНЕРОВ ENV

Разработчики приложений часто получали предупреждения о сканировании вредоносными ботнетами файлов конфигурации GIT или закрытых ключей SSH,

которые были случайно загружены в сеть, но сканирование файлов ENV было таким же распространенным, как и первые два.

По данным компании Greynoise, за последние три года для сканирования файлов ENV использовалось более 2800 различных IP-адресов, при этом за последний месяц было задействовано более 1100 сканеров.

Подобные проверки были также зарегистрированы компанией Bad Packets, занимающейся разведкой угроз, которая отслеживала наиболее распространенные пути к файлам ENV в Twitter в течение последнего года.

Злоумышленники, которые идентифицируют файлы ENV, в конечном итоге загрузят файл, извлекут все конфиденциальные учетные данные, а затем нарушат внутреннюю инфраструктуру компании.

Конечной целью этих последующих атак может быть что угодно: от кражи интеллектуальной собственности и коммерческих секретов до атак программ-вымогателей или установки скрытых вредоносных программ для крипто-майнинга.

Разработчикам рекомендуется протестировать и посмотреть, доступны ли файлы ENV их приложений в Интернете, а затем защитить любой файл ENV, который был случайно обнаружен. Для открытых файлов ENV также необходимо изменить все токены и пароли». ***(Catalin Cimpanu. Botnets have been silently mass-scanning the internet for unsecured ENV files // ZDNet (https://www.zdnet.com/article/botnets-have-been-silently-mass-scanning-the-internet-for-unsecured-env-files/). 21.11.2020).***

***

«Лондонский совет, подвергшийся кибератаке месяц назад, заявил, что некоторые службы могут быть недоступны или отключены в течение нескольких месяцев.

Хакни совет, который предоставляет услуги 280000 людей в восточной части Лондона, говорится в обновленной информации о кибератаке середины октября, что она продолжает упорно работать, чтобы восстановить поврежденные системы и закончить «существенные нарушения», которое помешало жителям получить доступ к некоторой услуге.

Совет охарактеризовал инцидент как «продвинутую криминальную кибератаку», затронувшую большое количество служб, и заявил, что работает вместе с Национальным центром кибербезопасности (NCSC) и Национальным агентством по борьбе с преступностью (NCA) над расследованием «отвратительной» атаки. Однако совет предоставил мало подробностей о том, что произошло.

«Некоторые из наших услуг могут быть недоступны или отключены в течение нескольких месяцев», - заявили в совете, но добавили, что некоторые ранее затронутые услуги были полностью или частично восстановлены, или команды совета создали новые или временные способы доступа жителей к ним.

«В некритических областях некоторые из наших услуг выполнялись медленнее, чем обычно, и в настоящее время мы не можем отвечать на все запросы и запросы так, как обычно», - заявили в совете.

«Ряд муниципальных услуг пострадали от сбоев, вызванных кибератакой, которая затронет наших жителей, включая такие области, как выплаты пособий и выплаты муниципальных налогов», - заявили в совете. Тем не менее, он добавил, что многие варианты оплаты по-прежнему доступны для аренды, платы за обслуживание, капитальных работ и гаражей.

Услуги, которые все еще затронуты, включают поиски земли и приложения для планирования, необходимые для продажи недвижимости, а также системы заказов и отчетности, которые совет использует для обработки отчетов, таких как шум, антиобщественное поведение и пропущенный сбор мусора. Также затронуты системы, которые совет использует для доступа к учетным записям, создания новых учетных записей и обработки платежей, таких как льготы, муниципальный налог, арендная плата и плата за обслуживание, а также онлайн-приложения, которые жители используют для управления ими самостоятельно.

Совет также заявил, что сообщения, отправленные на некоторые из его общедоступных адресов электронной почты в период с 12 октября по 26 октября, теперь недоступны, и что запросы, которые не получили ответа и остаются невыполненными, должны быть отправлены снова». ***(Steve Ranger. Cyberattack disruption could last for months, says council // ZDNet (https://www.zdnet.com/article/cyber-attack-disruption-could-last-for-months-says-council/). 16.11.2020).***

***

«Service NSW, единый центр правительства Нового Южного Уэльса по оказанию услуг, в апреле 2020 года подвергся кибератаке, в результате которой была скомпрометирована информация 186000 клиентов.

После четырехмесячного расследования, начавшегося в апреле, Служба Нового Южного Уэльса заявила, что обнаружила, что 738 ГБ данных, состоящих из 3,8 миллиона документов, были украдены из 47 учетных записей электронной почты сотрудников.

Однако служба NSW заверила, что не было никаких доказательств того, что отдельные данные учетной записи MyService NSW или базы данных Service NSW были скомпрометированы во время атаки.

«В ходе этого тщательного первого шага было обнаружено около 500 000 документов, в которых упоминается личная информация», - заявил в сентябре генеральный директор Service NSW Деймон Рис. «Данные состоят из документов, таких как рукописные заметки и формы, сканированные изображения и записи приложений транзакций».

Представляя свой бюджет на 2020-2021 годы во вторник, правительство сообщило о юридических и следственных расходах, которые оно, как ожидается, понесет в результате атаки.

«В апреле 2020 года Служба Нового Южного Уэльса уведомила полицию и власти о кибератаке, которая потенциально скомпрометировала информацию о клиентах», - говорится в бюджетных документах [PDF]. «Расследование этого дела все еще продолжается, однако ожидается, что Service NSW понесет судебные

издержки и расходы на расследование в размере приблизительно 7 миллионов австралийских долларов».

В другом месте государственного бюджета на 2020-2021 годы правительство в значительной степени расширило ряд инициатив, которые уже были запущены, и сосредоточило внимание также на том, как вывести штат из его дефицита в 16 миллиардов австралийских долларов.

Важной особенностью его бюджета стал Фонд цифрового перезапуска (DRF), которому будет выделено 1,2 млрд австралийских долларов в качестве капитала и 400 млн австралийских долларов в виде регулярного финансирования.

«Ключом к предоставлению качественных государственных услуг является обеспечение того, чтобы эти услуги соответствовали назначению и соответствовали потребностям сообщества. В этом бюджете правительство реализует амбициозную программу преобразований, основанную на оцифровке», - говорится в бюджетных документах.

Правительство штата заявило, что DRF будет поддерживать эту трансформацию, поскольку он нацелен на продвижение «общесекторального подхода к оцифровке и трансформации услуг» и поддерживает создание рабочих мест за счет «повышения производительности и эффективности во всем секторе».

DRF уже был объявлен, и в бюджете на 2019-2020 годы предусмотрено начальное финансирование в размере 100 миллионов австралийских долларов, но в бюджете на 2020-2021 годы предусмотрены дополнительные инвестиции, в том числе в школьные технологии, цифровые суды, электронное планирование, доходы штата Новый Южный Уэльс и кибернетику.

Напомним, что правительство надеется закрыть «цифровой разрыв» между региональными и столичными школами за счет лучшей интеграции цифровых технологий в школьную программу и инфраструктуру, выделив на эту инициативу 366 миллионов австралийских долларов в течение двух лет.

Между тем, 54,5 миллиона австралийских долларов были выделены на крупный проект реформирования цифровых судов и трибуналов с целью оцифровки услуг, повышения производительности правовой системы, совершенствования процессов и улучшения качества обслуживания клиентов.

45,8 млн австралийских долларов будут использованы для реализации следующего этапа услуги сквозного цифрового планирования через программу электронного планирования, а 17,5 млн австралийских долларов из DRF было выделено на улучшение качества обслуживания клиентов в режиме онлайн для ключевых онлайн-сервисов Revenue NSW.

Также в рамках DRF зарезервировано 240 миллионов австралийских долларов для инициатив в области кибербезопасности, включая 60 миллионов австралийских долларов в течение следующих трех лет для Cyber Security NSW.

Cyber Security NSW отвечает за обнаружение, сканирование и управление онлайн-уязвимостями и данными в различных отделах и агентствах.

Бюджет также направлен на поддержку роста передового производственного сектора штата с помощью новой отраслевой стратегии, которая, как он надеется, может создать больше рабочих мест в целом ряде отраслей, включая оборону и

космос, и стимулировать развитие новых отраслей, таких как кибербезопасность, medtech и другие цифровые технологии.

В другом месте штат также инвестирует в меры цифрового здравоохранения, которые «основываются на ключевых успехах, достигнутых во время COVID-19», и далее модернизируют систему здравоохранения.

50,4 миллиона австралийских долларов будут использованы для предоставления поддержки сотрудникам с технологической поддержкой, включая удаленную видеоконференцсвязь и расширение услуг телемедицины и соответствующей инфраструктуры, чтобы обеспечить больший доступ к поддержке психического здоровья для людей, находящихся в непосредственной кризисной ситуации.

Также будет разработана интегрированная система управления лабораторной информацией в масштабе штата, чтобы обеспечить беспрепятственный заказ, обработку и отчетность по более чем 70 миллионам тестов в год в штате NSW Health; будет внедрена система мониторинга рецептов в реальном времени для отслеживания прописанных лекарств, связанных с высоким риском причинения вреда, зависимости или злоупотребления.

В надежде заложить основы активного восстановления экономики, правительство также провело ряд реформ производительности, которые призваны помочь частным лицам и предприятиям быстро адаптироваться к новой среде, облегчить ведение бизнеса за счет устранения препятствий для инвестиций и инноваций., а также использовать возможности COVID-19 и внедрять новые технологии.

«Деловые инвестиции будут иметь решающее значение для устойчивого восстановления», - говорится в документах. «Правительство Нового Южного Уэльса поддерживает предприятия, пострадавшие от COVID-19, в адаптации, внедрении инноваций и инвестировании в новые виды деятельности.

«Целенаправленное сокращение времени торговли и других нормативных требований, введенное правительством Нового Южного Уэльса в разгар пандемии, помогло предприятиям перейти на альтернативные модели и стимулировать внедрение новых технологий.

«Казначей проведет общегосударственную оценку затрат и выгод от сохранения некоторых из этих временных изменений, чтобы способствовать более сильному восстановлению».

Штат также выделяет до 500 миллионов австралийских долларов в рамках своей программы Out and About, чтобы стимулировать расходы в местной экономике, включая рестораны, туристические объекты и культурные достопримечательности. Каждый взрослый житель будет иметь право потребовать до 100 австралийских долларов в виде цифровых ваучеров, которые можно потратить на питание и развлечения.

Тем временем, выделив 472 миллиона австралийских долларов, штат предоставит малым и средним предприятиям, которые не платят налог на заработную плату, доступ к цифровому ваучеру на 1500 австралийских долларов, который можно использовать для покрытия расходов на любые государственные сборы и сборы до 30 июня 2022 года.

Ваучеры доступны через портал MyService NSW и действуют в качестве скидки, при которой требование может быть подано после оплаты сборов и сборов.

Service NSW потратит почти 103 миллиона австралийских долларов, чтобы добавить 1000 сотрудников для поддержки проектов и расширить возможности службы поддержки Service NSW для реагирования на растущий спрос и изменение потребностей клиентов во время COVID-19». ***(Asha Barbaschow. Service NSW expecting cyber attack to set it back AU$7m in legal and investigation costs // ZDNet (https://www.zdnet.com/article/service-nsw-expecting-cyber-attack-to-set-it-back-au7m-in-legal-and-investigation-costs/). 17.11.2020).***

***

«Киберпреступники все чаще преследуют фармацевтическую промышленность, нацеливая сотрудников на фишинговые и вредоносные кампании, направленные на использование потенциальных уязвимостей в системе безопасности смартфонов и планшетов.

Фармацевтические препараты сейчас являются чрезвычайно важной целью, поскольку фармацевтические компании пытаются разработать вакцину от COVID-19, и уже было зарегистрировано несколько случаев хакерских кампаний, поддерживаемых государством, с попытками украсть интеллектуальную собственность у медицинских исследовательских институтов.

Исследователи из компании Lookout, занимающейся кибербезопасностью мобильных устройств, говорят, что в течение этого года наблюдался всплеск мобильных фишинговых атак, направленных на сотрудников фармацевтических компаний, поскольку киберпреступники пытаются получить доступ к конфиденциальным данным.

Компания анализирует телеметрию безопасности с почти 200 миллионов мобильных устройств и более 125 миллионов мобильных приложений по всей своей клиентской базе: это заявление было сделано после анализа обезличенных и агрегированных данных от клиентов Lookout в фармацевтической отрасли.

Согласно отчету, одна из причин увеличения числа атак, нацеленных на мобильные устройства, связана с переходом на удаленную работу в результате пандемии коронавируса, что означает, что сотрудники внезапно стали больше полагаться на мобильные устройства, чтобы быть продуктивными при работе из дома.

Хотя электронная почта остается наиболее распространенным средством для фишинговых атак, широкий спектр приложений для обмена сообщениями и социальных сетей, которые люди используют на своих смартфонах, предоставляет хакерам ряд различных вариантов доставки индивидуальных сообщений и вредоносных ссылок.

«Поскольку большинство из нас использует личные мобильные устройства для работы, злоумышленники могут создавать нас в социальных сетях, используя бесчисленные каналы, такие как SMS, iMessage, сторонние платформы обмена сообщениями и платформы социальных сетей», - сказал Хэнк Шлесс, старший менеджер по решениям безопасности в Lookout.

"Злоумышленник может настроить свое фишинговое сообщение в зависимости от того, какой из этих вариантов он решит использовать. Поскольку наше мобильное устройство всегда при нас, мы также склонны доверять сообщениям, которые им отправляются, что делает мобильные фишинговые атаки более эффективными.," добавил он.

Во многих случаях целью фишинговых атак является сбор учетных данных, когда злоумышленник пытается обманом заставить жертву передать свое имя пользователя и пароль. Благодаря этому киберпреступник может войти в систему как сотрудник и перемещаться по сетевой инфраструктуре, пытаясь найти и украсть конфиденциальные данные.

Хакеры также атакуют смартфоны и планшеты людей, работающих в фармацевтике, с целью распространения вредоносного ПО - по словам исследователей Lookout, в этом году их количество увеличилось более чем вдвое.

Эти атаки пытаются обманом заставить жертву загрузить вредоносное ПО на свое устройство, что затем позволяет злоумышленнику тайно контролировать устройство в фоновом режиме, отслеживая активность пользователя и позволяя злоумышленникам получить доступ к файлам и дискам.

«В фармацевтике мобильные устройства используются по всей цепочке поставок, от исследований и разработок до испытаний и вплоть до производства и распространения. Поскольку в облачных сервисах хранится так много проприетарных данных, к которым можно получить доступ через смартфоны и планшеты, успешное использование может привести к к серьезным юридическим последствиям и последствиям для компании», - сказал Шлесс.

Злоумышленники пытаются доставить вредоносное ПО, в том числе троян Monokle, SilkBean и Wroba.

Одна из причин, по которой вредоносные программы доказали свою эффективность против мобильных устройств, заключается в том, что значительное число пользователей продолжают использовать устаревшие операционные системы.

Применение обновлений операционной системы и исправлений безопасности имеет большое значение для защиты пользователей от злонамеренных атак, но организации и отдельные пользователи часто не делают этого быстро, что потенциально позволяет хакерам использовать известные уязвимости, в которых есть исправления безопасности.

Чтобы помочь защитить сотрудников - и, следовательно, всю организацию - от жертв хакеров, нацеленных на смартфоны, обновления безопасности для мобильных устройств следует рассматривать как традиционные конечные точки и применять как можно быстрее.

«Чтобы полностью обезопасить персонал фармацевтических компаний, мобильные устройства должны быть включены в общую стратегию безопасности», - сказал Шлесс». ***(Danny Palmer. WFH leads to surge in mobile phishing and malware attacks targeting pharmaceuticals companies // ZDNet (https://www.zdnet.com/article/wfh-leads-to-surge-in-mobile-phishing-and-malware-attacks-targeting-pharmaceuticals-companies/). 18.11.2020).***

***

«Злоумышленники злоупотребляют бесплатными инструментами и службами Google для создания убедительных фишинговых кампаний, которые крадут ваши учетные данные или заставляют вас установить вредоносное ПО.

Google предлагает широкий спектр бесплатного программного обеспечения и услуг, которые позволяют пользователям создавать документы, электронные таблицы, онлайн-формы и бесплатные веб-сайты. Эти инструменты используются учащимися, преподавателями, потребителями и предприятиями как простой способ обмениваться документами, проводить опросы или даже создавать сайты бесплатно.

К сожалению, если услуга бесплатна для нас, злоумышленники также могут злоупотреблять ею по своему усмотрению.

Злоумышленники бесплатно злоупотребляют сервисами Google

В новом отчете компании Armorblox, занимающейся защитой электронной почты, исследователи демонстрируют, как злоумышленники создают сложные фишинговые кампании с использованием сервисов Google, которые не только выглядят убедительно, но и не обнаруживаются.

Первый инструмент Google, который мы рассмотрим, - это бесплатная служба создания форм под названием Google Forms, которая позволяет любому создавать бесплатные онлайн-опросы, которые затем можно отправлять другим пользователям.

Однако злоумышленники злоупотребляют формами Google для создания сложных форм, которые пытаются украсть ваши учетные данные, например, поддельную форму восстановления учетной записи American Express ниже. Затем злоумышленники могут собирать любую предоставленную информацию позже.

Google Firebase - это платформа для разработчиков, используемая для создания мобильных и веб-приложений, размещаемых в облаке.

Злоумышленники используют Firebase для создания фишинговых целевых страниц, которые могут включать изображения, динамический контент и формы обработки. Поскольку страницы Firebase используют общий URL https://firebasestorage.googleapis.com, Armorblox заявляет, что они не будут «заблокированы никакими фильтрами безопасности из-за присущей им легитимности»…

Google предлагает бесплатную платформу веб-хостинга под названием Google Sites, которая позволяет пользователям создавать упрощенные веб-сайты, обслуживаемые из домена sites.google.com.

В примере, предоставленном Armorblox, мы видим страницу Сайтов Google, на которой размещена поддельная форма входа в Microsoft для кражи учетных данных учетной записи Microsoft.

Наконец, наиболее распространенный сервис Google, используемый для фишинговых атак, - это Документы Google. Эта служба используется не только для перенаправления получателей на кражу учетных данных и мошенничество с бухгалтерским учетом, но и для доставки вредоносного ПО.

Поскольку Google Docs так широко используется, почти все новые документы будут обходить безопасные почтовые шлюзы, пока они не будут идентифицированы как вредоносные.

«Поскольку Документы Google всегда присутствуют в нашей повседневной жизни, средний получатель не удивится, увидев ссылку на Документы Google в электронном письме от коллеги. Она также не будет заблокирована никаким фильтром безопасности электронной почты - не в День 0 Во всяком случае. Использование Google Doc в этом электронном письме призвано обмануть как глазную проверку получателя, так и традиционные уровни безопасности», - поясняет Armorblox в своем отчете.

Например, вы можете увидеть поддельную страницу загрузки «расчетного листа», которая перенаправляет пользователей на страницу, которая крадет учетные данные.

Документы Google также активно используются в кампаниях вредоносных программ BazarLoader в качестве промежуточной страницы для загрузки вредоносных программ, замаскированных под счета, информацию о COVID-19 и другие типы документов.

Хотя этот отчет был посвящен злоупотреблению службами Google, злоумышленники также используют бесплатные службы других компаний, включая Dropbox, Canva и Azure.

Чтобы защитить себя от подобных фишинговых атак, Armorblox рекомендует:

Следуйте рекомендациям по 2FA и управлению паролями

Подвергайте чувствительные электронные письма тщательной проверке зрения, особенно когда это касается денег.

Создайте свои собственные строки аутентификации

Дополните встроенное обнаружение угроз электронной почты дополнительными средствами

Даже если вы будете следовать всем этим рекомендациям, крайне важно рассматривать все электронные письма со ссылками и вложениями как подозрительные.

Не просто нажимайте на ссылки или открывайте вложения, вместо этого сначала отсканируйте их или обратитесь к администратору сети, если вы не уверены. Также всегда полезно позвонить отправителю по телефону, чтобы подтвердить, отправил ли он электронное письмо.

Только убедитесь, что вы не используете номер телефона, указанный в электронном письме, так как это может быть номер злоумышленника». ***(Lawrence Abrams. Google's free services are now phishing campaign's best friends // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/google-s-free-services-are-now-phishing-campaign-s-best-friends/). 19.11.2020).***

***

«Неизвестные злоумышленники сканируют веб-сайты WordPress с темами Epsilon Framework, установленными на более чем 150 000 сайтов и

уязвимыми для атак внедрения функций, которые могут привести к полному захвату сайта.

«На сегодняшний день мы наблюдаем всплеск более 7,5 миллионов атак на более чем 1,5 миллиона сайтов, нацеленных на эти уязвимости, с более чем 18 000 IP-адресов», - сказал Рам Галл, инженер по обеспечению качества Wordfence и аналитик угроз.

Продолжающаяся широкомасштабная волна атак на потенциально уязвимые веб-сайты WordPress нацелена на недавно исправленные уязвимости.

Хотя недостатки безопасности, обнаруженные в течение последних нескольких месяцев в темах, использующих Epsilon Framework, могут позволить захват сайта через цепочку эксплойтов, заканчивающуюся удаленным выполнением кода (RCE), большинство этих продолжающихся атак предназначены только для исследования уязвимостей.

«В настоящее время мы не предоставляем дополнительных подробностей об атаках, поскольку эксплойт еще не находится в зрелом состоянии и используется большое количество IP-адресов», - добавил Галл.

«Эти атаки используют POST-запросы к admin-ajax.php и поэтому не оставляют отдельных записей в журнале, хотя они будут видны в Wordfence Live Traffic».

Уязвимые версии темы

Известно, что эти версии целевых тем Epsilon Framework уязвимы для следующих атак:

Стройный
NewsMag
Activello
Illdy
Allegiant
Газета X
Pixova Lite
Блеск
MedZone Lite
Регина Лайт
Превзойти
Богатый
Bonkers
Антреас
NatureMag Lite

Владельцам и администраторам веб-сайтов, на которых запущены уязвимые версии этих тем, рекомендуется немедленно обновить их до исправленной версии, если она доступна.

Если в настоящее время патч недоступен, им следует как можно скорее переключиться на другую тему, чтобы заблокировать попытки атаки.

В мае еще одна массовая атака была направлена на примерно 900 000 сайтов WordPress в течение одной недели, пытаясь создать бэкдоры или перенаправить посетителей на сайты, рекламирующие вредоносную рекламу.

Спустя месяц в ходе очередной серии атак была предпринята попытка сбора учетных данных базы данных примерно с 1,3 миллиона сайтов WordPress путем загрузки файлов конфигурации». ***(Sergiu Gatlan. Hackers are actively probing millions of WordPress sites // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-are-actively-probing-millions-of-wordpress-sites/). 17.11.2020).***

***

«Киберзлоумышленники, использующие продвинутые периметры сети (Intelligent Edge), устройства с поддержкой 5G и достижения в области вычислительной мощности устройств, создадут волну новых и сложных угроз, беспрецедентных по скорости и масштабу. Кроме того, злоумышленники будут атаковать не только базовые сети, а продолжат использовать значительные ресурсы для нацеливания на развивающиеся периферийные среды, такие как удаленные сотрудники или даже новые периферийные OT-среды.

Компания Fortinet представляет прогнозы ландшафта киберугроз на 2021 год и далее глобальной аналитической и исследовательской группы FortiGuard Labs.

«События 2020 года демонстрируют, что киберпреступники способны использовать драматические изменения, происходящие в нашей повседневной жизни, в качестве новых возможностей для атак беспрецедентного масштаба. В 2021 году и далее мы столкнемся с еще одним значительным сдвигом, связанным с появлением новых продвинутых периметров сети (Intelligent Edge), которые станут чем-то большим, чем просто пользователи и устройства, удаленно подключающиеся к сети. Нацеливание на эти развивающиеся периметры не только создаст новые векторы атак, но и группы скомпрометированных устройств, которые смогут работать согласованно, чтобы атаковать на скоростях 5G. Чтобы быть на шаг впереди злоумышленников в этой грядущей реальности, все периметры должны быть частью более крупной, интегрированной и автоматизированной платформы безопасности, которая объединяет базовые сети, мультиоблачные среды, филиалы и удаленных сотрудников» – Дерек Мэнки, руководитель отдела аналитики безопасности и Global Threat Alliances, FortiGuard Labs.

Продвинутый периметр сети (Intelligent Edge) – возможность и цель

За последние несколько лет традиционный периметр сети был заменен несколькими периферийными средами, WAN, мультиоблачными средами, центрами обработки данных, средствами удаленной работы, IoT и другими средами, каждая из которых имеет свои уникальные риски. Одним из наиболее значительных преимуществ для киберпреступников во всем этом является то, что, хотя все эти среды связаны между собой, многие организации пожертвовали централизованной видимостью и единым контролем в пользу производительности и цифровой трансформации. В результате киберпреступники планируют свои атаки, ориентируясь на эти среды, и будут использовать возможности скорости и масштабирования, которые открывает 5G.

Трояны развиваются, чтобы целиться в периферию. В то время как конечные пользователи и их домашние ресурсы уже являются целями для

киберпреступников, более изощренные злоумышленники будут использовать их в качестве трамплина для атак на другие цели в будущем. Атаки на корпоративные сети, инициированные из домашней сети удаленного сотрудника, можно эффективно координировать, чтобы они не вызывали подозрений, особенно если четко известны характерные особенности пользования. В конце концов, продвинутые вредоносные программы могут также обнаруживать еще более ценные данные и тенденции с помощью новых EAT (Edge Access Trojans – троян доступа к периферии) и выполнять инвазивные действия, такие как перехват запросов из локальной сети для компрометации дополнительных систем или введения дополнительных команд атаки.

Роевые атаки с поддержкой периферии. Взлом и использование новых устройств с поддержкой 5G откроет возможности для более сложных атак. Киберпреступники добиваются прогресса в разработке и развертывании угроз на основе роя. В этих атаках используются захваченные устройства, разделенные на подгруппы, каждая из которых обладает специальными навыками. Они нацелены на сети или устройства как на интегрированную систему и обмениваются данными в режиме реального времени для уточнения своей атаки по мере ее проведения. Технологии роя требуют больших вычислительных мощностей для включения отдельных роевых ботов и эффективного обмена информацией между ними. Это позволяет им быстро обнаруживать уязвимости, делиться и сопоставлять данные, а затем менять методы атаки, с учетом обнаруженной информации.

Социальная инженерия может стать изощреннее. Смарт-устройства или другие домашние системы, которые взаимодействуют с пользователями, больше не будут просто целями для атак, а станут проводниками для более глубоких атак. Использование важной контекстной информации о пользователях, включая распорядок дня, привычки или финансовую информацию, может сделать атаки на основе социальной инженерии более успешными. Такие изощренные атаки могут привести к гораздо большему ущербу, чем просто отключение систем безопасности, камер или захват смарт-устройств, они могут поспособствуют вымогательству денег или получению дополнительных данных, скрытым атакам с использованием учетных данных.

Атаки вымогателей на ОТ-периферии могут стать новой реальностью. Программы-вымогатели продолжают развиваться, и по мере того, как ИТ-системы все больше объединяются с системами операционных технологий (ОТ), особенно если говорить о критически важной инфраструктуре – еще больше данных, устройств и, к сожалению, жизней окажутся в опасности. Вымогательство, клевета и порча уже являются торговли на рынке программ-вымогателей. В будущем человеческие жизни окажутся под угрозой, когда полевые устройства и датчики на ОТ-периферии, которые включают в себя критически важные инфраструктуры, будут все чаще становиться целями киберпреступников на местах.

Инновации в производительности вычислений – также в поле зрения злоумышленников

Другие типы атак, нацеленных на развитие производительности вычислений и инновации в области связи, специально киберпреступников, также не за горами.

Эти атаки позволят злоумышленникам охватить новую территорию и заставят защитников опередить киберпреступников.

Продвинутый криптомайнинг. Вычислительная мощность важна, если киберпреступники хотят масштабировать будущие атаки с помощью возможностей машинного обучения и искусственного интеллекта. В конце концов, атаковав периферийные устройства из-за их вычислительной мощности, киберпреступники смогут обрабатывать огромные объемы данных и узнавать больше о том, как и когда они используются. Это также может повысить эффективность криптомайнинга. Заражение ПК, который захватывают из-за их вычислительных ресурсов, часто выявляется, поскольку использование ЦП напрямую влияет на работу конечного пользователя. Взломанные периферийные устройства могли бы быть гораздо менее заметными.

Распространение атак из космоса. Возможность подключения спутниковых систем и в целом телекоммуникационного оборудования в целом может стать привлекательной целью для киберпреступников. По мере того, как новые системы связи расширяются и начинают больше полагаться на сеть спутниковых систем, киберпреступники нацеливаются на эти структуры. В результате взлом спутниковых базовых станций и последующее распространение вредоносного ПО через спутниковые сети может дать злоумышленникам возможность потенциально нацеливаться на миллионы подключенных пользователей в любом масштабе или проводить DDoS-атаки, которые могут препятствовать жизненно важным коммуникациям.

Угроза квантовых вычислений. С точки зрения кибербезопасности квантовые вычисления могут создать новый риск – в будущем они смогут бросить вызов эффективности шифрования. Огромная вычислительная мощность квантовых компьютеров смогут расшифровать некоторые асимметричные алгоритмы. В результате организациям необходимо будет подготовиться к переходу на квантово-устойчивые криптоалгоритмы с использованием принципа crypto agility, чтобы обеспечить защиту текущей и будущей информации. Хотя обычный киберпреступник не имеет доступа к квантовым компьютерам, его имеют некоторые государства, поэтому возможная угроза будет реальна, если сейчас не приготовиться для противодействия ей путем использования принципа crypto agility.

ИИ будет иметь решающее значение для защиты от будущих атак

По мере того, как эти тенденции атак постепенно становятся реальностью, лишь вопрос времени, когда задействованные ресурсы станут товаром, доступным в виде услуг в даркнете, или как часть наборов инструментов с открытым исходным кодом. Следовательно, для защиты от этих типов атак в будущем потребуется тщательное сочетание технологий, людей, обучения и партнерских отношений.

ИИ необходимо развиваться. Развитие ИИ имеет решающее значение для защиты от новых атак в будущем. Нужно развить искусственный интеллект до следующего поколения. Это будет включать использование локальных обучающих узлов на базе машинного обучения как части интегрированной системы, подобной нервной системе человека. Технологии с продвинутым ИИ, которые могут

предвидеть, регистрировать и противодействовать атакам, должны стать реальностью в будущем, потому что кибератаки будущего будут происходить за микросекунды. Основная роль людей будет заключаться в обеспечении того, чтобы системы безопасности получали достаточно информации, чтобы не только активно противодействовать атакам, но и фактически предвидеть атаки, избежать их.

Партнерские отношения жизненно важны для будущего. Нельзя ожидать, что организации будут защищаться от киберпреступников в одиночку. Им нужно будет знать, кому сообщить об атаке, чтобы можно было поделиться «цифровыми отпечатками пальцев» и чтобы правоохранительные органы могли выполнять свою работу. Поставщики услуг кибербезопасности, организации, занимающиеся исследованием угроз, и другие отраслевые группы должны сотрудничать друг с другом для обмена информацией, а также с правоохранительными органами, чтобы помочь ликвидировать противоборствующие инфраструктуры для предотвращения будущих атак. Киберпреступники не имеют границ в Интернете, поэтому борьба с ними также должна выходить за рамки границ. Только совместными усилиями мы сможем переломить эту ситуацию

Задействование команд Blue Teams (эксперты, занимающиеся предотвращением атак): тактика, приемы и процедуры (TTP) злоумышленников, изучаемые командами по анализу угроз, например, методички для злоумышленников, могут быть переданы в системы ИИ для обнаружения моделей атак. Точно так же, когда организации освещают тепловые карты активных в настоящее время угроз, интеллектуальные системы смогут проактивно скрывать сетевые цели и размещать привлекательные ловушки на путях атаки. В конце концов, организации смогут отреагировать на любые попытки контрразведки до того, как они произойдут, что позволит Blue Teams сохранить превосходящий контроль. Такой вид обучения дает членам группы безопасности возможность улучшить свои навыки, защищая сеть». ***(Использование продвинутого периметра сети в качестве оружия кардинально изменит скорость и масштаб будущих кибератак // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5702485-FortiGuard-Labs-predskazyvaet-chto.html). 19.11.2020).***

***

«Хакерские форумы - богатый источник информации об угрозах.

Dark Web / Darknet продолжает оставаться средой, в которой злоумышленники могут делиться украденными учетными данными и обсуждать успешные атаки. Фактически, в последние недели была обнаружена раскрытая личная информация из разных мест, от образовательных организаций до баз данных избирателей в США. Несмотря на то, что киберпреступные группировки в сети подвергались серьезным атакам, киберпреступники стремятся избежать обнаружения.

Но так же, как в Dark Web много плохого, есть и хорошее - в основном в виде информации, которую можно использовать для защиты организаций от атак.

Поскольку они так сосредоточены на том, чтобы делать то, что правильно, исследователи часто упускают из виду дополнительные богатые источники информации о киберугрозах, которые злоумышленники по сути раздают при

взаимодействии в сети. Другими словами: чтобы защищаться как хороший парень, вы должны думать как плохой парень. Попадание в голову злоумышленника дает ключ к разгадке того, как и почему он действует.

Понимание даркнета / дарквеба

В общем, термины «даркнет» и «дарквеб» более или менее взаимозаменяемы, но есть некоторые нюансы. Когда люди ссылаются на Dark Web, они обычно говорят о хакерских сайтах в Интернете, к которым вы можете получить доступ из обычного веб-браузера. Когда говорят о даркнете, это означает, что вам нужно специальное программное обеспечение. Самым распространенным из них является браузер Tor, но есть и другие.

Погружение во тьму

Чтобы понять, как действуют хакеры, полезно изучить их территорию. Распространенным источником данных для анализа угроз являются форумы злоумышленников и торрент / луковицы, обычно в даркнете, где хакеры часто обсуждают, покупают и продают вредоносные программы, программы-вымогатели и предложения по отказу в обслуживании.

По очевидным причинам многие из этих форумов требуют, чтобы исследователи преодолели значительное количество препятствий, чтобы получить к ним доступ. Некоторые форумы требуют какой-либо оплаты; другие требуют, чтобы за вас поручились как за настоящего хакера. А иногда вам нужно доказать свою достойность, продемонстрировав свою способность кодировать проблему безопасности или создавать вредоносное ПО.

Большинство злоумышленников на этих форумах мотивированы не только денежной выгодой. Они тоже ищут славы. Они хотят публиковать и рекламировать свои знания на форумах, которые будут иметь наибольшее количество просмотров, и многие хотят продемонстрировать свои навыки. Обычно они демонстрируют частые атаки, нацеленные на массовое количество людей и организаций, а не узкие, конкретные, целевые атаки. Таким образом, методы, которыми обмениваются на этих форумах, помогают защитникам понять культуру злоумышленников и способы защиты от частых атак.

Текущие тренды

Форумы по атакам позволяют исследователям понять, что интересно злоумышленникам. Проникновение в сознание злоумышленника не только позволяет исследователям угроз предвидеть риски и действия в ходе атаки, но также помогает нам начать профилирование определенных киберпреступников. Угрожающее поведение во многом похоже на отпечатки пальцев и может быть очень полезным при обнаружении определенных угроз и защите от них.

Одна из тенденций на этих форумах по атакам, которая была популярна и вызвала много дискуссий за последние несколько месяцев, - это безопасность на различных платформах веб-встреч. Большинство этих дискуссий не имеют злого умысла и, вероятно, связаны с людьми, которые просто хотят понять или обсудить конкретную тему. Однако в некоторых редких случаях очевидно, что когда приложение получает достаточно болтовни, это происходит из-за того, что злоумышленники начинают исследовать уязвимости или тестировать код.

Исследователи угроз также используют текстовые дампы, содержащие имена пользователей, имена, пароли и другую информацию. Это часто случается с данными, когда киберпреступники или даже люди в вашей организации намеренно или непреднамеренно передают пароли или другую личную информацию (PII). Эти данные, конечно, могут поставить под угрозу всю вашу организацию. По крайней мере, организации должны проверить, не попали ли они в ловушку этих типов пакетов учетных данных и утечек данных.

Повторное складывание шансов

Кибератаки заведомо оппортунистичны, и им также нравится хвастаться своими победами. Поскольку исследователи угроз изо всех сил стараются опережать своих врагов, они часто упускают из виду ключевую информацию в даркнете и даркнете, которая могла бы им помочь. Изучение хакерских форумов и текстовых дампов - это лишь два способа, с помощью которых исследователи могут собрать ценную информацию, которая поможет им защитить сети, за которые они несут ответственность. По этой причине обучение исследователей кибербезопасности должно включать методы доступа к темному онлайн-миру, чтобы хорошие парни могли лучше понять, как действуют плохие парни, и победить их в своей собственной игре.

Другой ключевой частью этой экосистемы является роль правоохранительных органов. Исследователи угроз могут и должны работать с правоохранительными органами, чтобы делиться информацией об угрозах простым и доступным способом. Это должна быть улица с двусторонним движением. Борьба с киберпреступностью не может быть решена в одностороннем порядке только правоохранительными органами; это совместная ответственность, которая требует установления доверительных отношений между государственным и частным сектором». ***(Aamir Lakhani. Digging into the Dark Web: How Security Researchers Learn to Think Like the Bad Guys // Threatpost (https://threatpost.com/dark-web-security-researchers-bad-guys/161172/). 12.11.2020).***

***

«Группа ученых из Грацского технического университета, университета Бирмингема, а также Центра информационной безопасности имени Гельмгольца в Германии (CISPA) раскрыла детали новой атаки Platypus. Название – это акроним, образованный от «Power Leakage Attacks: Targeting Your Protected User Secrets». Platypus переводится на русский язык как «утконос», и такое название было выбрано из-за способности утконоса улавливать электрические токи своим клювом.

Атака Platypus и связанные с ней проблемы отслеживаются как CVE-2020-8694 (Linux + Intel), CVE-2020-8695 (Intel) и CVE-2020-12912 (Linux + AMD). Также нужно отметить, что исследование проводилось в рамках проекта, который частично финансировался Intel.

Атака полагается на эксплуатацию RAPL-интерфейса процессоров Intel (Running Average Power Limit), то есть использует компонент, который позволяет прошивкам и приложениям контролировать энергопотребление ЦП и DRAM. В сущности, RAPL позволяет понять, сколько электроэнергии потребляет процессор

для выполнения конкретных задач, и эта система годами использовалась для отслеживания и оптимизации производительности приложений и оборудования.

Platypus позволяет узнать, какие данные обрабатываются внутри ЦП, ориентируясь на значения RAPL и обнаруживать ключи шифрования, пароли, конфиденциальные документы и другие данные. Обычно доступ к такой информации защищен множеством систем безопасности, включая KASLR (рандомизации адресного пространства ядра) и аппаратно изолированные середы, такие как Intel SGX. Но Platypus позволяет обойти защитные механизмы, просто через наблюдение за изменениями энергопотребления.

В ходе проведенных исследователями тестов, обнаружилось, что за 20 секунд можно обойти KASLR, наблюдая за энергопотреблением в RAPL, а затем получить данные из ядра Linux.

В другом тесте удалось получить данные, которые обрабатывались в защищенных анклавах Intel SGX. Атака Platypus извлекала приватные ключи RSA из анклава SGX, и для этого потребовалось отслеживать данные RAPL в течение 100 минут. В свою очередь, для извлечения ключей шифрования AES-NI из анклава SGX и из пространства памяти ядра Linux, требуется от 26 до 277 часов.

По мнению исследователей, лучше всего Platypus работает против Linux-систем. Это связано с тем, что ядро Linux поставляется с фреймворком powercap — универсальным драйвером для взаимодействия с RAPL и другими API-интерфейсами, позволяющими отслеживать изменения энергопотребления.

Хотя атаки возможны и на устройства под управлением Windows и macOS, в этих случаях на целевые машины должно быть установлено приложение Intel Power Gadget, чтобы преступники могли взаимодействовать с RAPL-интерфейсом.

Вместе с тем атаки Platypus, нацеленные на анклавы Intel SGX, работают независимо от ОС.

Самая скверная новость заключается в том, что атаку Platypus можно провести удаленно. Злоумышленнику не понадобится физический доступ к целевой машине, вместо этого вредоносный код может быть скрыт внутри приложения, которое останется лишь каким-то образом установить на машину жертвы.

По данным ученых, Platypus работает против десктопных и серверных процессоров Intel. Кроме того, инженеры Intel сообщили, что атака затрагивает и некоторые мобильные и встроенные процессоры. Список процессоров Intel, для которых опасна атака Platypus, можно здесь.

В Intel уже подготовили обновленные версии микрокода, блокирующие атаки Platypus, и компания уже распространила их среди производителей, которые вскоре включат патчи в обновления для своих продуктов. Обновление также получило и ядро Linux.

В Intel подчеркивают, что специалистам компании неизвестно о фактических атаках, использующих Platypus. Более того, большинство процессоров, для которых Platypus является угрозой, — это новейшие модели, которые поддерживаются как Intel, так и производителями устройств. То есть обновления явно не заставят себя ждать.

Разумеется, авторы Platypus не имели возможности протестировать на уязвимость все устройства, доступные сегодня на рынке. Однако RAPL-интерфейс

в своих продуктах используют и другие производители, поэтому исследователи полагают, что им тоже может угрожать опасность. Так, один из специалистов рассказал журналистам ZDNet о том, что исследовательская группа провела ряд экспериментов на процессорах AMD, и тоже наблюдала утечку данных через потребление энергии. Та же проблема может касаться устройств на базе ARM, а другие производители, включая Nvidia, Marvell и Ampere, используют в своих продуктах весьма схожие с RAPL решения». ***(Мария Нефёдова. Атака Platypus позволяет воровать данные с процессоров Intel // Хакер (https://xakep.ru/2020/11/11/platypus/). 11.11.2020).***

***

«Американская телекоммуникационная компания Verizon опубликовала свой первый отчет о кампаниях по кибершпионажу, основанный на материалах Verizon Data Breach Investigations Report (DBIR) за семь лет и на более чем 14-летнем опыте, предоставленном специалистами Threat Research Advisory Center (VTRAC).

Как выяснили эксперты, в случаях кибершпионажа более 80% преступников действовали в интересах правительств стран и только 4% были связаны с организованной преступностью. Бывшие сотрудники компаний и организаций составили 2% от всех кибершпионов.

Наиболее пострадавшими от кибершпионажа отраслями за последние семь лет были: государственный сектор, производство, профессиональная деятельность, информация, горнодобывающая промышленность, коммунальные услуги, образование и финансовая отрасль. Больше всего кибератак пришлось на государственный сектор (31%), за которым следуют производственная (22%) и профессиональная отрасли (11%).

Основными целями компрометации во время кибершпионажа были персональные компьютеры и ноутбуки (88%), сотовые телефоны (14%) и web-приложения (10%). Самым распространенным видом скомпрометированной информации были учетные данные (56%), секреты (49%), внутренние документы (12%) и государственные тайны (7%).

В отчете говорится, что, хотя сеть организации может быть скомпрометирована за секунды, на обнаружение взлома могут уйти целые годы. В 91% случаев время компрометации составляло от нескольких секунд до дней, в 88% случаев на хищение данных преступникам требовалось от пары минут до недель, а на обнаружение 69% инцидентов у компаний ушло несколько месяцев или даже лет.

По словам представителей Verizon, документ должен послужить руководством для экспертов в области кибербезопасности, ищущих способы улучшить состояние киберзащиты своей организации и возможности реагирования на инциденты». ***(Более 80% киберщпионов действуют в государственных интересах // SecurityLab.ru (https://www.securitylab.ru/news/514161.php). 18.11.2020).***

***

«Эксперты исследовательского центра «Лаборатории Касперского» представили прогноз угроз на следующий год.

В 2021 году киберпреступники станут активно использовать в своих атаках последствия пандемии коронавируса, а наряду с COVID-19 трендом среди злоумышленников станет поиск брешей в новом поколении связи 5G, который станет более распространённым.

Как отмечают специалисты Global Research and Analysis Team, правительства разных стран станут чаще заявлять о причастности конкретной группы к той или иной атаке, информационно-технологические компании будут активнее преследовать брокеров эксплойтов нулевого дня в судебном порядке.

Другими трендами станут уже встречающиеся атаки с целью выкупа, когда у компаний шифруют данные и требуют заплатить за их восстановление, а кроме того активный переход на удалённую работу откроет для киберпреступников возможность активнее похищать личные данные. При этом последствия кибератак будут более разрушительными из-за повсеместного внедрения технологий и интернета в нашу жизнь.

Мир меняется очень быстро, и невозможно быть уверенным в том, что будет происходить завтра. Количество и сложность перемен, свидетелями которых мы стали и которые влияют на ландшафт угроз, могут привести к самым разным сценариям. В мире нет ни одной команды экспертов, которая имела бы исчерпывающее представление обо всех сложных кибератаках, но, как показал наш предыдущий опыт, мы способны предвидеть многие продвинутые угрозы и, как следствие, лучше готовиться к ним. Мы продолжим изучать тактики и методы злоумышленников, делиться тем, что узнали, и оценивать последствия обнаруживаемых целевых атак», — подчеркнул заместитель руководителя глобального центра исследований и анализа угроз «Лаборатории Касперского» Сергей Новиков…». ***(Максим Вершинин. Больше вреда и атаки на 5G: специалисты по кибербезопасности предупреждают о проблемах 2021 года // ООО «Фэшн Пресс» (https://www.popmech.ru/technologies/news-645763-bolshe-vreda-i-ataki-na-5g-specialisty-po-kiberbezopasnosti-preduprezhdayut-o-problemah-2021-goda/). 23.11.2020).***

***

«Чикагская компания, занимающаяся транспортными технологиями, Rand McNally, работает над восстановлением функциональности сети после кибератаки, поразившей ее системы в начале этой недели.

Rand McNally - американская компания, основанная в 1856 году, которая предоставляет ведущее программное обеспечение для оптимизации маршрута и управления автопарком перевозчикам, судоходным компаниям и сторонним поставщикам логистических услуг.

Компания также владеет облачной телематической платформой и распространяет производимые ею технологии подключенных транспортных средств, потребительские путешествия и образовательные продукты.

Некоторые системы отключены после атаки

«Недавно мы обнаружили нарушение работы некоторых частей нашей компьютерной сети», - говорится в сообщении компании в Facebook во вторник. «Мы начали немедленное расследование, которое включало отключение некоторых систем и работу со специалистами по компьютерной криминалистике, чтобы определить характер и масштаб события.

«Мы прилагаем все усилия, чтобы восстановить работоспособность наших систем. Благодарим вас за терпение и понимание и приносим извинения за любые неудобства».

В отдельном уведомлении, отправленном клиентам во вторник, Рэнд МакНалли сообщил, что нет никаких указаний на то, что данные клиентов были затронуты кибератакой.

Rand McNally не смог предоставить график восстановления или оценку того, сколько времени потребуется для восстановления работоспособности сети.

Кроме того, начиная с утра вторника, главный веб-сайт компании и сайт автопарка были отключены, чтобы на следующий день работать с ограниченной функциональностью.

Прямо сейчас на сайтах Рэнда МакНалли отображаются уведомления о сбоях, в которых говорится, что «мы обновляем наши системы сейчас и скоро вернемся к работе».

Клиенты могут запросить помощь с продуктами Fleet (TND 760/765, HD100, DC 200, DC 210) здесь, а с GPS и другой электроникой (TND, OverDryves, планшеты, гарнитуры) здесь через чат поддержки.

Ранее сегодня Rand McNally разослал пользователям своих электронных устройств регистрации (ELD) новое уведомление по электронной почте, в котором говорилось, что кибератака затронула только ее размещенные и сетевые системы.

«На навигационные функции наших устройств GPS это не повлияет - эти устройства продолжают работать, как и другая бытовая электроника», - добавили в компании.

«Обратите также внимание на то, что в нашем интернет-магазине возникают значительные задержки при доставке».

В процессе реагирования и восстановления мы помним о постоянно растущем уровне сложности этих инцидентов. Мы наняли опытных профессиональных консультантов, чтобы направлять наши усилия, и мы тщательно оцениваем любые риски. Мы сделали значительные шаги в направлении восстановления и продолжаем расследование, чтобы лучше понять инцидент и способы предотвращения сбоев в будущем. - Рэнд МакНалли

Платформа DriverConnect ELD не работает

Однако в заявлении, опубликованном для Land Line, представитель Рэнда Макнелли сказал, что платформа ELD компании не работает, и предложил использовать бумажное ведение журнала до восстановления пораженных систем.

Устройства ELD - это электронные бортовые журналы, которые должны использовать все водители, чтобы они не могли управлять автомобилем дольше, чем разрешено законом.

«Сеть, которая поддерживает нашу платформу DriverConnect ELD, не работает», - сказал представитель. «Согласно правилам FMCSA, мы инструктируем

автопарки и водителей использовать бумажное ведение журнала, пока мы не сможем восстановить наши системы».

«Мы заверяем вас, что мы фокусируем наши ресурсы на восстановлении функциональности нашей сети, чтобы возобновить предоставление всего спектра наших услуг».

Хотя Рэнд МакНелли не сделал официального заявления по этому поводу, кибератака, которая в настоящее время затрагивает его системы, демонстрирует все признаки атаки с использованием программ-вымогателей, начиная с крупномасштабных сбоев в работе и продолжающихся усилий по восстановлению сети…». ***(Sergiu Gatlan. Truck routing provider Rand McNally hit by cyberattack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/truck-routing-provider-rand-mcnally-hit-by-cyberattack/). 26.11.2020).***

***

«Киберпреступники, стремящиеся украсть личную информацию, травят граждан США электронными письмами, якобы отправленными правительственными учреждениями, предлагающими федеральную помощь.

Злоумышленники рассылают сообщения, якобы от органов федерального правительства, предлагающих финансовую помощь или помощь по безработице во время пандемии.

Персональные данные и учетные данные

Целью фишинговых кампаний является сбор личных данных, которые могут быть использованы для кражи личных данных, а также имен пользователей и паролей, которые могут быть использованы для атак с заполнением учетных данных.

В отношении одного вредоносного сообщения компания Inky, занимающаяся защитой электронной почты, сообщает, что киберпреступники заманивали жертв поддельной государственной программой, предлагающей денежные выплаты на сумму до 5800 долларов.

Ссылка на программу выглядит подозрительно, но нажатие на нее ведет к «угнанному домену, который выдает себя за федеральное правительство США», - говорится в сегодняшнем отчете Инки.

Форма на вредоносном сайте первоначально запрашивает у жертвы имя и дату рождения, чтобы получить доступ к другой форме, которая запрашивает дополнительную информацию, включая номер социального страхования, водительские права, адрес, почтовый индекс, штат, номер телефона и адрес электронной почты.

После заполнения всех данных мошенники благодарят жертву за предоставленную информацию и дают обещание связаться с ними «как можно скорее».

Второе фишинговое письмо - это предупреждение о подозрительной активности. Он олицетворяет программу помощи по безработице при пандемии (PUA), управляемую каждым штатом. Тот факт, что сообщение, похоже, исходит от федерального правительства, должен быть красным флагом.

Как и в предыдущем сообщении, ссылка в этом письме ведет на страницу, размещенную в домене, который был взломан.

Запрошенная здесь информация - это имя пользователя и пароль жертвы. После получения данных жертва перенаправляется в настоящую программу помощи по страхованию от безработицы Министерства труда США.

«Это всего лишь два примера фишинговых атак, соответствующих сегодняшним заголовкам. Презентации предназначены для того, чтобы загнать беспокойство обычных людей, которые вряд ли заметят небольшие несоответствия, орфографические ошибки и странные названия ссылок, пока не станет слишком поздно»- Inky» ***(Ionut Ilascu. Crooks impersonate US govt agencies offering financial aid // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/crooks-impersonate-us-govt-agencies-offering-financial-aid/). 24.11.2020).***

***

«Федеральное бюро расследований США (ФБР) предупреждает широкую общественность о рисках, связанных с недавно зарегистрированными доменами, связанными с ФБР, которые подделывают некоторые официальные веб-сайты федеральных правоохранительных органов.

Предупреждение поступило в виде публичного объявления, выпущенного сегодня через Центр жалоб на Интернет-преступления (IC3) ФБР.

«Федеральное бюро расследований (ФБР) выпускает это объявление, чтобы помочь общественности распознать и избежать подделки связанных с ФБР Интернет-доменов», - говорится в сообщении IC3 PSA.

«ФБР наблюдало, как неустановленные кибер-субъекты регистрировали многочисленные домены, подделывающие законные веб-сайты ФБР, что указывает на потенциал будущей оперативной деятельности».

Риски, связанные с подделкой доменов

Национальные государственные или финансово мотивированные злоумышленники часто используют подобные домены в атаках, предназначенных для сбора учетных данных и финансовой информации целей, для распространения вредоносных программ, а также для распространения ложной информации.

Поддельные домены, используемые в этом типе атак, обычно создаются с использованием версий легитимных доменов с ошибками или коммутируемых доменов верхнего уровня - в данном случае .com или .net вместо .gov, используемого официальным веб-сайтом правительства США ФБР.

Похожие домены, о которых предупреждает ФБР, также могут использоваться для создания поддельных электронных писем, которые позволят злоумышленникам убедить своих жертв щелкнуть и открыть вредоносные ссылки и веб-сайты.

Кроме того, «представители общественности могут неосознанно посещать поддельные домены в поисках информации о миссии, услугах или новостях ФБР», - добавляет ФБР.

«ФБР призывает всех представителей американской общественности критически оценивать веб-сайты, которые они посещают, и сообщения,

отправляемые на их личные и рабочие адреса электронной почты, для поиска надежной и проверенной информации ФБР».

ФБР также предоставляет список рекомендаций, чтобы помочь общественности обнаружить эти похожие домены, если они будут использоваться в будущих вредоносных кампаниях:

Проверьте написание веб-адресов, веб-сайтов и адресов электронной почты, которые выглядят заслуживающими доверия, но могут быть имитацией законных веб-сайтов, посвященных выборам.

Убедитесь, что операционные системы и приложения обновлены до самых последних версий.

Обновляйте антивирусное и антивирусное программное обеспечение и регулярно проводите сканирование сети.

Не включайте макросы для документов, загруженных из электронной почты, за исключением случаев крайней необходимости и после того, как убедитесь, что файл не является вредоносным.

Не открывайте электронные письма или вложения от неизвестных лиц. Не общайтесь с отправителями нежелательной электронной почты.

Никогда не предоставляйте личную информацию по электронной почте. Имейте в виду, что многие электронные письма с запросом вашей личной информации могут оказаться законными.

По возможности используйте надежную двухфакторную аутентификацию с использованием биометрических данных, аппаратных токенов или приложений аутентификации.

Используйте белый список доменов, чтобы разрешить исходящий сетевой трафик на веб-сайты, которые считаются безопасными.

Отключите или удалите ненужные программные приложения

Убедитесь, что посещаемый вами веб-сайт имеет сертификат Secure Sockets Layer (SSL).

Высокая вероятность использования в будущих атаках

PSA ФБР также содержит приложение с некоторыми примерами выявленных поддельных Интернет-доменов, связанных с ФБР, десятки таких доменов были обнаружены недавно и, возможно, готовятся к будущим атакам.

Хотя на данный момент нет никаких признаков того, что похожие домены уже использовались в атаках, они могут использоваться как хакерскими группами, поддерживаемыми государством, так и киберпреступниками в рамках шпионажа или финансово мотивированных кампаний, нацеленных на предприятия и частных лиц.

fbi-news.com, fbi-intel.com, fbimaryland.org, fbi-fraud.com, fbi-ny.com, fbi-gov.network, fbiusagov.com, fbiusgov.com, fbiusa.net, fbi-usa. us и fbihelp.org - это лишь некоторые из наиболее интересных и потенциально наиболее опасных, если они будут использоваться в будущих вредоносных кампаниях.

В прошлом месяце ФБР также предупредило о потенциальном использовании поддельных доменов Бюро переписи населения США в будущих вредоносных кампаниях по фишингу и краже учетных данных.

Защита доменов .gov от попыток незаконной регистрации

Раньше было довольно легко зарегистрировать поддельный домен .gov, но начиная с марта 2020 года правительство США значительно усложнило несанкционированным организациям или отдельным лицам возможность обхода официального процесса регистрации .gov.

Организации, которые хотят зарегистрировать домен .gov сейчас, должны использовать нотариально заверенные подписи в процессе регистрации для доменов .gov, чтобы блокировать попытки использования фальшивой информации в авторизационном письме, требуемом Администрацией общих служб США (GSA), которая курирует Программа DotGov.

Ранее в этом году Агентство кибербезопасности и безопасности инфраструктуры (CISA) также поделилось планами по передаче управления TLD .gov от GSA, учитывая, что «домен верхнего уровня .gov (TLD) является критически важной инфраструктурой для тысяч федеральных, государственные и местные правительственные организации по всей стране ".

В прошлом году в Сенат также был внесен двухпартийный законопроект, известный как «Закон DOTGOV от 2019 года», цель которого, среди прочего, предоставить CISA полномочия по управлению TLD .gov после принятия на себя управления со стороны GSA». ***(Sergiu Gatlan. FBI warns of recently registered domains spoofing its sites // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-warns-of-recently-registered-domains-spoofing-its-sites/). 23.11.2020).***

***

«Эксперты исследовательского центра «Лаборатории Касперского» составили прогнозы, как изменится ландшафт сложных киберугроз в 2021 году.

Одним из ключевых и наиболее опасных трендов они называют покупку APT-группами ресурсов для первичного проникновения в сеть жертвы у других злоумышленников. Так, в 2020 году было зафиксировано большое количество целевых атак программ-вымогателей, начинавшихся с того, что злоумышленники закреплялись в системе с помощью обычного, не узкоспециализированного вредоносного ПО. Оно часто оказывалось связано с подпольными интернет-магазинами типа Genesis, где продаются украденные учётные данные. Эксперты полагают, что атакующие продолжат применять такие схемы при проведении сложных целевых кампаний.

Организациям рекомендуется тщательно проверять любое вредоносное ПО и принимать меры реагирования на каждом скомпрометированном компьютере, чтобы противостоять установке в сети более сложных киберугроз.

Также эксперты отметили ещё ряд тенденций, которые, по их мнению, будут преобладать в следующем году:

- правительства разных стран всё чаще будут громко заявлять о причастности конкретной группы к той или иной атаке. Раскрытие информации о кибероружии через официальные каналы правительственных организаций позволит активнее бороться с кампаниями кибершпионажа, поскольку рассекреченные инструменты использовать сложнее;

• компании Кремниевой долины последуют примеру WhatsApp, подавшей иск в 2020 году из-за компрометации учётных записей пользователей сервиса, и будут всё чаще преследовать брокеров эксплойтов нулевого дня в судебном порядке;

• вырастет число целевых атак на сетевые устройства: в результате глобального тренда на удалённую работу злоумышленники сосредоточатся на эксплуатации уязвимостей сетевых устройств, таких как VPN-шлюзы, и будут собирать учётные данные пользователей с помощью методов социальной инженерии, например, вишинга;

• угрозы с требованием выкупа: на смену случайным, несистематическим атакам с широким кругом потенциальных жертв приходят целевые атаки, в которых злоумышленники шифруют данные конкретной организации и требуют от неё крупный выкуп. Они будут разрабатывать для таких операций сложные дорогостоящие инструменты;

• атаки станут более разрушительными: их поверхность расширяется, поскольку наша жизнь всё больше зависит от технологий и интернет-подключения;

• эксплуатация уязвимостей в технологии 5G: чем популярнее она будет становиться, тем активнее злоумышленники станут искать в ней бреши;

• кроме того, организаторы сложных киберкампаний продолжат наживаться на пандемии и использовать её для проникновения в целевые системы, поскольку COVID-19 будет глобально влиять на жизнь людей и в следующем году.

«Мир меняется очень быстро, и невозможно быть уверенным в том, что будет происходить завтра. Количество и сложность перемен, свидетелями которых мы стали и которые влияют на ландшафт угроз, могут привести к самым разным сценариям. В мире нет ни одной команды экспертов, которая имела бы исчерпывающее представление обо всех сложных кибератаках, но, как показал наш предыдущий опыт, мы способны предвидеть многие продвинутые угрозы и, как следствие, лучше готовиться к ним. Мы продолжим изучать тактики и методы злоумышленников, делиться тем, что узнали, и оценивать последствия обнаруживаемых целевых атак», — говорит Сергей Новиков, заместитель руководителя глобального центра исследований и анализа угроз «Лаборатории Касперского». ***(Каким будет ландшафт сложных угроз в 2021 году // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5703090-Kakim-budet-landshaft-slozhnyx-ugro.html). 23.11.2020).***

***

«В то время как 2021 год представит развивающиеся угрозы и новые вызовы, он также предложит новые инструменты и технологии, которые, как мы надеемся, изменят баланс в сторону защиты…

Программы-вымогатели будут развиваться

Кибератаки нарастали с годами, с приходом и уходом различных тенденций. В 2021 году программы-вымогатели почти наверняка останутся значительной частью портфеля злоумышленников, но киберпреступники будут продолжать «добавлять ценность», также крадя данные перед их шифрованием. Мы уже видели, как они использовали эту дополнительную тактику вымогательства, но это

станет еще большей проблемой в сфере здравоохранения, где злоумышленники могут использовать украденные записи пациентов, чтобы шантажировать пациентов, угрожая опубликовать истории болезни.

К сожалению, продолжающиеся атаки на систему здравоохранения и медицинскую инфраструктуру, вероятно, приведут к серьезным последствиям в 2021 году. Кто-то, скорее всего, умрет в результате кибератаки. Единственные положительные результаты здесь заключаются в том, что этот трагический сигнал тревоги станет импульсом, необходимым для усиления защиты в сфере здравоохранения и сделает правоохранительные органы более агрессивными в преследовании киберпреступников.

По мере того, как киберпреступники продолжают развивать свои бизнес-модели, они становятся все смелее и нацелены на более широкий круг отраслей. Они по-прежнему будут преследовать возможные цели как низко висящие плоды, но ожидают более целенаправленных атак на компании и отрасли, которые ранее не считали себя подверженными высокому риску. Сюда входят любые организации, не входящие в первую пятерку: финансовые службы, правительство, здравоохранение, высшее образование или энергетический сектор.

Нулевые дни и криптовалюта

Атаки нулевого дня на популярные операционные системы и приложения также будут оставаться проблемой. Разработчики в целом стали более осторожными, но все еще есть возможности для улучшения. Награды за обнаружение ошибок (предлагаемые основными поставщиками для улучшения кода), но злоумышленники будут продолжать использовать свою версию той же модели и предлагать высокие выплаты людям, которые продают им эксплойты.

Криптовалюта остается нестабильным псевдотоваром, который одобряют защитники конфиденциальности и преступники, в то время как правительственные органы ненавидят его. С точки зрения кибербезопасности майнеры криптовалюты стали обычной полезной нагрузкой для злоумышленников, которые просто ищут вычислительные ресурсы. Мы, вероятно, увидим больше из них в будущем.

Правительства уже работают над регулированием этого пространства, и в 2021 году может появиться законодательство, направленное на контроль, если не полный запрет, использование криптовалют. Правоохранительным органам по всему миру необходимо будет сотрудничать, если они хотят иметь хоть какой-то шанс справиться с постоянно растущим подпольем киберпреступников. Развитие бизнес-моделей преступников может облегчить их преследование правоохранительными органами.

Цунами Интернета вещей - и подключенные автомобили

Устройства Интернета вещей (IoT) будут по-прежнему оставаться незамеченными и незамеченными, поскольку они скомпрометированы. В отличие от более крупных устройств, таких как медицинские системы визуализации, небольшие устройства Интернета вещей останутся уязвимыми и не будут исправлены, если не исправлены, поскольку они становятся повсеместными. Злоумышленники найдут новые и более творческие применения для этих устройств, возможно, найдя способы использовать их для взлома облачных контроллеров, на которые они часто полагаются.

Мы можем ожидать или, скорее, беспокоиться о кибератаках против подключенных транспортных средств последнего поколения. Несмотря на то, что не было известных атак на обновления программного обеспечения транспортных средств по беспроводной сети, они будут вызывать все большую озабоченность по мере того, как все больше производителей внедряют эту технологию. Мы также можем увидеть атаки на системы автоматического вождения в той или иной форме.

Хотя атаки с подтверждением концепции могут быть не чем иным, как спуфингом системы автопилота для остановки для препятствий, которых нет, или следования дорожной разметке на парковку, существует возможность серьезных атак на датчики и программное обеспечение, которые активируют эти технологии.

Меры безопасности, применяемые для защиты этих передовых систем, затрудняют внешние атаки. То же самое касается облачных инфраструктур и более современных операционных систем. Наша защита улучшается, а это значит, что злоумышленники могут проникнуть внутрь, где смогут.

Будь то взяточничество или компрометация учетной записи - то, что мы видели в 2020 году и, вероятно, увидим больше в 2021 году, вектор внутренних угроз, вероятно, усилится. Это вызовет растущую озабоченность в цепочке поставок, поскольку злоумышленники могут атаковать более мелкие, менее зрелые организации на своем пути к компрометации последующих целей.

Хорошие новости: защита улучшится

Одна из причин, по которой мы увидим больше внутренних атак, заключается в том, что инструменты управления паролями и многофакторная аутентификация (MFA) станут более распространенными. Это поможет снизить скорость атак с целью взлома аккаунтов с помощью фишинга и кражи данных.

Эти инструменты очень эффективны для снижения угрозы со стороны скомпрометированных учетных записей, при этом MFA на основе токенов является более эффективным из двух, но с годами их использование медленно росло. Однако недорогие физические токены и программные эквиваленты делают их доступными. Принятие пользователей по-прежнему будет проблемой в новом году и, возможно, еще несколько лет.

Мы также, вероятно, увидим рост технологий управления доступом на основе рисков, когда инструменты аналитики безопасности используются, чтобы помочь решить, какой уровень аутентификации подходит для каждого конкретного случая. Это снизит нагрузку на пользователей, требуя дополнительной проверки подлинности только при необходимости, и усложнит задачу злоумышленникам за счет привязки методов анализа поведения к стеку безопасности. Это также связано с архитектурами с нулевым доверием, рост которых также ожидается в 2021 году и далее.

Аналитика безопасности как технология получит более широкое применение, поскольку она будет включена в существующие стеки безопасности путем плавного слияния с существующими решениями. Это станет еще более важным по мере того, как расширенное обнаружение и ответ (XDR) перейдет от первоначального определения, ориентированного на поставщика, к более открытой модели, не зависящей от поставщика. Модели поведенческой аналитики будут продолжать совершенствоваться, что позволит получать более точные результаты,

поскольку агенты конечных точек продолжают совершенствоваться и передавать в стек более качественную информацию.

Если нам повезет, мы увидим сверхлегкие агенты, которые смогут развертываться на устройствах Интернета вещей и расширять защиту конечных точек в этом уязвимом секторе. Мы также увидим более широкое распространение технологий обмана. Хотя они не могут предотвратить атаки, они могут служить надежным ранним предупреждением и дополнять остальную часть стека.

2020 год был трудным для кибербезопасности и для мира в целом. В то время как 2021 год представит развивающиеся угрозы и новые вызовы, он также предложит новые инструменты и технологии, которые, как мы надеемся, изменят баланс в сторону защиты». ***(Tara Seals. Cybersecurity Predictions for 2021: Robot Overlords No, Connected Car Hacks Yes // Threatpost (https://threatpost.com/cybersecurity-predictions-2021-robot-overlords-connected-car/161594/). 27.11.2020).***

***

«Компания Check Point Software Technologies предупреждает пользователей об угрозах QR-кодов. Их использование резко возросло во время пандемии Covid-19: например, рестораны стали использовать QR-коды, чтобы клиенты могли просматривать меню на своем смартфоне или совершать бесконтактные платежи. QR-коды также применяются для регистрации участников на разных мероприятиях с помощью приложений для отслеживания контактов.

В свою очередь хакеры стремятся воспользоваться популярностью QR-кодов, заменяя оригинальные QR-коды другим кодом, который при сканировании запускает вредоносный URL-адрес или пытается загрузить вредоносное ПО.

Ранее федеральная полиция Бельгии уже предупреждала о мошенничестве в интернете с использованием QR-кодов. При сканировании вредоносный код пытается получить доступ к учетным данным для входа, которые используются для самых разных приложений на смартфоне – банковских, онлайн-магазинов. Далее вредоносная программа пытается украсть эти данные или настроить несанкционированные транзакции. ING Bank в Нидерландах также предупредил о мошеннических QR-кодах, которые пытаются связать злоумышленника со счетами клиентов ING через банковское приложение.

Недавний опрос MobileIron показал, что с марта по сентябрь 38% респондентов сканировали QR-код в ресторане, баре или кафе, 37% – в магазине. Более половины (51%) респондентов заявили, что у них нет или им не известно, установлено ли на их смартфонах защитное ПО. Во многих случаях на этих устройствах установлены как личные, так и бизнес-приложения, содержащие важные даны, а это подвергает организации повышенным кибер-рискам. Отчет Check Point 2020 Cyber Security Report показал, что 27% организаций по всему миру подверглись кибератакам с использованием мобильных устройств. 34% были атакованы вредоносными программами для мобильных устройств». ***(Мошенники стремятся использовать возросшую популярность QR-кодов // Компьютерное Обозрение***

(https://ko.com.ua/moshenniki_stremyatsya_ispolzovat_vozrosshuyu_populyarnost_qr-kodov_135443). 27.11.2020).

***

Діяльність хакерів та хакерські угруповування

«Исследователи обнаружили всемирную кампанию, нацеленную на компании, использующие недавно обнаруженную уязвимость ZeroLogon.

Считается, что активная кибератака является делом рук Cicada, которую также отслеживают как APT10, Stone Panda и Cloud Hopper.

Исторически группа угроз - впервые обнаруженная в 2009 году и которая, по мнению США, может спонсироваться правительством Китая - нацелена на организации, связанные с Японией, и эта последняя волна атак, похоже, ничем не отличается.

Исследователи Symantec задокументировали компании и их дочерние компании в 17 регионах, связанные с автомобильной, фармацевтической, инженерной отраслью и производителями управляемых услуг (MSP), которые недавно стали мишенью Cicada.

По данным компании, последняя волна атак Cicada была активна с середины октября 2019 года и продолжалась как минимум до октября этого года.

Cicada, похоже, хорошо обеспечена ресурсами и использует множество инструментов и техник. Это включает в себя боковую загрузку DLL, сетевую разведку, кражу учетных данных, утилиты командной строки, способные устанавливать корневые сертификаты браузера и декодировать данные, сценарии PowerShell, а также архивирование RAR и законного поставщика облачного хостинга для загрузки, упаковки и извлечения украденных Информация.

Особо следует отметить недавнее добавление в инструментарий хакерской группы; инструмент, способный использовать ZeroLogon. Уязвимость, отслеживаемая как CVE-2020-1472, получившая оценку 10 по CVSS, раскрытая и исправленная Microsoft в августе, может использоваться для подделки учетных записей контроллеров домена и взлома доменов, а также для компрометации служб идентификации Active Directory.

Cicada также запустила Backdoor.Hartip, специальную форму вредоносного ПО, которое ранее не использовалось в связи с APT, против своих целей.

Похоже, что группировка ориентирована на кражу информации и кибершпионаж. Интересующие данные - включая корпоративные записи, кадровые документы, служебные записки и информацию о расходах - часто упаковываются и отправляются на серверы управления и контроля (C2) Cicada.

«Время, которое злоумышленники проводят в сетях жертв, различается: злоумышленники проводят значительное количество времени в сетях одних жертв и всего несколько дней в сетях других жертв», - говорят исследователи. «В некоторых случаях злоумышленники тоже проводили некоторое время в сети, но затем активность прекращалась, но через несколько месяцев возобновлялась».

Кампания была оценена Cicada со "средней" степенью уверенности из-за подсказок о том, как скрывается код; использование боковой загрузки DLL и имен DLL, включая «FuckYouAnti», что было ранее задокументировано в отчете Cylance по тому же APT. Кроме того, окончательная полезная нагрузка объединяет QuasarRAT, который в прошлом использовался Cicada, а также Backdoor.Hartip.

«Очевидно, что Cicada по-прежнему имеет доступ к большому количеству ресурсов и навыков, позволяющих проводить сложную и широкомасштабную кампанию, подобную этой, поэтому группа остается очень опасной», - говорит Symantec. «Использование им инструмента для эксплуатации недавно обнаруженной уязвимости ZeroLogon и настраиваемого бэкдора [...] показывает, что он продолжает развивать свои инструменты и тактику для активного нацеливания на своих жертв». ***(Charlie Osborne. Hacking group exploits ZeroLogon in automotive, industrial attack wave // ZDNet (https://www.zdnet.com/article/cicada-hacking-group-exploits-zerologon-launches-new-backdoor-in-automotive-industry-attack-wave/). 18.11.2020).***

***

«Новая хакерская группа, спонсируемая Китаем (также известная как APT), за последние два года заразила вредоносным ПО более 200 систем в Юго-Восточной Азии.

Вредоносные инфекции являются частью широкомасштабной кибер-шпионаж кампании, проведенной группой под названием FunnyDream, согласно новому докладу, опубликованного сегодня охранной фирме Bitdefender.

Атаки в первую очередь были нацелены на правительства Юго-Восточной Азии. Хотя Bitdefender не назвал ни одной страны-жертвы, в отчете, опубликованном ранее этой весной другой компанией, занимающейся безопасностью, Kaspersky Lab определены цели FunnyDream в Малайзии, Тайване и на Филиппинах, причем большинство жертв находится во Вьетнаме.

И Bitdefender, и Kaspersky заявили, что группа по-прежнему активна даже сегодня и, похоже, в первую очередь заинтересована в кибершпионаже, концентрируясь на краже конфиденциальных документов с зараженных хостов, уделяя особое внимание национальной безопасности и промышленному шпионажу.

ПОДОБНЫЕ АТАКИ, ДАТИРУЕМЫЕ 2018 ГОДОМ

Согласно Bitdefender, большинство этих атак следовали простой схеме и объединяли три вредоносных программы - Chinoxy, PCShare и FunnyDream (вредоносное ПО, в честь которого была названа группа).

У каждого из трех штаммов вредоносных программ определенная роль. Chinoxy был развернут в качестве исходного вредоносного ПО, выступая в качестве простого бэкдора для первоначального доступа.

PCShare, известный китайский троян удаленного доступа с открытым исходным кодом, был развернут через Chinoxy и использовался для исследования зараженных хостов.

FunnyDream был развернут с помощью PCShare и был наиболее мощным и многофункциональным из трех, имел более продвинутые возможности сохранения и связи и использовался для сбора и эксфильтрации данных.

"Даже глядя на график использования инструмента, мы видим, что злоумышленники начали с развертывания ряда инструментов, предназначенных для быстрого и скрытого исследования и эксфильтрации данных, а затем решили использовать полный набор инструментов, в частности, набор инструментов FunnyDream, для длительного наблюдения. ", - сказала ZDNet Ливиу Арсен, исследователь глобальной кибербезопасности Bitdefender.

«Мы стали свидетелями компрометации государственной инфраструктуры и многолетнего упорства, нестандартных инструментов для эксфильтрации и использования инструментов для выживания за пределами земли - все это указывает на шпионскую кампанию, потенциально политически мотивированную», - добавил Арсен.

"Учитывая, что Юго-Восточная Азия столкнулась с множеством экономических и торговых проблем, связанных с переносом цепочек поставок из Китая в Юго-Восточную Азию, а также с повышением американо-китайских тарифов, эти усилия могут быть частью потенциальных китайских кампаний APT, направленных на правительственные учреждения Юго-Восточной Азии. для потенциального шпионажа, направленного на выяснение того, как правительства в регионе планируют действовать в этих изменениях.

«Некоторые страны в регионе даже пережили недавние выборы и изменения в управлении, все из которых могут заслужить интерес со стороны потенциальных китайских APT-групп с точки зрения того, как местные режимы могут идеологически и политически согласоваться с интересами Китая», - сказал ZDNet исследователь Bitdefender». ***(Catalin Cimpanu. More than 200 systems infected by new Chinese APT 'FunnyDream' // ZDNet (https://www.zdnet.com/article/more-than-200-systems-infected-by-new-chinese-apt-funnydream/). 17.11.2020).***

***

«На этой неделе сайт Vote Joe, созданный президентской кампанией Байдена-Харриса, был взломан и испорчен турецким хакером по имени RootAyyildiz.

Судя по свидетельствам и архивным снимкам сайта, взлом и искажение длились более 24 часов.

Сайт "Голосуй за Джо" поврежден на этой неделе

Примерно до 9 ноября, через несколько дней после президентских выборов в США в 2020 году, сайт vote.joebiden.com будет перенаправлять на iwillvote.com, согласно Wayback Machin e.

Однако на этой неделе сайт Vote Joe был захвачен, искажен и начал показывать сообщение на турецком языке, написанное злоумышленниками.

Хотя сайт Vote Joe теперь отключен, BleepingComputer заметил, что Google продолжает кэшировать поврежденную копию на момент написания.

Согласно заметке, оставленной хакерами на взломанном сайте, ответственность за взлом взял на себя RootAyyildiz.

Наряду с этим упоминаются и другие имена пользователей и псевдонимы, такие как «MarbeyliWerom», «b4rbarøssa», «oneshot» и «Turkish And Muslim Defacer».

Хакер утверждает, что они «не группа», а одинокий любитель родины.

В английском переводе сообщения прямо указано, что хакеры, стоящие за взломом, не являются «группой», несмотря на несколько псевдонимов, перечисленных в примечании.

«RootAyyildiz - это не группа или организация, а любитель Ватана, который сражается в одиночку», - говорится в переводе.

Ватан и Ватан - это слова, обозначающие «родину» или «родину» в арабском, турецком, урду и подобных языках.

Это искажение является турецким посланием, предупреждающим "поддерживаемые США так называемые политические партии, такие как хорошая партия chp hdp", чтобы они прекратили попытки влиять на политику в Турции.

В записке также содержится фотография 34-го султана Османской империи Абдул Хамида II.

Мелкий шрифт под фотографией, вероятно, является отсылкой к неудавшемуся государственному перевороту в Турции 15 июля 2016 года…

На момент написания BleepingComputer обнаружил, что домен vote.joebiden.com больше не доступен.

Хотя неизвестно, какой недостаток безопасности привел к повреждению сайта, это не первый случай уязвимости веб-службы президентской кампании…». ***(Ax Sharma. Joe Biden's 'Vote Joe' website defaced by Turkish Hackers // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/joe-bidens-vote-joe-website-defaced-by-turkish-hackers/). 21.11.2020).***

***

«Группа хакеров, спонсируемая Китаем, была замечена при попытке использовать уязвимость Windows Zerologon в атаках на японские компании и дочерние компании из различных секторов промышленности в 17 регионах по всему миру.

Эту глобальную кампанию кибершпионажа приписывают хакерам, поддерживающим государство APT10, на основании информации, собранной командой Symantec Threat Hunter Team, подразделением Broadcom, которое отслеживало атаки.

Атаки были обнаружены исследователями Symantec после обнаружения подозрительной загрузки сторонней библиотеки DLL в сети клиента.

«Первоначальное предупреждение Cloud Analytics позволило нашей команде по поиску угроз выявить дальнейших жертв этой деятельности, составить более полную картину этой кампании и связать эту деятельность с Cicada», - сказали в Symantec.

Жертвы кампании

Хакеры APT10 проводили эту кампанию примерно целый год, по крайней мере, с середины октября 2019 года до начала октября 2020 года.

В некоторых случаях субъекты APT10 оставались активными и незамеченными в сетях своих жертв в течение почти целого года, показывая, что у них есть инструменты и изощренность, чтобы эффективно скрывать свою вредоносную деятельность.

«Пострадавшие в основном крупные, хорошо известные организации, многие из которых связаны с Японией или японскими компаниями, что является одним из основных факторов, связывающих жертв», - поясняет Symantec.

Приведенная ниже карта показывает, что атаки APT10 также были нацелены на фирмы в пределах границ Китая, но эта компания была дочерней компанией японской фирмы, как и многие другие цели в этой кампании.

Среди информации, используемой для атрибуции атак, исследователи Symantec также упоминают настраиваемые загрузчики, используемые для доставки вредоносных полезных данных во все сети целей.

Также было замечено, что они использовали аналогичные методы запутывания, живые вне земли инструменты и конечную полезную нагрузку QuasarRAT (бэкдор, обычно используемый APT10), а также скоординированный таргетинг на несколько организаций одновременно.

Также было замечено, что злоумышленники APT10 использовали эксплойты Zerologon для кражи учетных данных домена и получения полного контроля над всем доменом после успешной эксплуатации уязвимых устройств.

Эта уязвимость также активно использовалась в атаках поддерживаемой Ираном хакерской группы MuddyWater (известной также как SeedWorm и MERCURY), начиная со второй половины сентября, и финансово мотивированной группы угроз TA505 (Chimborazo).

Время, проведенное злоумышленниками в скомпрометированных сетях, сильно варьировалось от нескольких дней до почти целого года, причем в некоторых случаях активность возобновлялась после месяцев полного молчания.

Китайские хакеры нацелены на Five Eyes

APT10 (также известный как Menupass, Stone Panda, Cloud Hopper) был активен по крайней мере с 2009 года и исторически нацелился на правительственные организации и частные компании из США, Европы и Японии.

Они известны тем, что сосредотачиваются на краже военной, разведывательной и деловой информации с взломанных целей и часто сосредотачивают свои атаки на японских организациях.

Правительство США предъявило обвинение двум хакерам APT10 в декабре 2018 года, показав, что группа успешно взломала Лабораторию реактивного движения НАСА, правительственные учреждения США, поставщиков управляемых услуг (MSP), включая IBM и Hewlett Packard Enterprise.

Хакеры APT1 также взломали системы Министерства военно-морского флота США, чтобы украсть конфиденциальную информацию более чем 100 000 человек.

После этого обвинения все страны, входящие в Five Eyes Intelligence Alliance (США, Канада, Великобритания, Новая Зеландия и Австралия), опубликовали заявления, приписывающие кражу интеллектуальной собственности и конфиденциальных коммерческих данных китайской APT-группе.

Такеши Осуга, пресс-секретарь министерства иностранных дел Японии, также сказал, что «Япония выявила постоянные атаки группы, известной как APT10, на различные внутренние цели… и выражает решительное осуждение таких атак».

Японские фирмы также являются ценными целями вымогателей.

По меньшей мере 11 японских компаний стали жертвами атак программ-вымогателей в период с июня по октябрь 2020 года, согласно отчету, опубликованному сегодня израильской разведывательной компанией KELA.

«Пострадавшие компании представляют производственную, строительную и государственную промышленность, при этом основные пострадавшие имеют около 143 миллиардов долларов, 33 миллиардов долларов и 2 миллиарда долларов годового дохода», - сказали в KELA.

С июня 2020 года сети нескольких других японских организаций также были скомпрометированы, включая, но не ограничиваясь, корпорации, университеты и нераскрытое японское министерство. Этот доступ очень легко может быть использован членами банды вымогателей для доставки полезной нагрузки и шифрования систем.

Что еще хуже и чтобы показать риски, с которыми сталкиваются японские организации из всех секторов, KELA также обнаружила данные, принадлежащие японским корпорациям, правительству и образовательным организациям, которые либо активно используются в даркнете, либо пользуются большим спросом.

«Все больше и больше участников угроз, группы Advanced APT и национальные государства рассматривают японские организации как ценные цели и активно атакуют их с помощью оппортунистических и целевых атак», - заключает KELA». ***(Sergiu Gatlan. Chinese APT10 hackers use Zerologon exploits against Japanese orgs // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/chinese-apt10-hackers-use-zerologon-exploits-against-japanese-orgs/). 18.11.2020).***

***

«Новая группа наемных хакеров, которую исследователи BlackBerry называют CostaRicto, продает свои услуги организациям, которым требуется опыт взлома на уровне APT в кампаниях кибершпионажа, охватывающих весь земной шар и нацеленных на множество секторов промышленности.

Набор инструментов этой группы наемных хакеров включает в себя нестандартные и невиданные ранее вредоносные программы, а также использование туннелей SSH, созданных в сетях их жертв, и прокси-серверов VPN, что позволяет им избегать обнаружения и скрывать свою вредоносную активность.

«Учитывая неоспоримый успех программы-вымогателя как услуги (RaaS), неудивительно, что рынок киберпреступников расширил свой портфель, добавив в список предлагаемых услуг специальные кампании по фишингу и шпионажу». - заявили исследователи из группы BlackBerry Research and Intelligence.

"Передача атак или определенных частей цепочки атак независимым группам наемников имеет ряд преимуществ для злоумышленника - это экономит его время и ресурсы и упрощает процедуры, но, что наиболее важно, он обеспечивает дополнительный уровень косвенного обращения, который помогает защитить настоящую личность. злоумышленника ".

Нацеливание на любого добавленного на их радаре

Наемники APT атаковали организации практически со всех континентов, включая Европу (Франция, Нидерланды, Австрия), Азию (Китай), Америку (США) и Австралию, с упором на цели из Южной Азии (Индия, Бангладеш и Сингапур)..

Такое сочетание целей из разных стран можно объяснить различными задачами, выполняемыми различными организациями, потенциально включая крупные организации и даже правительства.

Их атаки, направленные на Южную Азию, дают некоторые подсказки относительно операционной базы CostaRicto, откуда они запускают кампании кибершпионажа от имени клиентов.

Жертвы CostaRicto происходят из самых разных отраслей и «различаются по нескольким вертикалям, большая часть из которых - финансовые учреждения».

Группа была активна по крайней мере с октября 2019 года на основе временных меток вредоносных программ CostaRicto, хотя некоторые из их стадий полезной нагрузки устарели с 2017 года, что свидетельствует о том, что они использовались в предыдущих кампаниях, но для доставки других вредоносных полезных нагрузок.

«Передача шпионской кампании или ее части группе наемников может быть очень привлекательной, особенно для предприятий и частных лиц, которые ищут информацию о своих конкурентах, но могут не иметь необходимых инструментов, инфраструктуры и опыта для проведения атаки самостоятельно», Сказал BlackBerry.

«Но даже печально известные злоумышленники, имеющие опыт кибершпионажа, могут извлечь выгоду из добавления уровня косвенности к своим атакам. Используя наемника в качестве своего представителя, настоящий злоумышленник может лучше защитить свою личность и предотвратить попытки атрибуции».

Набор инструментов для взлома CostaRicto

Чтобы получить доступ к сетям своих жертв, хакеры используют неизвестный вектор проникновения, но BlackBerry заявляет, что возможны украденные учетные данные, фишинговые или купленные из неизвестных источников.

Попав внутрь, они развертывают удаленные туннели SSH и stager полезной нагрузки HTTP и обратного DNS, используемые для развертывания невиданного ранее бэкдора, получившего название Sombra.

Бэкдор доставляется в скомпрометированные системы через отражающий загрузчик PowerSploit или специально созданный дроппер на основе виртуальной машины, известный как CostaBricks.

Управляя своими командно-контрольными серверами с помощью комбинации соединений Tor и уровня прокси, CostaRicto также демонстрирует «операционную безопасность выше среднего».

«Набор инструментов, используемый в кампании CostaRicto, состоит из специально созданного вредоносного ПО, которое появилось примерно в октябре 2019 года и с тех пор редко встречается в открытом доступе. Следовательно, оно, по-видимому, является личным для этого конкретного противника», - объясняет BlackBerry.

«Более того, постоянная разработка, подробная система управления версиями и хорошо структурированный код, позволяющий легко расширять функциональность - все это говорит о том, что набор инструментов является частью долгосрочного проекта, а не разовой кампании». ***(Sergiu Gatlan. New stealthy hacker-for-hire group mimics state-backed attackers // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-stealthy-hacker-for-hire-group-mimics-state-backed-attackers/). 13.11.2020).***

***

«Group-IB, международная компания, специализирующаяся на предотвращении кибератак, приняла участие в операции Интерпола Falcon по пресечению деятельности киберпреступников из Нигерии. Группа, названная специалистами Group-IB TMT, несколько лет совершала массовые взломы корпоративной почты и похищала аутентификационные данные пользователей из браузеров, электронной почты и FTP-серверов, в том числе на продажу. Об успешной операции сообщил Интерпол.

Преступники, действующие как минимум с 2017 г., скомпрометировали не менее 500 тыс. государственных и частных компаний в более чем 150 странах, в том числе России. В результате трансграничной операции, в которой участвовали Управление по борьбе с киберпреступностью Интерпола, полиция Нигерии и компания Group-IB (отдел по расследованию международных киберпреступлений, Сингапур) в Лагосе были арестованы три киберпреступника. Расследование продолжается, некоторые участники преступной группы до сих остаются на свободе.

Группа занималась BEC-атаками (от англ. business email compromise – компрометация деловой почты) – это тип фишинг-атаки, основанный на социальной инженерии. Фишинговые электронные письма могут быть нацелены на определенных сотрудников организации или рассылаться массово. Они часто маскируются под запросы денежных переводов, сообщения от HR-департамента или коммерческие предложения и предназначены для кражи конфиденциальных данных.

Три члена группы, известные под инициалами «OC» (32 года), «IO» (34 года) и «OI» (35 лет), личности которых были установлены благодаря использованию технологий слежения за киберпреступниками Group-IB, а также оперативной работе международной команды расследований Group-IB и центра реагирования на инциденты кибербезопасности CERT-GIB, были арестованы в Лагосе нигерийским отделом киберполиции в рамках операции Falcon. По сообщению представителей нигерийской полиции, сведения, обнаруженные на устройствах арестованных членов группы TMT, подтвердили их причастность к преступной схеме и содержали данные, принадлежащие, как минимум, 50 тыс. пострадавших.

Эксперты Group-IB отслеживали активность группировки с 2019 г. и установили, что члены TMT могли скомпрометировать около 500 тыс. государственных и частных компаний. Проанализировав инфраструктуру и техники злоумышленников, специалисты смогли установить, что группа состоит из нескольких подразделений, а ряд ее членов до сих пор находится на свободе.

Информация о предполагаемых злоумышленниках, которых Group-IB смогла отследить, была передана в Управление по борьбе с киберпреступностью Интерпола.

Анализ деятельности киберпреступников показал, что группа, маскируясь под бренды различных организаций, использовала массовые фишинговые рассылки для доставки популярных вредоносных программ под видом заказов на закупку, запросов данных о товарах и даже предложений помощи в борьбе с коронавирусом:

Для рассылки фишинговых писем злоумышленники использовали инструменты Gammadyne Mailer и Turbo-Mailer. Кроме того, они пользовались платформой MailChimp, чтобы узнать, открыла ли жертва полученное сообщение.

Специалисты Group-IB отмечают, что группа использовала ранее взломанные почтовые аккаунты для новых фишинговых атак. Образцы электронных писем, обнаруженные и проанализированные системой Group-IB Threat Hunting Framework, были написаны на английском, русском, испанском и других языках, в зависимости от атакуемых целей.

Исследователи Group-IB считают, что киберпреступники, стоящие за этими кампаниями, используют исключительно общедоступные шпионские программы и трояны удаленного доступа (RAT), такие как AgentTesla, Loky, AzoRult, Pony, NetWire. Чтобы избежать обнаружения и отслеживания традиционными системами безопасности, группа использует публичные крипторы. Для коммуникации с командным сервером злоумышленники, в частности, применяли протоколы SMTP, FTP, HTTP.

Цель группы – кража аутентификационных данных из браузеров, электронной почты и FTP-клиентов. Как отмечают Group-IB, в ходе своей деятельности злоумышленникам удалось скомпрометировать организации по всему миру, в том числе в США, Великобритании, Сингапуре, Японии, России и даже у себя «дома» в Нигерии. Хотя специалисты продолжают изучать методы монетизации украденных данных, уже известно, что киберпреступники скорее всего продавали доступ к аккаунтам, а также конфиденциальные данные, извлеченные из электронных писем, на хакерских форумах тем, кто предлагал самую высокую цену…». ***(Group-IB помогла Интерполу выявить преступников из Нигерии, атаковавших компании по всему миру // CNews (https://safe.cnews.ru/news/line/2020-11-26_groupib_pomogla_interpolu_vyyavit). 26.11.2020).***

***

«APT TA416 вернулся в виде целевых фишинговых атак против ряда жертв - от Ватикана до дипломатов в Африке - с новой версией Golang своего загрузчика вредоносных программ PlugX.

Актер TA416 с расширенной постоянной угрозой (APT) вернулся с удвоенной силой: после месяца бездействия группа была замечена в проведении целевых фишинговых атак с использованием ранее не использовавшегося варианта Golang своего загрузчика вредоносных программ PlugX.

TA416, также известный как «Mustang Panda» и «RedDelta», был замечен в недавних кампаниях, нацеленных на организации, связанные с дипломатическими

отношениями между Ватиканом и Коммунистической партией Китая, а также на организации в Мьянме (все это кампании, о которых сообщалось ранее.). Группа также была недавно замечена в качестве мишеней для организаций, ведущих дипломатическую деятельность в Африке.

В ходе дальнейшего анализа этих атак исследователи обнаружили, что группа обновила свой набор инструментов, в частности, обновив свой вариант вредоносного ПО PlugX. Инструмент удаленного доступа PlugX (RAT) ранее использовался в атаках, направленных на правительственные учреждения, и позволяет удаленным пользователям осуществлять кражу данных или брать под контроль затронутые системы без разрешения или авторизации. Он может копировать, перемещать, переименовывать, выполнять и удалять файлы; регистрировать нажатия клавиш; отпечаток пальца зараженной системы; и больше.

«Поскольку исследователи безопасности продолжают публично сообщать об этой группе, они демонстрируют настойчивость в модификации своего набора инструментов, чтобы помешать анализу и избежать обнаружения», - заявили исследователи из Proofpoint в своем анализе в понедельник. «Хотя базовые изменения их полезной нагрузки не сильно увеличивают сложность атрибуции кампаний TA416, они действительно делают автоматическое обнаружение и выполнение компонентов вредоносных программ, независимых от цепочки заражения, более сложной задачей для исследователей».

Новые атаки

После почти месяца бездействия (после предыдущего исследования угроз) TA416 исследователи наблюдали «ограниченные признаки» возобновления целевого фишинга с 16 сентября по 10 октября. Следует отметить, что в этот период времени отмечался китайский национальный праздник (Национальный день) и последующий период неофициальных отпусков («Золотая неделя»), говорят исследователи.

Эти более поздние попытки целевого фишинга включали (продолжающееся) использование приманок социальной инженерии, которые отсылают к временному соглашению, недавно продленному между Ватиканским Святым Престолом и Коммунистической партией Китая (КПК). Исследователи из Recorded Future ранее раскрыли эту кампанию и сказали, что она произошла во время продления в сентябре 2020 года знаменательного временного соглашения между Китаем и Ватиканом 2018 года, называемого сделкой Китай-Святой Престол. Исследователи Proofpoint заявили, что они также наблюдали, как в это время группа угроз использовала поддельный заголовок электронной почты в целевых фишинговых сообщениях, которые, похоже, имитируют журналистов из Союза католических новостей Азии.

«Это сочетание тематического содержания социальной инженерии предполагает постоянное внимание к вопросам, относящимся к развивающимся отношениям между католической церковью и КПК», - говорят исследователи.

Хотя о некоторых из этих кампаний уже сообщалось, дальнейшее расследование атак выявило совершенно новый вариант загрузчика вредоносных программ PlugX TA416.

PlugX Вредоносное ПО

При более тщательном исследовании исследователи выявили два архива RAR, которые служат в качестве дропперов вредоносных программ PlugX.

Исследователи заявили, что исходный вектор доставки этих архивов RAR не может быть идентифицирован, «однако исторически наблюдалось, что TA416 включает URL-адреса Google Диска и Dropbox в фишинговых электронных письмах, доставляющих архивы, содержащие вредоносное ПО PlugX и связанные с ним компоненты», - заявили они.

Один из этих файлов оказался самораспаковывающимся архивом RAR. После извлечения архива RAR на хосте устанавливаются четыре файла и запускается переносимый исполняемый файл (PE) Adobelm.exe.

Adobelm.exe - это законный исполняемый файл Adobe, который используется для боковой загрузки hex.dll из библиотеки динамической компоновки (DLL). Он вызывает функцию экспорта hex.dll, которая называется CEFProcessForkHandlerEx.

«Исторически в кампаниях TA416 использовалось имя файла hex.dll и то же имя экспорта PE для обеспечения боковой загрузки DLL для Microsoft Windows PE DLL», - заявили исследователи. «Эти файлы служат загрузчиками и дешифраторами зашифрованных полезных нагрузок вредоносных программ PlugX».

Этот загрузчик вредоносных программ был идентифицирован как двоичный файл Golang; Исследователи заявили, что ранее они не наблюдали этот тип файлов, используемых TA416. Go - это язык программирования с открытым исходным кодом.

«Было обнаружено, что оба идентифицированных архива RAR содержат один и тот же зашифрованный файл вредоносной программы PlugX и образцы загрузчика Golang», - заявили они.

По словам исследователей, несмотря на изменение типа файла загрузчика PlugX, функциональность в основном остается прежней.

Файл читает, загружает, расшифровывает и выполняет полезную нагрузку вредоносного ПО PlugX. Затем вредоносная программа PlugX обращается к IP-адресу сервера управления и контроля (C2) 45.248.87 [.] 162. Исследователи заявили, что продолжающаяся активность TA416 демонстрирует, что противник постоянно вносит изменения в документированные наборы инструментов.

«Внедрение загрузчика Golang PlugX наряду с продолжающимися усилиями по шифрованию полезных нагрузок PlugX предполагает, что группа может осознавать повышенное обнаружение своих инструментов, и демонстрирует адаптацию в ответ на публикации, касающиеся их кампаний», - сообщает Proofpoint. «Эти корректировки инструментов в сочетании с периодическим пересмотром инфраструктуры командования и контроля говорят о том, что TA416 будет и дальше преследовать дипломатические и религиозные организации». ***(Lindsey O'Donnell. TA416 APT Rebounds With New PlugX Malware Variant // Threatpost (https://threatpost.com/ta416-apt-plugx-malware-variant/161505/). 23.11.2020).***

***

«Власти Индии сообщили, что крупное отключение электроэнергии, произошедшее в прошлом месяце в Мумбаи могло быть вызвано хакерами.

Отключение электроэнергии произошло в середине октября и повлияло на столичный район Мумбаи, вызвав значительные нарушения в работе систем управления движением и поездов. Потребовалось два часа на восстановление подачи электроэнергии только для основных служб, и до 12 часов — в некоторых пострадавших районах.

Как сообщило информагентство Mumbai Mirror, подразделение киберполиции обнаружило свидетельства того, что инцидент мог быть вызван кибератакой. Следователи выявили несколько подозрительных авторизаций на серверах, подключенных к энергоснабжающим компаниям. Предположительно, манипуляции с данными серверами могли вызвать сбой в работе систем. Активность преступников была прослежена до нескольких стран Южной Азии, и в настоящее время следователи пытаются определить, была ли она частью скоординированных кибератак.

По словам источников газеты India Today, следователи также обнаружили вредоносное ПО в диспетчерском центре, из-за которого предположительно произошел сбой. Центры распределения нагрузки несут ответственность за обеспечение работы электросети, мониторинг работы сети, а также планирование и диспетчеризацию электроэнергии». ***(Крупное отключение электроэнергии в Индии могло быть вызвано кибератакой // SecurityLab.ru (https://www.securitylab.ru/news/514260.php). 23.11.2020).***

***

«Потужна хакерська атака на Бундестаг тривала з 30 квітня по 20 травня 2015 року

Сім країн-партнерів Європейського союзу, у число яких входить і Україна, приєдналися до санкцій щодо громадян і структур Росії, відповідальних за кібератаку на Бундестаг у 2015 році. Про це йдеться у заяві верховного представника ЄС із закордонних справ і політики безпеки Жозепа Борреля.

«22 жовтня 2020 року Рада прийняла Рішення (CFSP) 2020/1537. Рішенням Ради додані дві фізичні особи та одну установу у список фізичних і юридичних осіб та організацій, щодо яких застосовуються обмежувальні заходи, викладені у додатку до рішення (CFSP) 2019/797. Країни-кандидати - Республіка Північна Македонія, Чорногорія та Албанія, а також країни Ісландія і Норвегія, що входять до Європейського економічного простору, а також Україна і Грузія приєднуються до цього рішення Ради», - сказано у заяві.

Повідомляється, що зазначені держави забезпечать відповідність своєї національної політики цим рішенням.

«Європейський союз приймає до відома це зобов'язання і вітає його», - заявив глава європейської дипломатії…» ***(Україна приєдналася до санкцій ЄС за кібератаку росіян на Бундестаг // Українські медійні системи (https://glavcom.ua/news/ukrajina-prijednalasya-do-sankciy-jes-za-kiberataku-rosiyan-na-bundestag-720449.html). 25.11.2020).***

***

Вірусне та інше шкідливе програмне забезпечення

«Фахівці міжнародного розробника антивірусного програмного забезпечення, експерта в області кіберзахисту - компанії ESET у День захисту від кіберзагроз розповіли про найпоширеніші шкідливі програми, які поширилися в 2020 році.

Відповідна інформація міститься на сайті ESET.

"Сьогодні відзначається День захисту від кіберзагроз, який був заснований компанією ESET для залучення уваги користувачів до безпеки своїх пристроїв під час роботи в Інтернеті. Оскільки ми живемо в епоху, коли життя стало неможливим без технологій, важливо бути обізнаними в питаннях кібербезпеки. Саме тому фахівці ESET підготували перелік найпоширеніших типів шкідливих програм, які загрожують інтернет-користувачам у 2020 році", - йдеться в повідомленні.

Шкідливі програми для Інтернету речей

За даними ESET, через постійне зростання ролі смарт-пристроїв у сучасному житті, збільшилася й кількість атак на ці девайси. Найбільш поширеним типом загроз, які спрямовані на пристрої Інтернету речей, є шкідливі боти.

"Після зараження ботами смарт-пристрої часто використовуються як канали зв'язку з іншими скомпрометованими пристроями в мережі, створюючи ботнети. Своєю чергою оператори ботнету можуть здійснювати безліч шкідливих дій, включаючи розгортання програм-вимагачів, здійснення DDoS-атак і крадіжки банківських облікових даних", - попереджають фахівці з кібербезпеки.

На жаль, пристрої Інтернету речей є легкою мішенню для зловмисників. Причиною цього є часте використання паролів за замовчуванням або слабких паролів, таких як "admin", а також відсутність своєчасних оновлень домашнього роутера. Перевіривши понад 100 тис. роутерів, дослідники ESET виявили, що 10 основних вразливостей пов'язані із застарілим програмним забезпеченням. Саме тому регулярне оновлення смарт-пристроїв є важливим елементом кібергігієни.

Шкідливі програми для пристроїв Android

Як повідомляється на сайті ESET, найпопулярнішою категорією загроз для Android у 2020 році стали шкідливі програми, які після інсталяції приховують свої іконки й заповнюють пристрій дратівливою повноекранною рекламою.

Такі програми з категорії прихованих додатків часто маскуються під привабливі ігри або корисні утиліти, таким чином змушуючи користувачів їх завантажити. Оскільки іконки цих додатків зникають після завантаження, користувачам складно визначити місцезнаходження шкідливої програми для її видалення.

"Для захисту пристрою слід використовувати Програму з безпеки, яка здатна виявляти і видаляти такі шкідливі програми", - радять в ESET.

Шкідливі торенти

Нещодавно компанія ESET виявила сімейство шкідливих торентів KryptoCibule, які використовувалися для швидкого поширення загроз. Зокрема,

загроза KryptoCibule використовує протокол BitTorrent, заманюючи користувачів завантажити зламане або піратське програмне забезпечення та ігри. Під виглядом легітимних програм загроза завантажує криптомайнер і компонент захоплення буфера обміну, який викрадає криптовалюту.

"Такі шкідливі програми, як KryptoCibule, є ще однією причиною для використання офіційних сайтів і торрент-сервісів", - підкреслили фахівці ESET.

Шкідливі програми для Mac

Як повідомляється на сайті ESET, раніше пристрої Mac вважалися більш захищеними від комп'ютерних загроз, проте зараз вони все частіше стають цілями кіберзлочинців. У 2020 році дослідники ESET виявили підроблені веб-сайти, які поширюють серед користувачів Mac шкідливі програми для торгівлі криптовалютою.

У липні 2020 року серед таких програм виявився троянський додаток Kattana, який був націлений на пристрої Mac. Кіберзлочинці використовували шкідливе програмне забезпечення GMERA для викрадення інформації (файли "cookie" браузера та облікові дані гаманців криптовалюти) і створення знімків екрану.

"Для надійного захисту комп'ютерів Mac від різних підроблених веб-сайтів і програм використовуйте рішення з безпеки", - відзначають фахівці.

Шкідливі листи

Експерти з кібербезпеки також розповіли, що перехід великої кількості користувачів на віддалений режим роботи сприяв збільшенню числа шкідливих програм, які поширюються через електронну пошту. Загальна кількість виявлених зразків шкідливих електронних листів зростає, а їх велика частина (25%) пов'язана з уразливістю Microsoft Office 2017 року.

"Саме тому важливо встановлювати автоматичні оновлення для своїх додатків Microsoft Office для захисту від шкідливих програм, які використовують відомі уразливості", - підсумували в ESET.

Як повідомляв УНІАН, раніше фахівці ESET оприлюднили основні тенденції поширення Інтернет-загроз за третій квартал 2020 року.

За даними ESET, в Україні щодня фіксується близько 300 тис. нових кіберзагроз для інформаційної безпеки. При цьому, знайти хакерів-зловмисників вкрай складно, компаніям залишається лише проводити щохвилинні моніторинги на предмет виявлення кіберзагроз з метою їхнього подальшого блокування…». ***(Фахівці з кібербезпеки в День захисту від кіберзагроз розповіли про найпоширеніші віруси 2020 року// УНІАН (https://www.unian.ua/science/komp-yuterni-virusi-fahivci-rozpovili-pro-nayposhirenishi-virusi-2020-roku-novini-11205614.html?_ga=2.71728851.1176991860.1605634398-1637720126.1600872078). 03.11.2020).***

***

«Анализ данных статистики Dr.Web за октябрь показал значительное увеличение общего числа обнаруженных угроз – на 37,8% по сравнению с сентябрем. Количество уникальных вредоносных программ при этом снизилось на 2,64%. Рекламные программы и загрузчики вредоносного ПО по-прежнему лидируют по общему количеству детектирований. В почтовом трафике на первых

позициях продолжает находиться банковский троян Trojan.SpyBot.699, а также вредоносы, использующие уязвимости документов Microsoft Office. Кроме того, пользователям продолжают угрожать различные модификации вредоносных HTML-документов, распространяемых в виде вложений и перенаправляющих на фишинговые сайты.

Число обращений пользователей за расшифровкой файлов продолжает держаться на одном уровне четвертый месяц. Самым распространенным шифровальщиком остается Trojan.Encoder.26996, на долю которого приходится 26,34% всех инцидентов.

Основные угрозы октября, по данным сервиса статистики «Доктор Веб»:

Adware.Downware.19741 – рекламное ПО, часто выступающее в роли промежуточного установщика пиратских программ;

Adware.Elemental.17 – семейство рекламных программ, попадающих на устройства путем подмены ссылок на файлообменных сервисах. Вместо ожидаемых файлов жертвы получают эти приложения, которые показывают рекламу, а также инсталлируют ненужное ПО;

Adware.Softobase.15 – программа-установщик, распространяющая устаревшее программное обеспечение. Меняет настройки браузера;

Trojan.LoadMoney.4020 – семейство программ-установщиков, вместе с требуемыми приложениями инсталлирующих на компьютеры жертв всевозможные дополнительные компоненты. Некоторые модификации трояна могут собирать и передавать злоумышленникам различную информацию об атакованном компьютере;

Trojan.AutoIt.289 – утилита, написанная на скриптовом языке AutoIt и распространяемая в составе майнера или RAT-трояна. Выполняет различные вредоносные действия, затрудняющие обнаружение основной полезной нагрузки.

Рейтинг вредоносных программ в почтовом трафике:

Tool.KMS.7 – хакерские утилиты, которые используются для активации продуктов Microsoft с поддельной лицензией;

Trojan.SpyBot.699 – многомодульный банковский троян. Позволяет киберпреступникам загружать и запускать на зараженном устройстве различные приложения и исполнять произвольный код;

W97M.DownLoader.2938 – семейство троянов-загрузчиков, использующих в работе уязвимости документов Microsoft Office. Предназначены для загрузки на атакуемый компьютер других вредоносных программ;

HTML.Redirector.33, HTML.Redirector.32 – вредоносные HTML-документы, как правило маскирующиеся под безобидные вложения к электронным письмам. При открытии перенаправляют пользователей на фишинговые сайты или загружают полезную нагрузку на заражаемые устройства.

По сравнению с прошлым месяцем в октябре в антивирусную лабораторию «Доктор Веб» поступило на 1,67% меньше запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков. При этом чаще всего встречались: Trojan.Encoder.26996 – 26,34%; Trojan.Encoder.567 – 9,84%; Trojan.Encoder.29750 – 6,35%; Trojan.Encoder.30356 – 2,54%; Trojan.Encoder.858 – 1,9%.

Статистика детектирований угроз на Android-устройствах показала, что в октябре было выявлено на 12,36% больше угроз, чем в сентябре. При этом почти втрое возросло число обнаружений потенциально опасных программ. Этот скачок произошел за счет распространения приложений, защищенных специализированным программным обфускатором, который злоумышленники могут использовать при создании троянов, усложняя их обнаружение антивирусами». ***(В октябре было обнаружено на 38% больше вредоносных программ // Компьютерное Обозрение (https://ko.com.ua/v_oktyabre_bylo_obnaruzheno_na_38_bolshe_vredonosnyh_programm_135229). 11.11.2020).***

***

«Eset представила рейтинг наиболее распространенных киберугроз, выявленных экспертами по информационной безопасности в III квартале 2020 года. После нескольких месяцев постоянного использования темы COVID-19 во вредоносных целях хакеры вернулись к ряду своих прежних тактик.

Поскольку многие компании в мире до сих пор работают в режиме хоум-офис, протокол удаленного рабочего стола (RDP) постоянно становится объектом интереса киберпреступников. Специалисты Eset зафиксировали увеличение на треть количества атак на уникальных пользователей методом подбора пароля. При этом попыток атак на RDP стало на 140% больше по сравнению с предыдущим кварталом.

После длительного спада в течение предыдущих месяцев активность криптомайнеров начала расти. Увеличение показателей выявления этого вида вредоносного ПО связано с повышением цены Bitcoin. Стоимость криптовалюты достигла наивысшего значения за последние два года. Если еще в марте 2020 года курс биткоина составлял $5000, то в сентябре криптовалюта оценивалась уже в $12000.

Кроме того, эксперты Eset обнаружили вредоносное программное обеспечение для получения криптовалюты KryptoCibule. Оно отличается сложностью тактики. В частности, угроза использует ресурсы устройства жертвы для добычи криптовалюты, а также пытается получить несанкционированный доступ к транзакциям пользователей, заменяя адрес кошелька в буфере обмена. Также вредоносная программа похищает файлы, связанные с криптовалютой, и использует комплекс методов, чтобы избежать обнаружения.

Общий объем обнаружения вредоносных электронных писем вырос на 9%. Наиболее распространенной, как и во II квартале, остается угроза Win/Exploit.CVE-2017-11882 — вредоносный документ, который использует уязвимость в Microsoft Office для загрузки дополнительных опасных программ на компьютер. Более 70% вредоносных вложений были исполняемыми файлами. Свыше 15% составили файлы скриптов и документы Office. Исполняемые файлы во вложениях часто маскировались с помощью двойных расширений. Так злоумышленники заставляли получателей открыть вложение, пользуясь тем, что расширение для известных типов файлов по умолчанию скрыты в Windows.

Общий объем выявленного спама вырос на 4% по сравнению с предыдущим кварталом. В третьем квартале злоумышленники все еще злоупотребляли темой коронавируса для получения прибыли. Используя финансовые трудности, с которыми многие столкнулись, кибермошенники выдавали себя за легитимные организации и пытались манипулировать жертвами для получения их конфиденциальной информации. Среди прочего, через такие рассылки распространялась версия печально известного вредоноса WannaCry.

Данные телеметрии Eset свидетельствуют, что летом и в начале осени атак программ-вымогателей стало меньше, но более половины из всех выявленных образцов в этой категории вирусов пришлось на Win/Filecoder.WannaCryptor». ***(Владимир Бахур. Eset представила рейтинг интернет-угроз за III квартал 2020 // CNews (https://safe.cnews.ru/news/line/2020-11-02_eset_predstavila_rejting_internetugroz). 02.11.2020).***

***

«Ботнет Muhstik, также известный как Mushtik, уже много лет нацелен на облачную инфраструктуру и Интернет вещей.

Ботнет в основном финансирует себя за счет добычи криптовалюты с использованием инструментов с открытым исходным кодом, таких как XMRig и cgminer.

В связи с этим вредоносным ПО появились новые подробности, проливающие свет на его гнусную деятельность и происхождение.

Muhstik - это ботнет, который использует известные эксплойты веб-приложений для взлома устройств Интернета вещей, таких как маршрутизаторы, с целью добычи криптовалюты.

Он использует серверы IRC для своей деятельности по управлению и контролю (C2).

Хотя ботнет Muhstik существует как минимум в 2018 году, в декабре 2019 года Palo Alto Networks определила новый вариант атаки ботнета и захвата маршрутизаторов Tomato.

Некоторые из уязвимостей, используемых Muhstik, включают ошибки Oracle WebLogic Server (CVE-2019-2725 и CVE-2017-10271) и недостаток Drupal RCE (CVE-2018-7600).

Фирма облачной безопасности Lacework предоставила дополнительный анализ и наблюдения, связанные с Muhstik.

Атака Muhstik выполняется в несколько этапов.

Сначала с сервера злоумышленника загружается файл полезной нагрузки с именем «pty», за которым следует номер…

«После успешной установки Mushtik свяжется с IRC-каналом для получения команд», - говорит Крис Холл, исследователь облачной безопасности в Lacework.

Серверы IRC - это инфраструктура C2, на которой работает ботнет Muhstik.

«Обычно Muhstik получает указание загрузить майнер XMRrig и модуль сканирования. Модуль сканирования используется для развития ботнета путем нацеливания на другие серверы Linux и домашние маршрутизаторы», - продолжил Холл.

Muhstik использует исходный код Mirai для шифрования конфигураций своей полезной нагрузки и модуля сканирования с помощью однобайтового шифрования XOR.

Лэйсворк объясняет, что образцы файлов, содержащие данные конфигурации Muhstik, обычно содержат следующую последовательность байтов: 4F 57 4A 51 56 4B 49 0F.

Это эквивалентное значение XOR (0x22) ключевого слова muhstik, которое может быть идентифицировано в распакованных двоичных файлах.

Странная атрибуция и упоминания об аниме

Однако более интересные детали появляются, когда исследователи Lacework пытаются проследить происхождение ботнета.

«Было обнаружено, что IRC C2 irc.de-zahlung.eu совместно использует сертификат SSL с сайтом jaygame.net», - объясняет Холл.

«Jaygame.net - это любительский сайт об игре с участием аниме-персонажа по имени «Джей». В настоящее время сайт использует идентификатор Google Analytics UA-120919167-1».

Было обнаружено, что этот идентификатор аналитики связан с двумя другими доменами: fflyy.su и kei.su.

В тестах BleepingComputer мы обнаружили, что указанный идентификатор Analytics действительно присутствует на jaygame.net, но больше не присутствует на двух других доменах.

Однако стоит отметить, что любой, в том числе злоумышленник, может включить идентификатор Google Analytics законного веб-сайта в свой собственный веб-сайт.

Другой домен со ссылками на аниме, используемый Мухстиком, - это pokemoninc.com. Принимая во внимание, что Кей (в kei.su) также может быть отсылкой к аниме-персонажу, согласно Ласеворку.

Отслеживая аналогичные корреляции, Лэйсворк проследил происхождение Мухстика до китайской судебно-медицинской фирмы.

«Все они имеют ссылки на один и тот же путь загрузки вредоносных программ, принадлежащий китайской судебно-экспертной компании Shen Zhou Wang Yun Information Technology Co., Ltd», - поясняет их сообщение в блоге.

Кроме того, Лэйсворк упоминает, что исходные образцы вредоносного ПО были загружены на VirusTotal сразу до того, как атаки Muhstik были обнаружены в реальных условиях.

В этих образцах было несколько строк с упоминанием «shenzhouwangyun», например в /home/wys/shenzhouwangyun/shell/downloadFile/tomato.deutschland-zahlung.eu_nvr

Это указывает на то, что «Шэнь Чжоу Ван Юнь, вероятно, является создателем вредоносного ПО, а не просто первым загрузчиком», - предположил Холл.

В прошлом исследователи также связывали Shen Zhou Wang Yun с вредоносной программой HiddenWasp Linux.

Актуальные индикаторы компромисса (IOC) Мухстика были предоставлены Lacework в виде CSV». ***(Ax Sharma. Chinese-linked Muhstik botnet targets Oracle***

WebLogic, Drupal // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/chinese-linked-muhstik-botnet-targets-oracle-weblogic-drupal/). 11.11.2020).

***

«Сильно обфусцированный и вредоносный проект NPM используется для кражи пользовательских токенов Discord и информации браузера у ничего не подозревающих пользователей.

NPM - это менеджер пакетов JavaScript, который позволяет разработчикам загружать и интегрировать различные модули JS из общедоступного реестра, содержащего более миллиона пакетов.

NPM - это открытая система, в которой каждый может отправлять модули для использования другими разработчиками.

Благодаря этой открытой системе злоумышленники все чаще загружают вредоносные модули, которые крадут данные, загружают и запускают программы или проявляют вредоносное поведение при использовании в других проектах.

Вредоносный NPM крадет данные браузера, токены Discord

25 августа 2020 года NPM удалил вредоносный пакет под названием «fallguys», предназначенный для кражи токенов Discord и информации браузера из Google Chrome, Brave Browser, Opera и Yandex Browser.

Сегодня компания Sonatype, занимающаяся безопасностью с открытым исходным кодом, обнаружила еще один вредоносный модуль, который крадет информацию браузера и токены Discord, называемый discord.dll, который считается преемником модуля fallguys.

Исследователь Sonatype Акс Шарма сказал BleepingComputer, что злонамеренные проекты NPM часто используют имена, похожие на имена законных проектов, чтобы обманом заставить разработчиков использовать их.

«Пакеты Typosquatting и brandjacking извлекают выгоду из стоимости существующего бренда и извлекают выгоду из невинной ошибки, совершенной пользователем», - пояснил Шарма.

Хотя он называется discord.dll, его файл package.json указывает на то, что модуль основан на другом проекте под названием JSTokenGrabber, который ранее находился на GitHub…» ***(Lawrence Abrams. Malicious NPM project steals Discord accounts, browser info // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/malicious-npm-project-steals-discord-accounts-browser-info/). 09.11.2020).***

***

«По данным «Лаборатории Касперского», бразильские зловреды вышли не только за пределы страны, но и на новый уровень: теперь они атакуют и мобильные устройства.

Так, в Guildma, одном из сложных семейств банковских троянцев с бразильскими корнями, появился новый зловред Ghimob. С его помощью атакующие шпионят за своими жертвами, расположенными в том числе в Парагвае, Перу, Португалии, Германии, Анголе и Мозамбике.

Это вредоносное ПО внедряется в систему через электронное письмо с сообщением о долге, который якобы числится за адресатом. Получателю предлагается пройти по ссылке, чтобы узнать больше. Если он нажимает на неё, то в систему загружается троянец для удалённого доступа. После успешной установки он отправляет на сервер информацию о модели мобильного устройства, о том, есть ли на нём настройки блокировки экрана, и список приложений. По данным экспертов, Ghimob может шпионить за 153 мобильными приложениями, в основном принадлежащими банкам, финтех-компаниям, криптовалютным биржам. Этот троянец умеет избегать ручного отключения, собирать данные, манипулировать тем, что изображено на экране, и предоставлять злоумышленникам возможность полностью контролировать устройство с помощью инструментов удалённого доступа.

Ghimob может скрываться от систем по борьбе с мошенничеством, внедряемых финансовыми организациями, и разблокировать экран устройства, так как обладает функцией записи и воспроизведения действий пользователя, в том числе связанных с вводом пароля. Для проведения мошеннической трансакции злоумышленники могут принудительно выключить экран устройства или воспользоваться уже открытым финансовым приложением в фоне, пока человек видит на экране другое приложение.

«Желание латиноамериканских злоумышленников распространить мобильные банковские троянцы по всему миру имеет долгую историю. Мы уже видели Basbanke, BRata, но они фокусировались на бразильском рынке. Ghimob — первый мобильный банковский троянец бразильского происхождения, готовый к международному распространению. Мы полагаем, что этот зловред относится к семейству Guildma по нескольким причинам, но главным образом потому, что они используют одну и ту же инфраструктуру. Мы рекомендуем финансовым организациям пристально следить за этими угрозами и одновременно улучшать процессы аутентификации, внедрять технологии борьбы с мошенничеством и использовать аналитические данные об угрозах, чтобы снизить вероятность успешных атак этого мобильного банковского троянца», — комментирует Дмитрий Галов, эксперт по кибербезопасности «Лаборатории Касперского». ***(Локальные зловреды научились атаковать и мобильные устройства по всему миру // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5701017-Lokalnye-zlovredy-nauchilis-atakova.html). 11.11.2020).***

***

«Злоумышленники используют рекламу поддельных обновлений Microsoft Teams для развертывания бэкдоров, которые используют Cobalt Strike для заражения сетей компаний вредоносным ПО.

Согласно отчету Bleeping Computer, Microsoft предупреждает своих клиентов о так называемых кампаниях «FakeUpdates» в закрытых рекомендациях по безопасности. Кампания нацелена на различные типы компаний, с недавними целями в секторе образования K-12, где организации в настоящее время зависят от использования приложений, таких как Teams, для видеоконференцсвязи из -за ограничений COVID-19.

Cobalt Strike - это инструмент моделирования массовых атак, который злоумышленники используют для распространения вредоносных программ, в частности программ-вымогателей. В последнее время было замечено, что злоумышленники использовали Cobalt Strike в атаках, использующих Zerologon, недостаток повышения привилегий, который позволяет злоумышленникам получить доступ к контроллеру домена и полностью скомпрометировать все службы идентификации Active Directory.

В сообщении Microsoft заявила, что в последней кампании FakeUpdates злоумышленники использовали рекламу в поисковых системах для продвижения лучших результатов программного обеспечения Teams в домен, который они контролируют и используют для гнусной деятельности, согласно отчету. Если жертва нажимает на ссылку, она загружает полезную нагрузку, которая выполняет сценарий PowerShell, который загружает вредоносный контент.

Согласно отчету, маяки Cobalt Strike входят в число полезных нагрузок, также распространяемых в рамках кампании, которые дают злоумышленникам возможность перемещаться по сети в поперечном направлении за пределы исходной системы заражения. Ссылка также устанавливает действительную копию Microsoft Teams в системе, чтобы она выглядела законной и не предупреждала жертв об атаке.

Вредоносное ПО, распространяемое кампанией, включает в себя инфостилер Predator the Thief, который крадет конфиденциальные данные, такие как учетные данные, данные браузера и платежи, согласно рекомендациям. Согласно отчету, Microsoft также наблюдала распространение бэкдора Bladabindi (NJRat) и стилера ZLoader в рамках последних кампаний.

Согласно отчету, в дополнение к кампаниям FakeUpdates, в которых используются приманки Microsoft Teams, технический гигант также видел аналогичные схемы атак как минимум в шести других кампаниях с вариациями той же темы, что предполагает более широкую атаку со стороны тех же злоумышленников. В другом случае, например, злоумышленники использовали службу сокращения URL-адресов IP Logger, предупреждает Microsoft.

Microsoft предложила ряд методов смягчения последствий последней волны атак FakeUpdates. Компания рекомендует людям использовать веб-браузеры, которые могут фильтровать и блокировать вредоносные веб-сайты, а также обеспечивать надежность паролей локальных администраторов, которые невозможно легко угадать.

Согласно отчету, права администратора также должны быть ограничены основными пользователями и избегать общедоменных учетных записей служб, которые имеют те же разрешения, что и администратор.

Организации также могут ограничить поверхность атаки, чтобы держать злоумышленников в страхе, блокируя исполняемые файлы, которые не соответствуют определенным критериям, или блокируя код JavaScript и VBScript от загрузки исполняемого содержимого, сообщила Microsoft». ***(Elizabeth Montalbano. Microsoft Teams Users Under Attack in 'FakeUpdates' Malware Campaign // Threatpost (https://threatpost.com/microsoft-teams-fakeupdates-malware/161071/). 10.11.2020).***

***

«Исследователи обнаружили нового червя, нацеленного на серверы x86 на базе Linux, а также на устройства Интернета вещей (IoT) Linux (которые основаны на процессорах ARM и MIPS).

Следует отметить, что вредоносная программа использует GitHub и Pastebin для размещения кода вредоносных компонентов и имеет как минимум 12 различных модулей атаки, которые исследователи называют «Gitpaste-12». Впервые он был обнаружен Juniper Threat Labs в ходе атак 15 октября 2020 года.

«Нет вредоносных программ - это хорошо, но черви особенно раздражают», - заявили исследователи из Juniper Threat Labs в своем сообщении в четверг. «Их способность распространяться автоматически может привести к боковому распространению внутри организации или к вашим хостам, пытающимся заразить другие сети через Интернет, что приведет к плохой репутации вашей организации».

Первая фаза атаки - это начальная компрометация системы. Различные модули атаки вредоносной программы включают 11 ранее обнаруженных уязвимостей. Сюда входят недостатки в Apache Struts (CVE-2017-5638), маршрутизаторах Asus (CVE-2013-5948), подключаемом модуле Webadmin для opendreambox (CVE-2017-14135) и маршрутизаторах Tenda (CVE-2020-10987).

По словам исследователей, вредоносная программа будет пытаться использовать известные эксплойты для этих уязвимостей для компрометации систем, а также может пытаться подобрать пароли. После компрометации системы основной сценарий оболочки затем загружается на машину жертвы и начинает загружать и выполнять другие компоненты Gitpaste-12.

Вредоносное ПО

Этот скрипт устанавливает задание cron, загружаемое из Pastebin. Задание cron - это планировщик заданий на основе времени в Unix-подобных компьютерных операционных системах. Задание cron вызывает сценарий и выполняет его снова каждую минуту; Исследователи полагают, что этот сценарий, по-видимому, является одним из механизмов, с помощью которого обновления могут быть отправлены в ботнет.

Затем он загружает сценарий с GitHub (https: // raw [.] Githubusercontent [.] Com / cnmnmsl-001 / - / master / shadu1) и выполняет его. Скрипт содержит комментарии на китайском языке и предлагает злоумышленникам несколько команд для отключения различных функций безопасности. К ним относятся снятие защиты системы, включая правила брандмауэра, selinux (архитектура безопасности для систем LinuxR), apparmor (модуль безопасности ядра Linux, который позволяет системному администратору ограничивать возможности программ), а также обычное программное обеспечение для предотвращения атак и мониторинга.

У вредоносного ПО также есть некоторые команды, отключающие агентов облачной безопасности, «что ясно указывает на то, что злоумышленник намерен атаковать инфраструктуру общедоступных облачных вычислений, предоставляемую Alibaba Cloud и Tencent», - заявили исследователи.

Gitpaste-12 также содержит команды, позволяющие запускать криптомайнер, нацеленный на криптовалюту Monero.

«Это также не позволяет администраторам собирать информацию о запущенных процессах, перехватывая системные вызовы readdir и пропуская каталоги для таких процессов, как tcpdump, sudo, openssl и т. Д. В / proc», - заявили исследователи. «Каталог '/ proc' в Linux содержит информацию о запущенных процессах. Например, он используется командой «ps» для отображения информации о запущенных процессах. Но, к сожалению для этого злоумышленника, эта реализация не дает того, что они от нее ожидают ».

Наконец, вредоносное ПО также содержит библиотеку (hide.so), загружаемую как LD_PRELOAD, которая загружает и выполняет файлы Pastebin) https: // pastebin [.] Com / raw / Tg5FQHhf), в которых размещается дополнительный вредоносный код.

Исследователи сообщили, что они сообщили об URL-адресе Pastebin, а также о репозитории Git, упомянутом выше, который загружает вредоносные сценарии для вредоносного ПО. Репозиторий Git был закрыт 30 октября 2020 г. «Это должно остановить распространение этого ботнета», - заявили исследователи.

Червячные особенности

Что касается возможностей червя, Gitpaste-12 также содержит сценарий, который запускает атаки на другие машины в попытке реплицировать и распространять вредоносное ПО.

«Вредоносная программа выбирает для атаки случайный / 8 CIDR и пробует все адреса в этом диапазоне», - утверждают исследователи. Бесклассовая междоменная маршрутизация (CIDR) - это метод распределения IP-адресов и IP-маршрутизации. Это означает, что атака нацелена на все IP-адреса в пределах случайного диапазона CIDR.

По словам исследователей, другая версия сценария также открывает порты 30004 и 30005 для команд обратной оболочки. Порт 30004 использует протокол управления передачей (TCP), который является одним из основных протоколов в сетях TCP / IP; а порт 30005 - это двунаправленный протокол на основе SOAP / HTTP, который обеспечивает связь между устройствами, такими как маршрутизаторы или сетевые коммутаторы, и серверами автоконфигурации…». ***(Lindsey O'Donnell. Gitpaste-12 Worm Targets Linux Servers, IoT Devices // Threatpost (https://threatpost.com/gitpaste-12-worm-linux-servers-iot-devices/161016/). 06.11.2020).***

***

«Ранее неизвестные вредоносные программы были обнаружены в ходе массовых атак на клиентов электронной коммерции в Латинской Америке.

Вредоносная программа, которую исследователи Cybereason Nocturnus назвали Chaes, развертывается злоумышленником в регионе LATAM для кражи финансовой информации.

В своем сообщении в блоге в среду группа по кибербезопасности сообщила, что бразильские клиенты крупнейшей в регионе компании электронной коммерции MercadoLivre находятся в центре внимания вредоносного ПО для кражи информации.

Штаб-квартира MercadoLivre находится в Буэнос-Айресе, Аргентина, и управляет как онлайн-площадкой, так и платформой для аукционов. В 2019 году у гиганта электронной коммерции было зарегистрировано около 320,6 миллиона пользователей.

Впервые обнаруженный Cybereason в конце 2020 года, Chaes распространяется через фишинговые кампании, в которых в электронных письмах утверждается, что покупка MercadoLivre была успешной. Чтобы попытаться улучшить внешний вид электронного письма, злоумышленники также добавили сноску «проверено Avast».

Сообщения содержат вредоносное вложение файла .docx. Ассаф Дахан, глава Cybereason по исследованию угроз, сообщил ZDNet, что вложение использует «технику внедрения шаблонов с использованием встроенной функции Microsoft Word для получения полезной нагрузки с удаленного сервера»

Если жертва щелкает файл, уязвимость используется для установления соединения с командным сервером (C2) злоумышленника, а также для загрузки первой вредоносной полезной нагрузки - файла .msi.

Затем этот файл развертывает файл .vbs, используемый для выполнения других процессов, а также файлы uninstall.dll и engine.bin, которые действуют как «движок» вредоносной программы. Еще три файла - hhc.exe, hha.dll и chaes1.bin - устанавливаются, которые объединяют основные компоненты Chaes. Также был зафиксирован модуль майнинга криптовалюты

Чаес создает ключи реестра для сохранения устойчивости основного движка вредоносного ПО и будет развертывать модули, замаскированные под законные процессы, для кражи системной информации, извлечения конфиденциальной информации из сеансов браузера Google Chrome, сбора учетных данных для входа в онлайн-учетные записи и кражи финансовой информации; в частности, при посещении домена MercadoLivre.

Особо следует отметить способность Чейза открывать сеанс Chrome. Активность отслеживается и контролируется с помощью подключения API и библиотеки Node.js Puppeteer. Страницы MercadoLivre и MercadoPago могут быть доступны без согласия на зараженных машинах. Вредоносная программа также может делать скриншоты посещенных страниц MercadoLivre и отправлять их на C2.

«Тревожным моментом в этой вредоносной программе на основе node.js является тот факт, что в большинстве случаев такое поведение считается нормальным, поскольку использование библиотеки Puppeteer для парсинга веб-страниц не является вредоносным по своей природе», - говорит команда. «Следовательно, обнаруживать подобные угрозы гораздо сложнее».

Однако Chaes, похоже, находится в активной разработке, так как исправленные версии вредоносного ПО более точно ориентированы на страницы MercadoLivre, связанные с покупками в электронной коммерции.

Cybereason в настоящее время изучает, используется ли вредоносное ПО в кампаниях против других компаний электронной коммерции, и предупреждает, что Chaes может указывать на «возможную будущую тенденцию использования библиотеки Puppeteer для дальнейших атак в других крупных финансовых

учреждениях». ***(Charlie Osborne. Chaes malware strikes customers of Latin America's largest e-commerce platform // ZDNet (https://www.zdnet.com/article/chaes-malware-strikes-customers-of-latin-americas-largest-e-commerce-platform/). 18.11.2020).***

***

«Вредоносное ПО Lazarus отслеживалось в новых кампаниях против южнокорейских цепочек поставок, которые стали возможными благодаря украденным сертификатам безопасности.

В понедельник исследователи кибербезопасности из ESET выявили злоупотребление сертификатами, украденными у двух отдельных законных южнокорейских компаний.

Lazarus, также известный как Hidden Cobra, является общим термином для избранных групп угроз, включая ответвления, подозреваемых в связях с Северной Кореей. Предполагается, что он несет ответственность за печально известный взлом Sony в 2014 году, Lazarus также был связан со взломами с использованием уязвимостей нулевого дня, фишинговых сообщений LinkedIn и развертывания троянов в кампаниях, включая Dacls и Trickbot.

В последние годы Lazarus расширил свою поверхность атаки не только для кражи конфиденциальных данных от корпораций, но и для компрометации криптовалютных организаций.

В этой атаке на цепочку поставок злоумышленники используют «необычный механизм цепочки поставок», сообщает ESET, в котором Lazarus нарушает стандартное требование для южнокорейских интернет-пользователей - необходимость установки дополнительного программного обеспечения безопасности при посещении правительственных или финансовых учреждений. веб-сайты сервисов.

Обычно пользователям необходимо загрузить WIZVERA VeraPort, программу, используемую для управления загрузкой программного обеспечения, которое необходимо для посещения определенных доменов. Эти обновления могут включать в себя плагины браузера, автономное программное обеспечение безопасности или инструменты проверки личности.

WIZVERA VeraPort использует цифровую подпись и криптографическую проверку загрузок.

«[Это] то, почему злоумышленники не могут легко изменить содержимое этих файлов конфигурации или создать собственный поддельный веб-сайт», - говорят исследователи. «Однако злоумышленники могут заменить программное обеспечение, которое будет доставлено пользователям WIZVERA VeraPort с законного, но взломанного веб-сайта. Мы полагаем, что именно такой сценарий использовали злоумышленники Lazarus».

Lazarus нацелился на более слабые звенья цепи, незаконно получив сертификаты для подписи кода от двух южнокорейских охранных компаний.

Конфигурация WIZVERA VeraPort по умолчанию обычно требует проверки подписей загруженных двоичных файлов перед выполнением. Однако диспетчер программного обеспечения проверяет только подпись, а не то, кому принадлежат сертификаты.

Чтобы использовать программное обеспечение, украденные, но действующие сертификаты использовались для запуска вредоносных программ Lazarus.

На данный момент были обнаружены два образца вредоносного ПО, маскирующие вредоносное ПО группы как законное южнокорейское программное обеспечение, которое часто загружается и запускается WIZVERA VeraPort. Имена файлов, значки и ресурсы, аналогичные законным программам, были созданы, чтобы не вызывать подозрений.

Если, например, жертва посещает вредоносный веб-сайт и невольно загружает скомпрометированное программное обеспечение, Lazarus затем запускает дроппер через WIZVERA VeraPort, который извлекает загрузчик и файлы конфигурации.

Затем устанавливается соединение с командным сервером (C2) злоумышленника, и последняя полезная нагрузка, троян удаленного доступа (RAT), развертывается на машине жертвы. RAT могут использоваться для поддержания скрытого наблюдения, сохранения через бэкдоры, а также для кражи данных или удаленного управления системой.

«Это сочетание взломанных веб-сайтов с поддержкой WIZVERA VeraPort и конкретными параметрами конфигурации VeraPort, которые позволяют злоумышленникам выполнить эту атаку», - заявляет ESET. «Владельцы таких веб-сайтов могут снизить вероятность таких атак, даже если их сайты скомпрометированы, путем включения определенных параметров (например, путем указания хэшей двоичных файлов в конфигурации VeraPort)». ***(Charlie Osborne. Lazarus malware strikes South Korean supply chains // ZDNet (https://www.zdnet.com/article/lazarus-malware-strikes-south-korean-supply-chains/). 16.11.2020).***

***

«Varonis опубликовала глобальный отчет о тенденциях в области вредоносных программ по итогам октября 2020 г.

В прошедшем месяце команда сетевой криминалистики Varonis проанализировала активность, наблюдаемую при реагировании на инциденты, проведении расследований сетевой криминалистики и обратной разработке образцов вредоносных программ.

Основными векторами атак в октябре стали: программы-вымогатели (43%), вредоносное ПО (15%), брутфорс (14%), криминальные группировки и APT-атаки (14%), компрометация деловой переписки (14%).

Кроме того, компания выделила несколько специфичных вредоносных программ, на которые стоит обратить особое внимание. Первая из них — Ryuk, разновидность программы-вымогателя, использующаяся для целевых атак. У модификаций Ryuk есть два основных способа заражения: фишинг, направленный на конкретных сотрудников внутри организации, а также использование заранее полученных учетных записей для доступа к устройствам внутри компании-жертвы через удаленный рабочий стол.

Еще одним опасным вредоносом аналитики называют Silent Librarian или Cobalt Dickens или TA407, который использует методы адресного фишинга и

атакует университеты. Цель этого ПО в краже научно-исследовательских данных. Silent Librarian базируется в Иране и, скорее всего, финансируется иранским правительством.

Эксперты также обращают внимание на латиноамериканский банковский троян Mekotio. Набор функций Mekotio часто меняется, и, более того, одновременно разрабатывается несколько его разновидностей. В основном троян распространяется через спам-рассылки и использует несколько этапов загрузки.

«В конце сентября группа сетевой криминалистики Varonis связалась с заказчиком после того, как наши системы отслеживания угроз выявили скрытую атаку с помощью программы-вымогателя. Во время расследования выяснилось, что у клиента был скомпрометированный пользователь Office365, с помощью которого злоумышленнику удалось получить доступ к локальной сети, взломать учетную запись службы и использовать ее для запуска программ-вымогателей Cobalt Strike и NetWalker. Наши коллеги использовали как базовые возможности ПО Varonis, так и продвинутый функционал поведенческого анализа, чтобы предоставить заказчику подробный отчет. Отчет включал в себя как сегменты данных, которые не были затронуты вирусом, так и индикаторы компрометации (IOC) программы-вымогателя NetWalker, чтобы заказчик смог провести расследование и в других системах кибербезопасности», — сказал глава Varonis в России Даниэль Гутман». ***(Varonis: в октябре 43% кибератак были осуществлены с помощью программ-вымогателей // CNews (https://safe.cnews.ru/news/line/2020-11-16_varonis_v_oktyabre_43_kiberatak). 16.11.2020).***

***

«Киберпреступная банда TrickBot выпустила сотую версию вредоносного ПО TrickBot с дополнительными функциями, позволяющими избежать обнаружения.

TrickBot - это вредоносное ПО, которое обычно устанавливается через вредоносные фишинговые сообщения электронной почты или другое вредоносное ПО. После установки TrickBot будет незаметно работать на компьютере жертвы, пока он загружает другие модули для выполнения различных задач.

Эти модули выполняют широкий спектр злонамеренных действий, включая кражу базы данных служб Active Directory домена, распространение в сети, блокировку экрана, кражу файлов cookie и паролей браузера, а также кражу ключей OpenSSH.

Известно, что TrickBot завершает атаку, предоставляя доступ к злоумышленникам, стоящим за вымогателями Ryuk и Conti, что еще больше усугубляет ситуацию.

В TrickBot v100 добавлены новые функции

После того, как в прошлом месяце Microsoft и их партнеры провели скоординированную атаку на инфраструктуру TrickBot, появилась надежда, что им потребуется время, чтобы восстановиться.

К сожалению, банда TrickBot все еще не утихает, о чем свидетельствует выпуск сотой сборки вредоносного ПО TrickBot.

Эта последняя сборка была обнаружена Виталием Кремезом из Advanced Intel, который обнаружил, что они добавили новые функции, которые затрудняют обнаружение.

В этом выпуске TrickBot теперь внедряет свою DLL в легитимный исполняемый файл Windows wermgr.exe (Windows Problem Reporting) прямо из памяти с помощью кода из проекта MemoryModule.

«MemoryModule - это библиотека, которую можно использовать для полной загрузки DLL из памяти - без предварительного сохранения на диск», - поясняет страница проекта на GitHub.

Первоначально запущенный как исполняемый файл, TrickBot внедрится в wermgr.exe, а затем завершит работу исходного исполняемого файла TrickBot.

По словам Кремеза, при внедрении DLL она будет делать это с помощью Doppel Hollowing или обработки двойного соединения, чтобы избежать обнаружения программным обеспечением безопасности.

«Этот метод использует транзакции, функцию NTFS, которая позволяет сгруппировать набор действий в файловой системе, и если какое-либо из этих действий не удается, происходит полный откат. Процесс инжектора создает новую транзакцию, внутри которой он создает новый файл, содержащий вредоносную полезную нагрузку. Затем он отображает файл внутри целевого процесса и, наконец, откатывает транзакцию. Таким образом создается впечатление, что файл никогда не существовал, даже если его содержимое все еще находится в памяти процесса, " Описание этого метода, сделанное исследователем безопасности Франческо Мурони.

Как видите, банда TrickBot не позволила нарушению своей инфраструктуры сдерживать их, и они продолжают интегрировать новые функции, чтобы предотвратить обнаружение вредоносного ПО.

К сожалению, это означает, что TrickBot останется здесь в обозримом будущем, а потребителям и предприятиям необходимо сохранять усердие и внимательно следить за тем, какие вложения электронной почты они открывают». ***(Lawrence Abrams. TrickBot turns 100: Latest malware released with new features // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/trickbot-turns-100-latest-malware-released-with-new-features/). 21.11.2020).***

***

«TroubleGrabber, новая программа для кражи учетных данных, обнаруженная исследователями безопасности Netskope, распространяется через вложения Discord и использует веб-перехватчики Discord для доставки украденной информации своим операторам.

Некоторые злоумышленники используют новую программу для кражи информации, чтобы нацеливаться на игроков на серверах Discord и украсть их пароли и другую конфиденциальную информацию.

Его возможности аналогичны другому штамму вредоносного ПО, получившему название AnarchyGrabber [1, 2, 3], который заражает пользователей Discord, также используется для сбора учетных данных и отключения двухфакторной аутентификации жертв (2FA).

Netskope обнаружила информационный кражу в октябре 2020 года при сборе данных для предыдущего отчета, при этом образцы TroubleGrabber (обнаруженные как варианты Razy) составляют более 85% от всех 1650 образцов вредоносного ПО, нацеленных на Discord в октябре.

Поток атак вредоносного ПО

Discord и Github используются для загрузки полезных нагрузок следующего этапа в папку C: / temp после заражения жертвы TroubleGrabber.

Вредоносная программа также использует веб-перехватчики Discord для связи со своим сервером управления и контроля (C2) и для отправки украденной информации жертв.

TroubleGrabber крадет широкий спектр важной информации, включая «токены веб-браузера, токены веб-перехватчиков Discord, пароли веб-браузера и системную информацию».

Вся эта собранная информация отправляется вредоносным ПО через сообщения чата с помощью веб-перехватчиков Discord на серверы Discord злоумышленников.

Вредоносное ПО создано злоумышленником по имени Itroublve. Автор TroubleGrabber в настоящее время управляет сервером Discord с более чем 500 участниками и размещает полезные нагрузки следующего этапа и генератор вредоносных программ в своей общедоступной учетной записи GitHub.

Netskope также обнаружила, что использовала руководство YouTube о том, как использовать TroubleGrabber, чтобы настроить свои собственные серверы Discord для размещения вредоносного ПО.

Техника распространения

TroubleGrabber известен тем, что в основном доставляется на компьютеры жертв с помощью прямой загрузки через ссылки вложения Discord.

«Мы определили более 1000 сгенерированных двоичных файлов, которые распространялись через URL-адреса для прямой загрузки с именами файлов, изображающими читы для игр, программы установки Discord и программные взломы», - говорит Netskope.

Вредоносное ПО распространялось через Discord в 97,8% обнаруженных заражений, «небольшое количество распространялось через anonfiles.com и anonymousfiles.io, сервисы, которые позволяют пользователям загружать файлы анонимно и бесплатно для создания общедоступной ссылки для скачивания».

В некоторых случаях кража информации также распространяется среди пользователей Discord с более чем 700 различных идентификаторов каналов сервера Discord.

«Основываясь на именах файлов и механизмах доставки, TroubleGrabber активно используется для целевых игроков», - заключает Netskope.

10 ноября лаборатория угроз Netskope поделилась индикаторами компрометации TroubleGrabber (IOC) с Discord, GitHub, YouTube, Facebook, Twitter и Instagram (чьи платформы использовались в атаках)». ***(Sergiu Gatlan. New TroubleGrabber Discord malware steals passwords, system info // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-troublegrabber-discord-malware-steals-passwords-system-info/). 13.11.2020).***

***

«Команда исследователей Check Point Research опубликовала отчет Global Threat Index с самыми активными угрозами в октябре 2020 года. Исследователи сообщают, что трояны Trickbot и Emotet по-прежнему возглавляют рейтинг самых распространенных вредоносных ПО в октябре. Они стали причиной резкого увеличения числа атак программ-вымогателей на больницы и медицинские учреждения по всему миру.

ФБР и другие правительственные организации США недавно выпустили предупреждение об атаках программ-вымогателей, нацеленных на сектор здравоохранения. Они сообщили, что в огромном количестве случаев (более миллиона) Trickbot используются для загрузки и распространения других программ-вымогателей, шифрующих файлы, например, таких как Ryuk. Также Ryuk распространяется через троян Emotet, который четвертый месяц подряд занимает 1-е место в рейтинге самых распространенных вредоносных программ.

По данным Check Point, в октябре сфера здравоохранения стала главной целью программ-вымогателей в США: количество атак увеличилось на 71% по сравнению с сентябрем 2020 года. Аналогичным образом, количество атак программ-вымогателей на медицинские организации и больницы в октябре увеличилось на 36% в странах Европы, Ближнего Востока и Африки и на 33% в странах Азиатско-Тихоокеанского региона.

Злоумышленники также часто атаковали российские медицинские организации. За полгода количество атак на российские медицинские организации составило 3% от всех атак на медицинские организации по всему миру.

В сентябре исследовали также сообщали, что русскоязычная группировка OldGremlin была связана, как минимум, с девятью атаками программ-вымогателей в этом году на медицинские лаборатории, банки, производителей и разработчиков ПО в России. Крупная российская медицинская компания, пострадавшая от хакеров, заплатила выкуп в размере 50 тысяч долларов в криптовалюте.

С начала пандемии COVID-19 мы наблюдаем рост атак вымогателей, — рассказывает Василий Дягилев, глава представительства Check Point Software Technologies Ltd в России и СНГ. — Злоумышленники стремятся воспользоваться пробелами в системе безопасности организаций, которые пытаются поддерживать удаленную работу сотрудников. За последние три месяца стремительно растет число атак, вызванных троянами TrickBot и Emotet. Особенный рост отмечается в сфере здравоохранения. Мы настоятельно рекомендуем медицинским организациям проявлять бдительность и стараться не допускать попадания на корпоративные устройства вредоносных программ».

Самое активное вредоносное ПО в октябре 2020 в России

Emotet — продвинутый самораспространяющийся модульный троян. Emotet когда-то был рядовым банковским трояном, а в последнее время используется для дальнейшего распространения вредоносных программ и кампаний. Новый функционал позволяет рассылать фишинговые письма, содержащие вредоносные вложения или ссылки.

Trickbot — один из доминирующих банковских троянов, который постоянно дополняется новыми возможностями, функциями и векторами распространения. Это гибкое и настраиваемое вредоносное ПО, которое может распространяться в рамках многоцелевых кампаний.

FormBook был впервые обнаружен в 2016 году: это инфостилер, предназначенный для ОС Windows. На подпольных хакерских форумах он позиционируется как MaaS из-за его развитых методов уклонения и относительно низкой цены. FormBook собирает учетные данные из различных веб-браузеров, делает снимки экрана, отслеживает и регистрирует нажатия клавиш, а также может загружать и выполнять файлы в соответствии с приказами своего командного сервера.

Самое активное вредоносное ПО в октябре 2020 в мире:

В октябре Emotet остается самым распространенным вредоносным ПО, затрагивая 12% организаций в мире. За ним следуют Trickbot и Hiddad, атаковавшие по 4% организаций каждый.

Emotet — продвинутый самораспространяющийся модульный троян. Emotet когда-то был рядовым банковским трояном, а в последнее время используется для дальнейшего распространения вредоносных программ и кампаний. Новый функционал позволяет рассылать фишинговые письма, содержащие вредоносные вложения или ссылки.

Trickbot — один из доминирующих банковских троянов, который постоянно дополняется новыми возможностями, функциями и векторами распространения. Это гибкое и настраиваемое вредоносное ПО, которое может распространяться в рамках многоцелевых кампаний.

Hiddad — Модульный бэкдор для Android, который предоставляет права суперпользователя для загруженного вредоносного ПО, а также помогает внедрить его в системные процессы. Он может получить доступ к ключевым деталям безопасности, встроенным в ОС, что позволяет ему получать конфиденциальные данные пользователя.

Самые распространенные уязвимости в октябре 2020

Удаленное выполнение кода MVPower DVR. В устройствах MVPower DVR существует уязвимость удаленного выполнения кода. Злоумышленник может использовать эту уязвимость для выполнения произвольного кода в уязвимом маршрутизаторе с помощью специально созданного запроса.

Обход аутентификации роутера Dasan GPON (CVE-2018-10561) — уязвимость обхода аутентификации, существующая в роутерах Dasan GPON. Успешное использование этой уязвимости позволит удаленным злоумышленникам получить конфиденциальную информацию и получить несанкционированный доступ к уязвимой системе.

Удаленное выполнение кода в заголовках HTTP (CVE-2020-13756) — заголовки HTTP позволяют клиенту и серверу передавать дополнительную информацию с помощью HTTP-запроса. Злоумышленник может использовать уязвимый заголовок HTTP для запуска произвольного кода на устройстве жертвы.

Самые активные мобильные угрозы в октябре 2020

В этом месяце Hiddad стал самым популярным вредоносным ПО для мобильных устройств. За ним следуют xHelper и Lotoor.

Hiddad — Модульный бэкдор для Android, который предоставляет права суперпользователя для загруженного вредоносного ПО, а также помогает внедрить его в системные процессы. Он может получить доступ к ключевым деталям безопасности, встроенным в ОС, что позволяет ему получать конфиденциальные данные пользователя.

xHelper — вредоносное приложение для Android, активно с марта 2019 года, используется для загрузки других вредоносных приложений и отображения рекламы. Приложение способно скрываться от пользовательских и мобильных антивирусных программ и переустанавливаться, если пользователь удаляет его.

Lotoor — программа использует уязвимости в операционной системе Android, чтобы получить привилегированный root-доступ на взломанных мобильных устройствах». ***(Обнаружен всплеск атак программ-вымогателей на медицинские учреждения по всему миру // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5702570-Obnaruzhen-vsplesk-atak-programmvym.html). 19.11.2020).***

***

«Киберпреступники разработали бэкдор ModPipe для осуществления атак на ресторанные PoS-решения от Oracle. По мнению исследователей из ESET, вредонос отличается необычной сложностью, о чем свидетельствуют многочисленные модули.

Бэкдор специально создан для атак на Oracle MICROS Restaurant Enterprise Series (RES) 3700 — пакет программного обеспечения для управления PoS-терминалами, используемый сотнями тысяч баров, ресторанов и отелей по всему миру. По словам экспертов, киберпреступники в основном атакуют ресторанные заведения в США.

Один из загружаемых модулей вредоносного ПО, получивший название GetMicInfo, обнаруживает и похищает учетные данные, позволяющие операторам ModPipe получать доступ к содержимому базы данных, включая различные определения и данные конфигурации, таблицы состояния и информацию о транзакциях PoS-терминала.

«Модуль содержит алгоритм, разработанный для сбора паролей баз данных путем их расшифровки из значений реестра Windows. Разработчики бэкдора обладают глубокими познаниями о целевом программном обеспечении жертв и выбрали данный сложный метод вместо сбора данных с помощью более простого, но «более громкого» подхода, такого как кейлоггинг», — отметили специалисты.

Тем не менее, информация базы данных, которую похищает модуль, не содержит номера кредитных карт клиентов заведений. В данном случае злоумышленники могут получить доступ только к именам владельцев карт. Эксперты предполагают, что существует еще один загружаемый модуль, позволяющий операторам вредоносного ПО расшифровывать более конфиденциальные данные.

Основной модуль загрузчика создает канал, используемый для связи с другими вредоносными модулями, а также отвечает за их реализацию и обеспечивает соединение с C&C-сервером злоумышленников.

Кроме того, существует ряд других загружаемых модулей для добавления определенных функций в бэкдор. Два компонента могут сканировать определенные IP-адреса или получать список запущенных процессов на устройстве. Операторы вредоноса также используют как минимум четыре других загружаемых модуля, функциональность которых пока полностью неизвестна». ***(Хакеры создали вредонос для атак на ресторанные PoS-решения от Oracle // SecurityLab.ru (https://www.securitylab.ru/news/514056.php). 13.11.2020).***

***

«Исследователи безопасности предупреждают о новом семействе вредоносных программ, которые в настоящее время нацелены на пользователей мобильных телефонов, чтобы молча подписать их на законные услуги с повышенным тарифом.

Вредоносная программа под названием WAPDropper представляет собой многофункциональный дроппер, который может доставить вредоносное ПО второго уровня и использует решение машинного обучения для обхода проблем CAPTCHA на основе изображений.

Многофункциональная капельница

Компания по кибербезопасности Check Point обнаружила WAPDropper в недавней кампании и обнаружила, что она подписывает жертв на премиальные услуги от законных поставщиков телекоммуникационных услуг в Малайзии и Таиланде.

Анализ вредоносной программы показал, что она имеет два модуля, специфичных для многофункциональных дропперов, которые могут загружать и запускать другие вредоносные программы на скомпрометированном устройстве.

В случае WAPDropper есть один модуль, отвечающий за получение вредоносного ПО второго уровня с сервера управления и контроля, а другой - за получение компонента дозвона премиум-класса…

Схема зарабатывания денег проста: больше звонков на номера с повышенным тарифом приносит больше прибыли киберпреступникам, которые могут идентифицировать владельцев специальных номеров или сотрудничать с ними.

Обход CAPTCHA

По данным Check Point, операторы WAPDropper используют обычную тактику, интегрируя вредоносное ПО в приложения, поставляемые неофициальными магазинами.

Попав на устройство жертвы, вредоносная программа обращается к серверу управления и контроля (C2), чтобы получить премиум-номеронабиратель.

В техническом отчете исследователи говорят, что первоначальная активность вредоносного ПО начинается со сбора сведений о зараженном устройстве, включая следующую информацию:

Идентификатор устройства

MAC-адрес

ID подписчика
Модель устройства
Список всех установленных приложений
Список запущенных сервисов
Имя самого верхнего пакета действий
Экран включен
Включены ли уведомления для этого приложения
Может ли это приложение рисовать наложения
Количество свободного места для хранения
Общий объем RAM и доступная RAM
Список несистемных приложений

Затем запускается компонент веб-просмотра, который загружает целевые страницы для дополнительных услуг и завершает подписку. В один пиксель компонент практически не виден на экране.

Если есть проблема с CAPTCHA на основе изображений, Check Point сообщает, что WAPDropper использует услуги китайской компании Super Eagle, которая предоставляет решения для распознавания изображений на основе технологии машинного обучения.

Взлом тестов CAPTCHA был возможен в течение долгого времени и упростился с помощью кода, специально созданного для этой задачи, который находится в свободном доступе в Интернете.

В случае WAPDropper доступны два варианта. Первый предполагает загрузку изображения CAPTCHA и отправку его на сервер, другой - извлечение DOM-дерева файла и его отправка на сервер, принадлежащий китайской компании Super Eagle, которая предоставляет услуги распознавания изображений на основе машинного обучения.

По данным Check Point, WAPDropper распространяется через неофициальные магазины Android. Избегание этих торговых площадок снижает риск компрометации». ***(Ionut Ilascu. New WAPDropper malware stealthily subscribes you to premium services // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-wapdropper-malware-stealthily-subscribes-you-to-premium-services/). 24.11.2020).***

***

«Blackrota нацелена на ошибку безопасности в Docker, но ее практически невозможно проанализировать с помощью обратного анализа.

Исследователи обнаружили новый бэкдор, написанный на языке программирования Go (Golang), который вскружил им голову из-за высокого уровня обфускации.

Бэкдор под названием Blackrota был впервые обнаружен в приманке, принадлежащей исследователям, пытающимся использовать уязвимость несанкционированного доступа в Docker Remote API. Что отличает бэкдор, так это использование обширных методов защиты от обнаружения, что делает вредоносное ПО чрезвычайно трудным для анализа - то, что, по словам исследователей, обычно не наблюдается с вредоносными программами на основе Golang.

«Исторически мы видели вредоносные программы, написанные на Go, которые в лучшем случае удалялись во время компиляции, а в худшем - слегка запутывались, без особых затруднений при обратном анализе», - заявили исследователи из 360 Netlab во вторник. «Blackrota предлагает новый подход к обфускации и представляет собой наиболее запутанное вредоносное ПО, написанное на Go в формате ELF, которое мы обнаружили на сегодняшний день».

Исследователи назвали вредоносную программу Blackrota из-за ее доменного имени для командования и управления (C2) (blackrota.ga). Threatpost обратился в 360 Netlab за дополнительной информацией о конкретной уязвимости, на которую нацелена.

Вредоносное ПО

По словам исследователей, бэкдор Blackrota в настоящее время доступен только для Linux в формате исполняемого и связываемого файлов (ELF) и поддерживает архитектуры процессоров x86 / x86-64. ELF - это распространенный стандартный формат исполняемых файлов. После дальнейшего расследования исследователи обнаружили, что Blackrota настроена на основе того, что они назвали «geacon».

Это тип маяка, используемый вредоносным ПО для связи с сервером C2, запроса инструкций или для эксфильтрации собранных данных. Этот маяк, в частности, реализован на языке Go и ранее использовался с помощью CobaltStrike, стандартного инструмента моделирования атак, который злоумышленники используют для распространения вредоносных программ и управления взломанными узлами.

Этот маяк реализует различные ключевые функции для бэкдора Blackrota, позволяя ему выполнять команды оболочки (CMD_SHELL), загружать файлы (CMD_UPLOAD), загружать указанные файлы (CMDDOWNLOAD), просматривать файлы (CMD_FILE_BROWSE), устанавливать время задержки сна (CMD_SLEEP) и изменять каталоги (CMD_CD).

Запутывание

Когда дело доходит до обфускации, различные тактики затрудняют анализ и обнаружение Blackrota. Во- первых, вредоносная программа использует gobfuscate, инструмент с открытым исходным кодом для кода Go, чтобы скрыть исходный код перед компиляцией. Он скрывает различные элементы исходного кода Go со случайными заменами символов, включая имена пакетов, имена глобальных переменных, имена функций, имена типов и имена методов.

«С тысячами функций со случайными строковыми именами и большим количеством типов данных, методов и глобальных переменных с произвольными именами мы не могли быть уверены, какие сторонние пакеты Go использовались в образце, что делало обратный анализ практически невозможным для двигаться вперед», - заявили исследователи.

Gobfuscate также заменяет все строки, используемые в коде, кодировками XOR (шифр XOR - это криптографическая логическая операция, которая сравнивает два входных бита и генерирует один выходной бит). В этом случае каждой строке назначается функция декодирования XOR, которая динамически декодирует строки во время выполнения программы.

«Blackrota использует gobfuscate для сокрытия символической и типовой информации, что является «дверью жизни» таких инструментов обратного анализа», - заявили исследователи. «Символьная информация, которую они анализируют и восстанавливают, становится нечитаемой, и невозможно разобраться в символической и типовой информации, и невозможно узнать, какие сторонние пакеты были импортированы в проект. Это значительно усложняет процесс обратного анализа».

Еще одним препятствием для анализа является то, что язык Go использует полностью статические ссылки для создания двоичных файлов - это означает, что все коды, используемые в стандартных и сторонних библиотеках, упакованы в двоичные файлы, что приводит к очень большим двоичным файлам.

«Эта характеристика, с точки зрения обратного анализа, означает, что когда вы открываете двоичный файл Go в инструменте дизассемблирования, вы видите тысячи или даже десятки тысяч функций», - говорят исследователи. «Если эти функции не имеют соответствующей символики, будет сложно провести обратный анализ двоичных файлов Go».

Исследователи заявили, что обфусцированные вредоносные программы, написанные на Go, встречаются редко, но встречались и раньше. Штамм вымогателя под названием EKANS, который представляет собой вариант вымогателя, написанный на Golang, был ранее обнаружен с использованием того же метода обфускации, что и, например, Blackrota. Исследователи предупредили, что эти новые типы вредоносных программ создадут головную боль для защитников безопасности, продвигающихся вперед, когда дело доходит до анализа и обнаружения.

«Метод обфускации Blackrota и EKANS создает новые проблемы для обратного анализа», - говорят исследователи. «По мере того, как язык Go становится все более популярным, в будущем на Go будет написано все больше и больше вредоносных программ… мы будем следить за тем, что будет происходить». ***(Lindsey O'Donnell. Blackrota Golang Backdoor Packs Heavy Obfuscation Punch // Threatpost (https://threatpost.com/blackrota-golang-backdoor-obfuscation/161544/). 24.11.2020).***

***

«Эксперты по информационной безопасности заявили о росте популярности ПО с инструментами обхода одной из самых распространенных систем безопасности типа «песочница», запускающей файлы в изолированной виртуальной среде. По их данным, большая часть таких программ используется для шпионажа. Специалисты связывают рост популярности использования ПО для обхода «песочниц» со смещением вектора хакерских атак от финансового сектора на предприятия, где одним из ценнейших ресурсов является коммерческая тайна.

Залечь на дно в киберпространстве

Специалисты Positive Technologies (PT) выяснили, что 69% изученных программ с инструментами обхода «песочницы» использовалось в хакерских атаках с целью шпионажа. 31% такого же вредоносного ПО (ВПО) служил злоумышленникам для получения финансовой выгоды. Для этого в компании

проанализировали 36 семейств ВПО, которыми на протяжении последних 10 лет пользовались 23 хакерские группировки.

Все вредоносные программы разбили на пять категорий. Выяснилось, что в 56% случаев техники обхода «песочниц» и систем наблюдения внутри них внедрялись в ВПО для удаленного доступа. В загрузчики (вредоносные файлы, маскирующиеся под безопасные, которые при запуске скачивают другое ВПО. — «Известия») они встраивались в 14% случаев. На долю программ-шифровальщиков приходится 11% исследованного ВПО. Столько же (11%) — у банковских троянов. Еще 8% — у шпионских программ.

Программам с инструментами обхода «песочницы» PT уделила внимание именно потому, что она является распространенным видом защиты компьютерных систем от ВПО. Метод подразумевает создание изолированного фрагмента, например, операционной системы внутри полноценной ОС. В нем компьютер открывает потенциально опасные файлы и тестирует их на наличие вредоносного кода. Только после проверки программы в виртуальном пространстве она получает доступ к полноценной версии системы.

Зачастую главной целью ВПО является обход «песочницы» или как минимум определение того, что программа запустилась в виртуальной среде. Равно как и «песочница» не всегда детектирует в проверяемом ПО вредоносный алгоритм, само ВПО тоже может не понять, что оно запустилось в виртуальной среде. Специалисты по информационной безопасности и хакеры постоянно соревнуются в совершенствовании своих систем детектирования.

Старший аналитик Positive Technologies Ольга Зиненко говорит, что популярность инструментов обхода «песочницы» в ПО для удаленного доступа и загрузчиках объясняется тем, что обычно именно эти программы используются в разведке и сборе информации о целевой системе.

— Если злоумышленники обнаружат, что ВПО начало исполнение в виртуальной среде, то они не станут развивать этот вектор атаки и загружать на компьютер жертвы вредоносную нагрузку, а постараются скрыть свое присутствие, прекратив работу ВПО, — пояснил эксперт.

Информация дороже денег

Positive Technologies также отмечает, что 25% исследуемых ими группировок за последние 10 лет были активны именно в последние два года. Этот факт и рост числа ВПО с возможностями обхода виртуализации компания связывает с увеличением исследований образцов шпионского ПО экспертами по кибербезопасности.

Руководитель департамента системных решений Group-IB Станислав Фесенко объясняет активность хакерских группировок, вооруженных специфическим ВПО, смещением вектора атак с финансового сектора на предприятия топливно-энергетического комплекса (ТЭК), промышленного типа и госсектора.

— В основном эти атаки проводят с целью промышленного шпионажа, перепродажи доступа к инфраструктуре, хищения персональных данных пользователей или клиентов, — сказал эксперт.

«Мы проследили изменения в методах обхода «песочниц» и средств анализа и видим, что одно и то же ВПО в разные годы использует разные методы. Кроме того, злоумышленники стараются использовать одновременно несколько технологий», — говорится в отчете Positive Technologies.

Эксперт Group-IB, в свою очередь, указал на то, что профессиональные группировки давно полагаются на несколько техник обхода «песочниц».

— Просто сейчас системы обхода виртуализации маскируются качественнее, чем раньше. Мы считаем, что средства поведенческого анализа должны эволюционировать, чтобы не допустить обнаружения виртуальной среды изнутри, — сообщил Станислав Фесенко.

Посвящать в подробности работы известных Group-IB хакерских уловок для обхода «песочниц» эксперт отказался: раскрытие такой информации может подсказать злоумышленникам направление, в котором стоит развивать ВПО.

APT-группировки

Руководитель направления аналитики и спецпроектов ГК InfoWatch Андрей Арсентьев подчеркивает, что улучшение вредоносных программ могут позволить себе только APT-группировки, обладающие мощными финансовыми и кадровыми ресурсами.

— Хакерам-одиночкам практически невозможно развивать подобные инструменты, — пояснил эксперт.

По его данным, последние техники обхода «песочниц» предполагают использование методов искусственного интеллекта. В частности, хакерские программы могут анализировать окружение «песочницы», получать данные об операционных системах, хранилищах и подстраиваться под поведение пользователей.

— Злоумышленники стараются тщательно скрыть вредоносные функции от исследователей безопасности и минимизировать вероятность обнаружения ВПО по известным индикаторам компрометации (Indicator of Compromise, IOC), — сообщила Ольга Зиненко.

IOC — это наблюдаемый в Сети или на конкретном устройстве объект (или активность), который с большой долей вероятности указывает на несанкционированный доступ к системе (то есть ее компрометацию). Такие индикаторы используют для обнаружения вредоносной активности на ранней стадии, а также для предотвращения известных угроз.

Исходя из этого, PT считает, что классические средства защиты могут не справиться с обнаружением современных образцов вредоносных программ. Поэтому компания рекомендует для выявления ВПО анализировать поведение файлов в безопасной виртуальной среде». ***(Роман Кильдюшкин. Код за кодом: 70% вредоносного ПО используется для шпионажа // Известия (https://iz.ru/1090041/roman-kildiushkin/kod-za-kodom-70-vredonosnogo-po-ispolzuetsia-dlia-shpionazha). 23.11.2020).***

***

«Злоумышленники часто развивают свои вредоносные программы для Linux. BlackTech с новым ELF_PLEAD вредоносных программ и Winnti в

PWNLNX инструмент недавние примеры. Одновременно с этой тенденцией мы обнаружили новую версию прокси-трояна Linux, относящуюся к группе Stantinko. На момент публикации этого вредоносного ПО обнаружено только одно обнаружение в VirusTotal.

Группа Stantinko известна тем, что нацелена на операционные системы Windows с текущими кампаниями, начиная с 2012 года. Вредоносное ПО группы в основном состоит из майнеров и бот-сетей рекламного ПО.

В официальном документе от 2017 года, в котором описывается деятельность Stantinko, исследователи ESET проанализировали прокси-сервер трояна Linux. До сих пор это была единственная известная вредоносная программа для Linux, принадлежащая Stantinko.

Мы обнаружили новую версию этого троянца для Linux, замаскированного под httpd. httpd - это сервер протокола передачи гипертекста Apache, широко используемая программа на серверах Linux. Версия образца - 2.17, а старая версия - 1.2 *.

Мы считаем, что это вредоносное ПО является частью более широкой кампании, использующей взломанные серверы Linux. Ниже мы приводим технический анализ вредоносного ПО и сравниваем его с предыдущей версией.

Технический анализ

Имя файла новой версии прокси - httpd, и на момент написания этой статьи в VirusTotal обнаружено только одно обнаружение. На рисунке 1 ниже показан результат VirusTotal. Образец был загружен 7 ноября 2020 года из России, одной из основных целевых стран Stantinko. Образец представляет собой 64-битный двоичный файл ELF без разметки.

Поток вредоносных программ

После выполнения вредоносная программа проверит файл конфигурации, который доставляется вместе с вредоносной программой на зараженную машину. Вредоносная программа ожидает, что файл конфигурации будет расположен по адресу «/etc/pd.d/proxy.conf». Если файл конфигурации не существует или в нем отсутствует требуемая структура, вредоносная программа завершает работу без каких-либо дополнительных вредоносных действий. На рисунке 2 ниже показан фрагмент логики анализа конфигурации. Конфигурации хранятся в виде пар ключ / значение.

Предполагается, что в файле конфигурации будут следующие ключи: proxy_ip, port, redirect_url, localhost, ip_header и request_header_log_files.

После проверки и анализа структуры файла конфигурации вызывается функция start_demon, и прокси-сервер запускает сам себя. Затем он создает сокет и прослушиватель для приема соединений от клиента. Мы считаем, что клиенты, взаимодействующие с этим троянцем, - это другие зараженные машины, участвующие в кампании…

Как только клиент подключается к слушателю, программа вызывает функцию on_client_connect. Сначала он проверяет, является ли метод запроса GET, POST или NOTIFY.

Если метод запроса - GET, программа ответит HTTP-ответом 301 redirect, содержащим параметр redirect_url из файла конфигурации. Это означает, что если

C&C IP просто ищется, например, с помощью браузера, ответ может вводить в заблуждение, перенаправляя на безопасный веб-сайт, не оставляя следов дополнительной полезной нагрузки, которая используется в атаке. Если метод запроса - POST или NOTIFY, вредоносная программа создаст запрос POST для отправки на C&C сервер на основе заголовков и содержимого HTTP-запроса клиента с помощью функции create_post_data. Затем программа вызовет функцию mysql_server_do_request, которая отвечает за отправку запроса POST на C&C…

Запрос POST отправляется по одному из следующих путей на C&C сервере:

/kbdmai/index.php

/kbdmai/dht/index.php

/kbdmai/DRTIPROV/index.php

/kbdmai/winsvc/index.php

/kbdmai/anti_rstrui/index.php

Путь выбирается в функции detect_proxy_script на основе данных, отправленных от клиента. Мы считаем, что каждый путь обеспечивает разную полезную нагрузку в рамках цепочки атаки кампании. IP-адрес C&C хранится как параметр proxy_ip в файле конфигурации. Наконец, прокси пересылает ответ C&C обратно клиенту…

Сравнение версий

С разницей между двумя версиями почти три года, троянские прокси имеют схожее назначение, но не идентичны. В этом разделе мы сравним версии 1.2 * и 2.17 по трем критериям: параметры, функциональность и структура ELF.

Параметры

В новой версии (2.17) используется файл конфигурации, который сбрасывается на машину жертвы вместе с вредоносной программой. Файл конфигурации содержит IP-адрес C&C вместе с другими параметрами. В старой версии (1.2 *) C&C жестко запрограммирован в двоичном коде, что упрощает блокировку трафика кампании после обнаружения двоичного файла.

Функциональность

В дополнение к функциям прокси старая версия получает файлы и команды самообновления от C&C. Новая версия более проста в том, что она работает только как прокси.

Структура ELF

Обе версии 1.2 * и 2.17 не имеют ограничений и включают символы отладки. Старая версия связана статически, а новая версия - динамически.

Связь со стантинко

После загрузки файла в Intezer Analyze мы заметили, что новый вариант имеет несколько имен функций со старым. Эти функции, такие как get_binary_full_path и read_variable_string, в новой версии не вызываются статически. Мы почти уверены, что эти функции остались от предыдущего варианта.

Интересно, что пути C&C намекают на некоторые из предыдущих кампаний Stantinko, основанные на исследовании ESET. Пример жестко заданных путей показан на рисунке 7. Имя корневого каталога - kbdmai. «KDBMAI.dll» - это имя файла вредоносной программы, использовавшееся Stantinko в 2012 году. Кроме

того, командный сервер вредоносной программы размещался в сети kdbmai [.] Net. Еще один интересный справочник - DRTIPROV. DRTIPROV является частью пути к базе данных программ (pdb) от одного из вредоносных программ группы Windows.

Stantinko - это новейшее вредоносное ПО, нацеленное на серверы Linux, которое скрывается под радаром и присоединяется к таким угрозам, как Doki, IPStorm и RansomEXX.

Код из нового образца Stantinko теперь индексируется в базе данных генома Intezer...» ***(Avigayil Mechtinger. Stantinko's Proxy After Your Apache Server // Intezer (https://www.intezer.com/blog/research/stantinkos-proxy-after-your-apache-server/). 24.11.2020).***

***

Програми-вимагачі

«Группа программ-вымогателей начала размещать рекламу в Facebook, чтобы заставить жертв заплатить выкуп.

Когда в 2012 году впервые были представлены современные программы-вымогатели, мы стали свидетелями новой атаки с вымогательством, при которой злоумышленники вымогают жертв, шифруя их файлы, а затем требуют выкуп, чтобы получить дешифратор.

В ноябре 2019 года банды программ -вымогателей приняли новую стратегию двойного вымогательства, в которую вовлечены хакеры, которые также крадут незашифрованные файлы перед шифрованием устройств. Затем злоумышленники угрожают разместить эти украденные файлы на сайтах утечки данных программ-вымогателей, если выкуп не будет уплачен.

С тех пор банды вымогателей стали хорошо разбираться в средствах массовой информации: они публикуют пресс-релизы или связываются с журналистами, чтобы поделиться своими последними действиями по оказанию давления на жертв…». ***(Lawrence Abrams. Ransomware gang hacks Facebook account to run extortion ads // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/ransomware-gang-hacks-facebook-account-to-run-extortion-ads/). 11.11.2020).***

***

«В минувшие выходные тайваньский производитель ноутбуков Compal Electronics подвергся атаке программы-вымогателя DoppelPaymer, при этом злоумышленники потребовали выкуп почти в 17 миллионов долларов.

Compal является вторым по величине производителем ноутбуков с оригинальным дизайном (ODM) в мире. Известные компании, включая Apple, HP, Dell, Lenovo и Acer, проводят ребрендинг своих устройств и дизайнов, проводят ребрендинг.

Требуется выкуп в размере 16,7 миллиона долларов

В минувшие выходные тайваньские СМИ сообщили, что Compal подверглась кибератаке, но производитель ноутбуков заявил, что это просто «аномалия» в их системе автоматизации офиса.

«Лу Цинсюн сказал, что основная причина была в неисправности в системе автоматизации офиса. Компания подозревалась в том, что она подверглась вторжению хакеров. Она срочно отремонтировала большую часть этого и, как ожидается, вернется к нормальной работе сегодня»,

«Лу Цинсюн подчеркнул, что хакеры не шантажируют Compal, как сообщает внешний мир, и в настоящее время все работает нормально», - сообщает UDN.

С тех пор BleepingComputer подтвердил, что Compal подвергся атаке программы-вымогателя DoppelPaymer после того, как мы получили записку о выкупе, использованную в этой атаке.

DoppelPaymer - это программа-вымогатель, известная своей атакой на корпоративные цели путем получения доступа к учетным данным администратора и их использования для распространения по сети Windows. Получив доступ к контроллеру домена Windows, они развертывают полезные данные программы-вымогателя на всех устройствах в сети.

Согласно платежному сайту DoppelPaymer Tor, на который есть ссылка в записке о выкупе, банда вымогателей требует 1100 биткойнов, или 16 725 500 долларов США по сегодняшним ценам, чтобы получить дешифратор.

Согласно записке с требованием выкупа и прошлой истории DoppelPaymer, злоумышленники, вероятно, украли незашифрованные данные в рамках своей атаки.

Эти украденные данные затем используются в качестве стратегии двойного вымогательства, когда банды вымогателей угрожают выпустить файлы на сайтах утечки данных, если выкуп не будет уплачен.

Следует отметить, что первоначальные требования о выкупе являются «стартовой» ценой и обычно согласовываются с более низкой суммой для жертв, которые решают заплатить выкуп.

Другие жертвы, на которые в прошлом нападал DoppelPaymer, включают PEMEX (Petróleos Mexicanos), город Торранс в Калифорнии, университет Ньюкасла, округ Холл в Джорджии и Bretagne Télécom». ***(Lawrence Abrams. Laptop maker Compal hit by ransomware, $17 million demanded // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/laptop-maker-compal-hit-by-ransomware-17-million-demanded/). 09.11.2020).***

***

«Новая программа-вымогатель под названием Pay2Key была нацелена на организации из Израиля и Бразилии, зашифровывая их сети в течение часа в целевых атаках, которые все еще расследуются.

Майкл Гиллеспи, создатель ID Ransomware, также видел сообщения от жертв Pay2Key, преимущественно с бразильских IP-адресов.

Хотя эта программа-вымогатель использовалась в атаках против нескольких бразильских организаций, она не связана со вчерашними атаками RansomExx, нацеленными на правительственные сети Бразилии.

Шифрует сети за один час

В новом отчете Check Point исследователи говорят, что злоумышленники, стоящие за программой-вымогателем Pay2Key, вероятно, используют публично открытый протокол удаленного рабочего стола (RDP) для получения доступа к сетям жертв и развертывания исходных вредоносных нагрузок.

Хотя операторы Pay2Key проникают в целевые сети и действуют в них до того, как программа-вымогатель начинает шифрование систем, у них есть «возможность быстро распространить программу-вымогатель в течение часа по всей сети».

Оказавшись в сети жертвы, злоумышленники установят сводное устройство, которое будет использоваться в качестве прокси для всех исходящих сообщений между компьютерами, зараженными вымогателем, и серверами управления и контроля (C2) Pay2Key.

Это помогает им избежать или, по крайней мере, снизить риск обнаружения перед шифрованием всех доступных систем в сети с помощью одного устройства для связи со своей собственной инфраструктурой.

Выкуп до 140 тысяч долларов

Как и в случае с другими операциями с программами-вымогателями, управляемыми человеком, субъекты Pay2Key будут использовать легитимный портативный инструмент Microsoft PsExec для удаленного выполнения полезных нагрузок программы-вымогателя под названием Cobalt.Client.exe на сетевых устройствах целевых организаций.

После успешного шифрования устройства программа-вымогатель отправит в систему записку о выкупе, настроенную для каждой взломанной организации и использующую имя [ORGANIZATION] _MESSAGE.TXT.

В записке с требованием выкупа также упоминается, что некоторые файлы жертв были украдены во время атак, но Check Point еще не нашла доказательств этого.

Операторы Pay2Key в настоящее время требуют относительно невысокого выкупа, при этом Check Point видит, что они требуют от 7 до 9 биткойнов (примерно от 110 до 140 тысяч долларов) за жертву. BleepingComputer требует выкупа всего в 4 биткойна (около 62 тысяч долларов).

Эта программа-вымогатель не основана на коде из ранее обнаруженных штаммов, и образцы Pay2Key были обнаружены только одним ядром защиты от вредоносных программ при отправке в VirusTotal.

Судя по артефактам компиляции, похоже, что Pay2Key внутренне называется «Cobalt» разработчиками, для которых английский язык не является родным, согласно строкам и формулировкам журнала.

Программа-вымогатель использует гибрид симметричной и асимметричной схемы шифрования, в которой используются алгоритмы AES и RSA, при этом сервер C2 является тем, который доставляет открытый ключ RSA во время выполнения, что указывает на то, что Pay2Key не сможет зашифровать машины без подключения к Интернету или если сервер C2 сервер не в сети.

«Хотя атака все еще расследуется, недавние атаки программ-вымогателей Pay2Key указывают на то, что к тенденции целевых атак программ-вымогателей

присоединяется новый злоумышленник, представляющий хорошо продуманную операцию для максимального увеличения ущерба и минимизации уязвимости», - заключили исследователи Check Point». ***(Sergiu Gatlan. New Pay2Key ransomware encrypts networks within one hour // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/new-pay2key-ransomware-encrypts-networks-within-one-hour/). 06.11.2020).***

***

«Итальянский производитель спиртных напитков Campari Group подвергся атаке программы-вымогателя Ragnar Locker, в ходе которой якобы было украдено 2 ТБ незашифрованных файлов. Чтобы восстановить свои файлы, Ragnar Locker требует 15 миллионов долларов.

Campari Group - итальянская компания по производству напитков, известная своими популярными брендами спиртных напитков, включая Campari, Frangelico, SKYY vodka, Epsolon, Wild Turkey и Grand Marnier.

…в понедельник Campari опубликовала заявление для прессы, в котором заявили, что в минувшие выходные подверглись кибератаке, в результате которой были отключены ИТ-службы и сеть.

«Campari Group сообщает, что предположительно 1 ноября 2020 года он стал объектом атаки вредоносного ПО (компьютерного вируса), которая была своевременно идентифицирована. ИТ-отдел Группы при поддержке экспертов по ИТ-безопасности немедленно принял меры для ограничения распространения. вредоносного ПО в данных и системах. Поэтому компания временно приостановила предоставление ИТ-услуг, поскольку некоторые системы были изолированы, чтобы обеспечить их санитарную обработку и постепенный перезапуск в условиях безопасности для своевременного восстановления нормальной работы», - сказал Campari в заявление.

Из-за этой атаки веб-сайты Campari и Campari Group в настоящее время не работают.

Рагнар Локер утверждает, что украл 2 ТБ данных

В образце Ragnar Locker, обнаруженном сегодня исследователем безопасности Pancak3 и установленном BleepingComputer, записка с требованием выкупа ясно показывает, что она использовалась в атаке против Campari Group.

В записке о выкупе группа Ragnar Locker утверждает, что во время атаки украла 2 ТБ незашифрованных файлов, включая банковские выписки, документы, договорные соглашения, электронные письма и многое другое.

В качестве доказательства того, что они украли данные, записка о выкупе содержит восемь URL-адресов для скриншотов некоторых украденных данных. Эти снимки экрана предназначены для конфиденциальных документов, таких как банковские выписки, паспорт Великобритании, налоговые формы W-4 для сотрудников, таблица с номерами SSN и соглашение о конфиденциальности.

Pancak3 сообщил BleepingComputer, что Ragnar Locker утверждает, что зашифровал большинство серверов Campari Group из двадцати четырех стран и требует 15 миллионов долларов в биткойнах за дешифратор.

В эту цену также входит обещание удалить данные со своих файловых серверов и не публиковать и не передавать данные, а также отчет о проникновении в сеть и рекомендации по повышению безопасности.

Следует отметить, что служба согласования программ-вымогателей Coveware обнаружила, что операции с программами-вымогателями все чаще не выполняют свое обещание удалить украденные данные после уплаты выкупа.

В этом году Рагнар Локер участвовал и в других крупных атаках, в том числе на португальского транснационального энергетического гиганта Energias de Portugal (EDP) и французскую компанию морского транспорта и логистики CMA CGM.

Bleeping Computer обратился в Campari Group с вопросами, касающимися этой атаки, но не получил ответа». ***(Lawrence Abrams. Campari hit by Ragnar Locker Ransomware, $15 million demanded // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/campari-hit-by-ragnar-locker-ransomware-15-million-demanded/). 05.11.2020).***

***

«Банды программ-вымогателей все чаще не выполняют свое обещание удалить украденные данные после того, как жертва заплатит выкуп.

В 2019 году группа вымогателей Maze представила новую тактику, известную как двойное вымогательство, когда злоумышленники крадут незашифрованные файлы, а затем угрожают опубликовать их, если не будет уплачен выкуп.

Теперь жертвы вымогают не только с помощью шифрования файлов, но и из-за риска публикации их данных, что приведет к утечке данных.

Эта тактика была быстро принята другими программами-вымогателями, которые начали создавать сайты утечки данных, используемые для публикации украденных файлов жертв.

Как часть этой тактики двойного вымогательства, большинство операций с программами-вымогателями требуют от жертвы уплаты единственного выкупа, который предоставит как дешифратор для их зашифрованных файлов, так и обещание не делиться украденными файлами и их удаление.

Некоторые операции с программами-вымогателями, такие как AKO / Ranzy, требуют двух выкупов: один для дешифратора, а другой - для того, чтобы не публиковать украденные данные.

Банды вымогателей не сдерживают своего обещания

В опубликованном сегодня отчете о программах-вымогателях Coveware за третий квартал 2020 года мы узнаем, что некоторые банды вымогателей не сдерживают своего обещания удалить украденные данные после уплаты выкупа.

Согласно новому отчету, определенные группы сливают украденные данные после уплаты выкупа, используют поддельные данные в качестве доказательства удаления или даже повторно вымогают у жертвы те же данные, которые были оплачены, чтобы не разглашаться.

Sodinokibi : Жертвы, которые заплатили, были повторно вытеснены через несколько недель с угрозами опубликовать тот же набор данных.

Netwalker : опубликованные данные о компаниях, которые заплатили за это, чтобы не просочились

Меспиноза : данные о компаниях, которые заплатили за это, не просочились

Conti : поддельные файлы отображаются как доказательство удаления

Мейз, Сехмет и Эгрегор, которые, по всей видимости, связаны между собой, также упоминались как имеющие проблемы с сохранением данных в секрете после получения оплаты. В разговоре с BleepingComputer генеральный директор Coveware Билл Сигел объяснил, что по мере роста Maze их работа стала дезорганизованной, и данные жертвы были ошибочно размещены на сайте утечки данных.

Сигел также сообщил BleepingComputer, что Конти использовал сайты для обмена файлами, чтобы поделиться доказательствами украденных данных с жертвами. При загрузке данных на эти сайты также создаются ссылки для удаления, которые позволяют любому, у кого есть ссылка, удалить загруженные данные.

По словам Сигела, Conti предоставил жертвам фальшивые ссылки для удаления после уплаты выкупа, которые содержали фиктивные данные, а не реальные данные жертвы. Эти ссылки предназначались для того, чтобы обмануть жертву, заставив думать, что их данные были удалены, хотя в действительности Конти продолжал хранить данные.

В отличие от дешифратора программы-вымогателя, которую злоумышленник не может забрать после того, как она была предоставлена, жертва не может точно узнать, удаляет ли операция вымогателя украденные данные после того, как был произведен выкуп.

В связи с этим Coveware сказал BleepingComputer, что нет смысла платить выкуп, поскольку нет никакого способа узнать наверняка, что он не будет использован для вымогательства в будущем.

Помня об этом, Coveware говорит жертвам ожидать следующего, если они решат заплатить, поэтому их данные не разглашаются:

Данные не будут удалены достоверно. Жертвы должны предполагать, что он будет продан другим субъектам угрозы, продан или удержан 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.

В любом случае данные могут быть опубликованы по ошибке или намеренно, прежде чем жертва сможет даже ответить на попытку вымогательства.

Компании должны автоматически предполагать, что их данные были переданы множеству злоумышленников и что они будут использоваться или утечка каким-либо образом в будущем, независимо от того, платили ли они.

Вместо этого компании должны рассматривать атаку как нарушение данных и должным образом информировать всех клиентов, сотрудников и деловых партнеров о том, что их данные были украдены в соответствии с требованиями закона.

Это заставляет компании выглядеть лучше, пытаясь поступать правильно, и дает тем, кто был разоблачен, возможность отслеживать и защищать свои учетные записи от мошенничества». ***(Lawrence Abrams. Scam PSA: Ransomware gangs don't always delete stolen data when paid // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/scam-psa-ransomware-gangs-dont-always-delete-stolen-data-when-paid/). 04.11.2020).***

***

«Новая программа-вымогатель RegretLocker использует множество дополнительных функций, которые позволяют ей шифровать виртуальные жесткие диски и закрывать открытые файлы для шифрования.

RegretLocker был обнаружен в октябре и представляет собой простую программу-вымогатель с точки зрения внешнего вида, поскольку он не содержит длинных записок о выкупе и использует для связи электронную почту, а не сайт оплаты Tor.

При шифровании файлов он добавляет безобидно звучащее расширение .mouse к зашифрованным именам файлов.

Однако недостаток внешнего вида компенсируется расширенными функциями, которые мы обычно не видим при заражении программами-вымогателями, как описано ниже.

RegretLocker монтирует виртуальные жесткие диски

При создании виртуальной машины Windows Hyper-V виртуальный жесткий диск создается и сохраняется в файле VHD или VHDX.

Эти файлы виртуального жесткого диска содержат необработанный образ диска, в том числе таблицу разделов и разделы диска, и, как и обычные диски, могут иметь размер от нескольких гигабайт до терабайт.

Когда программа-вымогатель шифрует файлы на компьютере, шифрование большого файла неэффективно, поскольку это снижает скорость всего процесса шифрования.

В образце программы-вымогателя, обнаруженной MalwareHunterTeam и проанализированной Виталием Кремезом из Advanced Intel, RegretLocker использует интересную технику монтирования файла виртуального диска, чтобы каждый из его файлов мог быть зашифрован индивидуально.

Для этого RegretLocker использует функции Windows Virtual Storage API OpenVirtualDisk, AttachVirtualDisk и GetVirtualDiskPhysicalPath для монтирования виртуальных дисков.

Как показано в отладочном сообщении программы-вымогателя, она специально ищет VHD и монтирует их при обнаружении.

После того, как виртуальный диск смонтирован как физический диск в Windows, программа-вымогатель может зашифровать каждый из них по отдельности, что увеличивает скорость шифрования.

Считается, что код, используемый RegretLocker для монтирования VHD, был взят из недавно опубликованного исследования исследователя безопасности smelly__vx.

Помимо использования API виртуального хранилища, RegretLocker также использует API диспетчера перезапуска Windows для завершения процессов или служб Windows, которые сохраняют файл открытым во время шифрования.

При использовании этого API Кремез сообщил BleepingComputer, что если имя процесса содержит «vnc», «ssh», «mstsc», «System» или «svchost.exe», программа-вымогатель не остановит его. Этот список исключений, вероятно, используется для предотвращения завершения критических программ или программ, используемых злоумышленником для доступа к скомпрометированной системе.

Функция Windows Restart Manager используется только несколькими программами-вымогателями, такими как REvil (Sodinokibi), Ryuk, Conti, ThunderX / Ako, Medusa Locker, SamSam и LockerGoga.

RegretLocker на данный момент не очень активен, но это новое семейство, за которым мы должны следить». ***(Lawrence Abrams. New RegretLocker ransomware targets Windows virtual machines // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/new-regretlocker-ransomware-targets-windows-virtual-machines/). 03.11.2020).***

***

«Киберотдел Федерального бюро расследований США (ФБР) предупредил партнеров из частного сектора об увеличении активности программ-вымогателей Ragnar Locker после подтвержденной атаки с апреля 2020 года.

Флэш-оповещение MU-000140-MW, выпущенное вчера для партнеров ФБР, было скоординировано с DHS-CISA и предоставляет специалистам по безопасности и системным администраторам индикаторы компрометации для защиты от постоянных злонамеренных действий этой банды вымогателей.

«ФБР впервые обнаружило вымогатель Ragnar Locker1 в апреле 2020 года, когда неизвестные субъекты использовали его для шифрования файлов крупной корпорации за выкуп примерно в 11 миллионов долларов и пригрозили выпустить 10 ТБ конфиденциальных данных компании», - говорится в сообщении ФБР в сообщении TLP: WHITE flash alert.

«С тех пор Ragnar Locker использовался против растущего списка жертв, включая поставщиков облачных услуг, компаний связи, строительства, путешествий и корпоративного программного обеспечения».

Тактика Ragnar Locker

Актеры Ragnar Locker вручную развернут полезные нагрузки программы-вымогателя для зашифрованных систем жертв после этапа разведки, чтобы помочь им обнаружить сетевые ресурсы, резервные копии компании и различные другие конфиденциальные файлы, которые необходимо собрать для кражи данных.

Банда программ-вымогателей также известна тем, что часто переключает методы обфускации полезной нагрузки, чтобы избежать обнаружения, а также тем, что использовала специальные алгоритмы упаковки и шифровала файлы жертв с виртуальных машин Windows XP, развернутых в их системах.

Вредоносная программа Ragnar Locker также перечислит все запущенные службы, чтобы уничтожить те, которые используются поставщиками управляемых услуг для удаленного управления сетями своих клиентов.

Пройдя этапы разведки и перед развертыванием, субъекты Ragnar Locker сбрасывают целенаправленный исполняемый файл вымогателя, который добавляет настраиваемое расширение «RGNR_», где является хеш-кодом NETBIOS-имени компьютера.

Эта программа-вымогатель имеет встроенный ключ RSA-2048, а также сбрасывает пользовательские заметки о выкупе в зашифрованных системах.

Примечания о выкупе Ragnar Locker включают название компании жертвы, ссылку на сайт Tor и сайт утечки данных, где банда вымогателей опубликует данные жертвы.

Хотя ФБР не предоставило дополнительной информации о крупной корпорации, системы которой были зашифрованы в апреле, подробности полностью соответствуют атаке на многонационального энергетического гиганта Energias de Portugal (EDP).

EDP - один из крупнейших операторов энергетического сектора Европы, в котором работает более 11 500 сотрудников, и поставляет энергию более чем 11 миллионам клиентов в 19 странах на 4 континентах.

Злоумышленники Ragnar Locker смогли похитить около 10 ТБ конфиденциальной информации компании о выставлении счетов, контрактах, транзакциях, клиентах и партнерах.

Они также украли экспорт базы данных менеджера паролей KeePass, содержащий имена пользователей, пароли, учетные записи, URL-адреса и заметки сотрудников EDP.

Представитель EDP сообщил BleepingComputer, что атака не повлияла на критически важную инфраструктуру компании и службу энергоснабжения.

В течение прошлого года ФБР также выпустило предупреждения о программах- вымогателях LockerGoga, MegaCortex, Maze, Netwalker и ProLock после объявления государственной службы о мощных атаках программ-вымогателей на государственные и частные организации США с октября 2019 года». ***(Sergiu Gatlan. FBI warns of increasing Ragnar Locker ransomware activity // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-warns-of-increasing-ragnar-locker-ransomware-activity/). 20.11.2020).***

***

«Ведущему поставщику облачного программного обеспечения Blackbaud предъявили иск по 23 предложенным групповым искам потребителей в США и Канаде, связанных с атакой программы-вымогателя, от которой компания пострадала в мае 2020 года.

Blackbaud работает в странах по всему миру, включая США, Великобританию, Австралию и Канаду.

Атака программы-вымогателя, непосредственно виновная в привлечении к ответственности поставщика программного обеспечения, была раскрыта компанией 16 июля 2020 года.

Организации, пострадавшие от атаки программ-вымогателей на Blackbaud, включают длинный список организаций, таких как благотворительные организации, некоммерческие организации, фонды и университеты из США, Канады, Великобритании и Нидерландов.

Компания заявила, что ей удалось помешать злоумышленникам полностью зашифровать ее системы, но не раньше, чем они украли «копию подмножества данных» из собственной среды.

Blackbaud заплатила выкуп, запрошенный злоумышленниками после того, как они подтвердили, что украденные данные были уничтожены.

Судебные иски и запросы регуляторов данных

Сегодня компания Blackbaud подтвердила, что она была названа ответчиком по 23 предполагаемым групповым искам, связанным с майской атакой программ-вымогателей, в своем квартальном отчете за третий квартал 2020 года, поданном в Комиссию по ценным бумагам и биржам США (SEC).

«На сегодняшний день мы фигурируем в качестве ответчика по 23 предполагаемым групповым искам потребителей (17 в федеральных судах США, 4 в судах штатов США и 2 в судах Канады) по обвинениям в нанесении ущерба в результате инцидента безопасности», - сказал Блэкбауд.

"Истцы по этим делам, которые якобы представляют различные классы отдельных составляющих наших клиентов, как правило, утверждают, что пострадали от предполагаемых действий и / или бездействия с нашей стороны в связи с инцидентом безопасности, и утверждают, что различные нормы общего права и законодательные акты иски о возмещении денежного ущерба, судебном запрете, судебных издержках и гонорарах адвокатов, а также другие средства правовой защиты ".

Поставщик облачного программного обеспечения также получил около 160 исков, связанных с атакой программ-вымогателей, от клиентов и / или их адвокатов в США, Великобритании и Канаде.

Запросы об атаке также были сделаны правительственными агентствами и регуляторами данных, включая консолидированное требование гражданского расследования от имени 43 генеральных прокуроров штатов и округа Колумбия.

Кроме того, Федеральная торговая комиссия США, Министерство здравоохранения и социальных служб США, Управление комиссара по информации Великобритании (ICO), Управление комиссара по информации Австралии и Управление комиссара по вопросам конфиденциальности Канады также направили сообщения., запросы и просьбы.

«Мы можем быть названы стороной в дополнительных судебных процессах, другие претензии могут быть заявлены нашими клиентами или их избирателями или от их имени, и мы можем стать объектом дополнительных правительственных запросов, запросов или расследований», - добавил Блэкбауд.

«Государственные органы также могут стремиться наложить обязательства, судебный запрет, указы о согласии или другие гражданские или уголовные санкции, которые могут, среди прочего, существенно увеличить наши расходы на безопасность данных или иным образом потребовать от нас изменить способ ведения нашего бизнеса».

Расходы, открытые данные и риски безопасности

Blackbaud пришлось потратить более 3 миллионов долларов на ликвидацию последствий атаки в период с июля по сентябрь, а также было зарегистрировано почти 3 миллиона долларов накопленных страховых возмещений за тот же период.

Поставщик облачного программного обеспечения также рассчитывает справиться с повышенными расходами, связанными с продолжающимся реагированием на атаку и усилиями по усилению защиты.

«За три месяца, закончившихся 30 сентября 2020 года, мы зафиксировали 3,2 миллиона долларов расходов и 2,9 миллиона долларов США в виде начисленных страховых возмещений, связанных с происшествием, связанным с безопасностью, а за девять месяцев, закончившихся 30 сентября 2020 года, мы зафиксировали 3,6 миллиона долларов расходов и 2,9 миллиона долларов. начисленных страховых возмещений в связи с происшествием, связанным с безопасностью», - сказали в компании.

В прошлом месяце Блэкбауд также подтвердил в заявке 8-K SEC, что злоумышленники, стоящие за майской атакой программы-вымогателя, смогли получить доступ к незашифрованной банковской информации, учетным данным и номерам социального страхования некоторых клиентов.

В зависимости от того, какая банда вымогателей украла эти данные, его готовность фактически уничтожить их, как и было обещано, после получения выкупа, и что они будут с ними делать, если они не будут уничтожены, клиентам Blackbaud, возможно, придется столкнуться с большим количеством угроз безопасности учитывая очень деликатный характер раскрываемой информации.

Известно, что более 20 операций вымогателей крадут конфиденциальные документы с серверов своих жертв перед шифрованием сетевых систем.

Операторы программ-вымогателей Maze, объявившие вчера о закрытии операций, были первой известной бандой вымогателей, опубликовавшей украденные данные Allied Universal за неуплату выкупа в ноябре 2019 года». ***(Sergiu Gatlan. Blackbaud sued in 23 class action lawsuits after ransomware attack // BleepingComputer.com(https://www.bleepingcomputer.com/news/security/blackbaud-sued-in-23-class-action-lawsuits-after-ransomware-attack/). 03.11.2020).***

***

«Согласно сообщению, опубликованному в понедельник на ее веб-сайте, в результате атаки вымогателя публичная библиотека Нортгемптона была временно закрыта.

«Мы надеемся, что скоро откроемся для публики», - говорится в сообщении. «Затронутые [компьютерные] серверы были отключены, а некоторые библиотечные услуги уже восстановлены. Может пройти несколько дней, прежде чем все библиотечные службы заработают в полную силу. Мы тесно сотрудничаем с нашей ИТ-компанией, чтобы предотвратить будущие атаки. Все буклеты открыты в настоящее время».

Согласно сообщению, библиотека не хранит номера социального страхования или информацию об оплате кредитной картой в своей компьютерной системе. Посетителям, которые использовали Wi-Fi библиотеки, рекомендуется изменить

свои пароли и регулярно проверять свою личную информацию». ***(ANDREW SCOTT. Ransomware attack temporarily closes Northampton Area Public Library // The Morning Call (https://www.mcall.com/news/local/mc-nws-ransomware-attack-closes-northampton-library-20201118-fzcwd2byyzhz3e7rguyynnilwm-story.html). 17.11.2020).***

***

«Более четверти организаций, которые становятся жертвами атак программ-вымогателей, предпочитают платить выкуп, поскольку они чувствуют, что у них нет другого выбора, кроме как уступить требованиям киберпреступников - а средняя сумма выкупа сейчас составляет более 1 миллиона долларов.

Исследование Crowdstrike, основанное на ответах тысяч специалистов по информационной безопасности и лиц, принимающих решения в области ИТ по всему миру, показало, что 27% заявили, что их организация заплатила выкуп после того, как их сеть была зашифрована с помощью программы-вымогателя.

В то время как правоохранительные органы заявляют, что организации никогда не должны уступать и платить выкуп, многие компании оправдывают оплату тем, что получение ключа дешифрования от злоумышленников рассматривается как самый быстрый и простой способ восстановить сеть.

Однако выплата выкупа в биткойнах не только побуждает банды вымогателей продолжать кампании, потому что они знают, что они прибыльны, но также нет гарантии, что хакеры действительно восстановят сеть полностью.

Заражение сетей с помощью программ-вымогателей оказывается очень прибыльным делом для киберпреступников: согласно данным отчета, средняя сумма выкупа, выплачиваемого за атаку, составляет 1,1 миллиона долларов.

Помимо стоимости выкупа, также вероятно, что организация, подвергшаяся атаке программы-вымогателя, потеряет доход из-за потерянных операций во время простоя, что сделает жертву этих кампаний дорогостоящим мероприятием.

Тем не менее, нападение программі-вымогателя действительно служит тревожным сигналом для большинства жертв; более трех четвертей респондентов опроса заявили, что после успешной атаки с использованием программ-вымогателей их организация обновила свое программное обеспечение и инфраструктуру безопасности, чтобы снизить риск будущих атак, в то время как две трети внесли изменения в своих сотрудников службы безопасности с той же целью в уме.

Непонятно, почему почти четверть тех, кто становится жертвой атак программ-вымогателей, не планируют вносить какие-либо изменения в свои планы кибербезопасности, но, оставив все без изменений, они, вероятно, рискуют стать жертвой будущих атак.

Это особенно актуально в 2020 году, который принес организациям дополнительные уязвимости кибербезопасности из-за увеличения числа людей, работающих из дома из-за пандемии коронавируса.

«В условиях удаленной работы поверхность атаки многократно увеличилась, и безопасность не может быть второстепенным приоритетом бизнеса», - сказал

Зеки Туреди, технический директор CrowdStrike в регионе EMEA…». ***(Danny Palmer. Why ransomware is still so successful: Over a quarter of victims pay the ransom // ZDNet (https://www.zdnet.com/article/why-ransomware-is-still-so-successful-over-a-quarter-of-victims-pay-the-ransom/). 18.11.2020).***

***

«Новое исследование показало, что австралийские организации, эксплуатирующие мультиоблачные инфраструктуры, подвергаются большему риску подвергнуться атаке программ-вымогателей и с большей вероятностью будут платить хакерам за получение их данных в случае атаки.

Veritas в своем австралийском отчете о глобальной устойчивости к программам-вымогателям за 2020 год [PDF] сообщила, что только 43% австралийских респондентов заявили, что их безопасность соответствует растущей сложности их ИТ-среды.

Согласно отчету, около 57% австралийских организаций используют мультиоблачную среду и 15-20 облачных сервисов. Он показал, что 33% организаций с более чем 20 облаками заплатили выкуп в полном объеме, по сравнению с 19% компаний, имеющих менее пяти облаков, которые поступили так же.

В то же время среднее количество облаков, развернутых организациями, которые частично заплатили выкуп, составило 11,47 против 6,17 у предприятий, которые вообще не платили.

Опрос, который был проведен в сентябре 2020 года и включает ответы 150 австралийских старших ИТ-руководителей компаний с численностью сотрудников 1000 и более человек, также показал, что бизнес со сложной облачной архитектурой, вероятно, будет препятствовать быстрому восстановлению после атаки программ-вымогателей.

В то время как 41% предприятий с менее чем пятью облачными провайдерами в своей инфраструктуре столкнулись с нарушением работы менее чем на один день, 67% с более чем 20 облачными облаками потребовалось от пяти до 10 дней, чтобы вернуться в нормальное русло.

«Мы наблюдаем отставание между быстрым расширением поверхности угроз, которое связано с увеличением числа облачных вычислений, и развертыванием решений для защиты данных, необходимых для их защиты, - сказал управляющий директор Veritas Technologies Говард Файфф.

«Наше исследование показывает, что соответствие Essential Eight имеет решающее значение. К счастью, некоторые компании вкладывают средства, чтобы закрыть этот пробел в отказоустойчивости, но если это не будет сделано быстрее, компании останутся уязвимыми».

Что касается инвестиций, более половины австралийских компаний рассказали, что они увеличили свой бюджет безопасности из-за пандемии COVID-19, при этом Veritas отметила, что те, кто увеличил свои инвестиции в безопасность, смогли быстрее восстановить свои данные.

Например, компания указала на то, что 53% австралийских ИТ-руководителей заявили, что они потратили больше на безопасность после пандемии

и смогли восстановить 90% или более своих данных по сравнению с 43% тех, кто потратил меньше.

Тем не менее, результаты показывают, что предстоит еще многое сделать, поскольку средний бизнес может восстановить только 82% своих данных, сказал Veritas.

Когда дело дошло до изучения того, какие инструменты защиты данных были реализованы, главными из них были установка инструментов безопасности и поведенческого анализа, антивирусное программное обеспечение и безопасность конечных точек, а также резервное копирование данных.

Несмотря на то, что австралийские организации продолжают подвергаться риску атак программ-вымогателей, если сравнивать их в глобальном масштабе, они все же находятся в лучшем положении. Австралийские организации подверглись атакам с использованием программ-вымогателей 1,14, что ниже среднемирового показателя 1,87». ***(Aimee Chanthadavong. Survey says Australian companies adopting multi-cloud more likely to pay ransom // ZDNet (https://www.zdnet.com/article/survey-says-australian-companies-with-multi-cloud-more-likely-to-pay-ransom/). 19.11.2020).***

***

«Операторы вымогательской программы Egregor стали выводить на принтеры и кассовые аппараты требования выкупа после шифрования файлов в уязвимых компаниях. Это делается, чтобы обеспечить максимальную публичность.

«Ваши файлы у нас»

Операторы шифровальщика Egregor стали применять новую тактику вымогательства: после шифрования файлов в уязвимой корпоративной сети они выводят требование выкупа на все доступные принтеры.

Подобные случаи были отмечены в южноамериканской торговой сети Cencosud — как минимум в Аргентине и Чили. Сообщение от злоумышленников выводится на всем, что способно печатать текст на бумаге, от принтеров до кассовых аппаратов.

По данным экспертов издания Bleeping Computer, злоумышленники используют отдельный скрипт для печати, который запускается уже после того, как отработал основной исполняемый файл шифровальщика.

Egregor — относительно новый шифровальщик-вымогатель, появившийся в сентябре 2020 г. Его операторы не только шифруют, но и крадут данные, требуя с жертв двойной выкуп.

Как он проникает в атакованные системы, доподлинно неизвестно. Вероятнее всего, речь идет о социальной инженерии — наиболее распространенном методе заражения сетевой инфраструктуры. К настоящему времени есть масса свидетельств тому, что Egregor работает по принципу партнерской программы, и что многие бывшие партнеры шифровальщика Maze переключились на него после того, как операторы Maze объявили о сворачивании деятельности.

Чтобы все знали

Что касается вывода требования выкупа на принтеры, то смысл этой акции заключается в повышении публичности.

Egregor ранее в 2020 г. был отмечен в атаках на такие компании как Ubisoft, Crytek, а также Barnes&Noble. Итог этих атак пока неизвестен.

«Владельцы атакованного бизнеса будут пытаться максимально скрывать факт успешной атаки, если закон не обязывает их делать что-то другое, — отмечает Дмитрий Кирюхин, эксперт по информационной безопасности компании SEC Consult Services. — Кибератака, особенно с использованием шифровальщика, — это не только материальный, но и репутационный ущерб, который немедленно приводит еще и к снижению стоимости ценных бумаг жертв атаки. Поэтому коммерческие структуры охотнее попытаются все скрыть и решить вопрос приватным порядком, если это возможно, или вовсе проигнорировать атаку».

«Операторы Egregor, в свою очередь, пытаются сделать все, чтобы сделать атаку максимально публичной, — добавляет эксперт. — Это используется как дополнительный рычаг давления. Стоит, впрочем, напомнить, что единственный правильный способ реагировать на такие атаки — не платить. К сожалению, иногда бизнес воспринимает выплату выкупа как меньшее из зол, хотя на деле все обстоит ровно наоборот: каждая такая успешная операция — это гарантия новых атак». ***(Роман Георгиев. Хакеры-вымогатели захватывают принтеры компаний и печатают на них требования выкупа // CNews (https://safe.cnews.ru/news/top/2020-11-20_hakeryvymogateli_zahvatyvayut). 20.11.2020).***

***

«Компания Miltenyi Biotec, занимающаяся биомедицинскими и клиническими исследованиями, сообщает, что она полностью восстановила системы после атаки вредоносного ПО, которая произошла в прошлом месяце и затронула глобальную ИТ-инфраструктуру компании.

2500 сотрудников Miltenyi Biotec из 28 стран разрабатывают продукты для клеточных исследований и терапии для клиницистов и исследователей, которые работают над вакцинами и лекарствами от COVID-19.

Она также предоставляет антигены SARS-CoV-2 исследователям, участвующим в разработке вакцины против SARS-CoV-2…

На данный момент компания заявила, что успешно восстановила все операционные процессы, затронутые атакой вредоносного ПО в прошлом месяце. Однако в некоторых странах компания по-прежнему сталкивается с проблемами с их электронной почтой и телефонной системой.

Милтеньи Биотек добавил, что клиентам следует ожидать задержек с выполнением заказов из-за временных операционных проблем, влияющих на системы в течение последних двух недель.

Клиентам также рекомендуется обращаться в случае возникновения срочных дел, требующих немедленной помощи.

«Примите наши извинения за возможные неудобства», - добавила Miltenyi Biotec.

Клиенты, испытывающие трудности, могут связаться с ними, используя список альтернативных контактных номеров, доступных здесь.

Атака программ-вымогателей Mount Locker

Несмотря на то, что Miltenyi Biotec не раскрыла природу вредоносного ПО, которое привело к простоям в работе в течение последних двух недель, банда вымогателей Mount Locker заявила об атаке в начале этого месяца.

Mount Locker

Злоумышленники похитили 5% из 150 ГБ данных, которые, по их утверждениям, были украдены из сети компании на своем сайте утечки данных 4 ноября 2020 года, в виде ZIP-архива, содержащего чуть более 1 ГБ документов Miltenyi Biotec.

Программы-вымогатели Mount Locker начали работать в июле 2020 года после того, как они начали взламывать корпоративные сети, красть конфиденциальные данные и развертывать полезные нагрузки для шифрования систем в сети жертв.

Записки о выкупе Mount Locker, которые видел BleepingComputer, показывают, что в некоторых случаях банда вымогателей Mount Locker требует выкуп в несколько миллионов долларов.

Банда запустила сайт Mount Locker News & Leaks, на котором публиковались украденные файлы жертв, отказывающихся платить выкуп.

Mount Locker также известна тем, что угрожает жертвам связаться со СМИ, телеканалами и газетами, если выкуп не будет уплачен.

К сожалению, программа-вымогатель Mount Locker использует ChaCha20 + RSA-2048, и на данный момент нет возможности восстановить зашифрованные файлы бесплатно…». ***(Sergiu Gatlan. Biotech research firm Miltenyi Biotec hit by ransomware, data leaked // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/biotech-research-firm-miltenyi-biotec-hit-by-ransomware-data-leaked/). 13.11.2020).***

***

«Чилийская многонациональная розничная компания Cencosud подверглась кибератаке со стороны программы-вымогателя Egregor, которая повлияла на работу магазинов.

Cencosud - одна из крупнейших розничных компаний в Латинской Америке с более чем 140 000 сотрудников и доходом в 15 миллиардов долларов в 2019 году. Cencosud управляет широким спектром магазинов в Аргентине, Бразилии, Чили, Колумбии и Перу, включая магазины товаров для дома Easy, супермаркеты Jumbo., и универмаги Парижа.

В эти выходные Cencosud подвергся атаке с использованием программ-вымогателей, которые зашифровали устройства во всех торговых точках и повлияли на работу компании.

По словам аргентинского издателя Clarín, розничные магазины все еще открыты, но некоторые услуги пострадали.

Например, в магазине Easy в Буэнос-Айресе отображается знак, предупреждающий клиентов о том, что они не принимают кредитную карту «Cencosud Card», не принимают возврат или не разрешают забирать покупки через Интернет из-за технических проблем.

Egregor - это программа-вымогатель как услуга, которая начала работать в середине сентября, как раз тогда, когда другая группа вымогателей, известная как Maze, начала прекращать свою деятельность. BleepingComputer узнал от злоумышленников, что многие хакеры, сотрудничавшие с Maze, теперь работают с Egregor.

Clarín также сообщила, что принтеры в многочисленных торговых точках в Чили и Аргентине, таких как магазины товаров для дома Easy, начали распечатывать записки о выкупе, поскольку устройства зашифрованы.

Эта функция - известная «особенность» программы-вымогателя Egregor, которая автоматически распечатывает записки о выкупе на подключенных принтерах после того, как файлы на устройстве были зашифрованы. В случае атак в масштабе сети это потенциально может привести к распечатке тысяч записок о выкупе по всей организации.

В записке о выкупе не приводятся ссылки на доказательства кражи данных, но у Egregor есть история кражи незашифрованных файлов перед развертыванием своих программ-вымогателей.

Эгрегор был ответственен за другие громкие атаки на Crytek, Ubisoft и Barnes and Noble …» ***(Lawrence Abrams. Retail giant Cencosud hit by Egregor Ransomware attack, stores impacted // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/retail-giant-cencosud-hit-by-egregor-ransomware-attack-stores-impacted/). 14.11.2020).***

***

«Фирма Coveware, занимающаяся переговорами о программах-вымогателях, поместила операцию DarkSide во внутренний ограниченный список после того, как злоумышленники объявили о планах размещения инфраструктуры в Иране.

Когда программа-вымогатель DarkSide шифрует сеть, их филиалы крадут незашифрованные файлы, которые они угрожают выпустить, если не будет уплачен выкуп.

Эта стратегия двойного вымогательства всегда подвергается атакам со стороны правоохранительных органов и охранных компаний, которые пытаются нарушить работу или закрыть сайты утечки данных программ-вымогателей, на которых публикуются украденные файлы.

DarkSide планирует разместить инфраструктуру в Иране

Чтобы предотвратить отключение службы утечки данных, банда DarkSide объявила на этой неделе, что они строят распределенную и устойчивую систему хранения данных в Иране и других «непризнанных республиках». В этой системе, если один сервер будет отключен, данные останутся и будут доступны на других серверах.

В октябре Управление по контролю за иностранными активами (OFAC) Министерства финансов США выпустило информационное сообщение, в котором предупредило участников переговоров о программах-вымогателях и американские компании о том, что уплата выкупа может привести к нарушениям санкций и штрафам.

В качестве примеров санкционированных хакерских групп, которые, как известно, борются с программами-вымогателями, в сообщении упоминается:

Наложены санкции на разработчика шифровальщика Cryptolocker Евгения Михайловича Богачева в декабре 2016 года (начиная с 2013 года Cryptolocker использовался для заражения более 234 000 компьютеров, примерно половина из которых находилась в США)

Наложены санкции на двух иранцев за оказание материальной поддержки программе-вымогателю SamSam в ноябре 2018 года (SamSam использовался для нацеливания в основном на правительственные учреждения и компании США, начиная с конца 2015 года и продолжаясь примерно 34 месяца)

Группа Lazarus и две подгруппы, Bluenoroff и Andariel, были подвергнуты санкциям в сентябре 2019 года (эти группы были связаны с программой-вымогателем WannaCry 2.0, которая заразила около 300000 компьютеров в не менее 150 странах в мае 2017 года)

Evil Corp и ее лидер Максим Якубец были подвергнуты санкциям в декабре 2019 года (базирующаяся в России организация по борьбе с киберпреступностью использовала вредоносные программы Dridex для сбора учетных данных для входа в систему из сотен банков и финансовых учреждений в более чем 40 странах, что привело к кражам на сумму более 100 миллионов долларов, начиная с 2015 года; Evil Corp недавно добавила в свой арсенал программу-вымогатель WastedLocker).

Помимо санкций против этих хакерских групп, правительство США ввело санкции против Ирана.

Поскольку выплаты выкупа DarkSide могут использоваться для оплаты иранским хостинг-провайдерам за эту новую систему утечки данных, Coveware поместила программу-вымогатель DarkSide во внутренний ограниченный список и больше не будет обеспечивать с их помощью выплаты выкупа.

"Собственный TOR-сайт DarkSide объявляет о намерении использовать инфраструктуру, размещенную в Иране, санкционированном узле. Цель этой инфраструктуры - хранить данные, украденные у жертв атак с выкупом. Вероятно, что часть доходов от любой предполагаемой выплаты выкупа DarkSide будет использоваться для оплаты поставщиков услуг в Иране. Соответственно, мы поместили DarkSide в наш ограниченный список ", - сказал BleepingComputer генеральный директор Coveware Билл Сигел.

BleepingComputer стало известно, что в электронном письме, отправленном партнерам, объясняется, что это решение Coveware, а не часть какой-либо политики США.

С учетом сказанного, хостинг серверов DarkSide в Иране станет дополнительным препятствием, с которым придется столкнуться бизнесу при определении того, будут ли они платить выкуп». ***(Lawrence Abrams. DarkSide ransomware's Iranian hosting raises U.S. sanction concerns // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/darkside-ransomwares-iranian-hosting-raises-us-sanction-concerns/). 15.11.2020).***

***

«Команды программ-вымогателей как услуги (RaaS) активно ищут партнеров, чтобы разделить прибыль, полученную от внешних атак с использованием программ-вымогателей, нацеленных на известные государственные и частные организации.

Некоторые считают службы RaaS услугами по аренде программ-вымогателей, при которых злоумышленники, взламывающие сети целей, платят комиссию за использование вредоносного ПО RaaS. На самом деле таким образом сдается или продается только программа-вымогатель самого низкого качества.

Более известные банды вымогателей реализуют частные партнерские программы, в которых партнеры могут подавать заявки и резюме для подачи заявки на членство.

Для партнеров, которые приняты в программу, разработчики программ-вымогателей получают скидку 20-30%, а партнеры получают 70-80% выкупных платежей, которые они генерируют.

Чтобы зашифровать системы жертв, аффилированные лица будут запрашивать услуги хакера, который получает доступ к сетям целей, получает права администратора домена, собирает и эксфильтрует файлы, а затем передает всю информацию, необходимую для получения доступа и шифрования данных обратно в аффилированные лица..

Прибыль, получаемая от уплаченных выкупов после каждой из атак, затем будет разделена между командой RaaS, хакерами, взломавшими сеть (взломщик), и партнерской программой вымогателей, как правило, в равных долях.

Уровни банд программ-вымогателей

На данный момент существует более двух десятков активных банд, занимающихся вымогательством как услуга, которые активно стремятся передать вымогательские атаки сторонним организациям.

Как говорится в отчете, опубликованном сегодня компанией Intel 471, занимающимся разведкой угроз, есть также «известные частные банды, действующие в тесных, сплоченных криминальных кругах, использующие прямые и частные каналы связи, о которых мы мало знаем».

Банды программ-вымогателей Intel 471, наблюдавшиеся в прошлом году, можно разделить на три разные группы (или уровни) в зависимости от их известности и времени, в течение которого они были активны.

Они варьируются «от хорошо известных групп, которые стали синонимами программ-вымогателей, до вновь сформированных вариантов, выросших из неудач старых, до совершенно новых вариантов, которые могут иметь возможность свергнуть текущие клики высшего уровня».

Банды вымогателей TIER 1 - это группы, которые за последние годы успешно выкупили сотни миллионов выкупов.

Подавляющее большинство из них также используют дополнительные схемы вымогательства, такие как кража конфиденциальной информации из сетей своих жертв и угроза утечки ее, если не будет уплачен выкуп.

Экипажи RaaS, включенные в группу TIER 1: DopplePaymer (используется в атаках на Pemex, Bretagne Télécom, Университет Ньюкасла, Университет Дюссельдорфа), Egregor (Crytek, Ubisoft, Barnes & Noble), Netwalker / Mailto

(Equinix, UCSF, Государственный университет штата Мичиган, Toll Group) и REvil / Sodinokibi (Travelex, аэропорт Нью-Йорка, местное правительство Техаса).

Ryuk находится на вершине рейтинга, и его полезные нагрузки были обнаружены примерно в каждой третьей атаке программ-вымогателей за последний год.

Группа также известна тем, что доставляет свои полезные нагрузки в рамках многоэтапных атак с использованием векторов заражения Trickbot, Emotet и BazarLoader для легкого проникновения в сети своих целей.

Филиалы Ryuk также стояли за огромной волной атак на систему здравоохранения США и за вымогательство огромных выкупов, собрав 34 миллиона долларов с одной жертвы в начале этого года.

Операции TIER 2 RaaS постепенно выросли до большего числа филиалов в течение 2020 года и были вовлечены в несколько подтвержденных атак.

Вымогатели группа, включенная в этом ярусе является SunCrypt, Conti, Clop, Рагнар Локер, Pysa / Mespinoza, Avaddon, DarkSide (считается осколком Revil), и многими другими.

Как и банды вымогателей TIER 1, они также используют тактику вымогательства кражи данных в качестве вторичного метода вымогательства.

Команды TIER 3 RaaS предлагают вновь созданные филиалы, но, согласно Intel 471, «информация об успешных атаках, объеме атак, полученных платежах или стоимости смягчения последствий ограничена».

Группы, помеченные как новые банды TIER 3, включают Nemty, Wally, XINOF, Zeoticus, CVartek.u45, Muchlove, Rush, Lolkek, Gothmog и Exorcist.

Другие активные группы RaaS

Помимо группировок программ-вымогателей, перечисленных Intel 471 как активно ищущих партнеров, BleepingComputer также знает о других крупных и новых командах RaaS.

Например, Dharma - это давний RaaS, который существует с 2017 года и известен как ответвление программы-вымогателя Crysis, которая начала работать в 2016 году.

Dharma не использует сайты утечки данных, и нет обширных сообщений о краже данных. Выкуп, который собирают их филиалы, может варьироваться от тысяч до сотен тысяч долларов США.

LockBit, еще одна широко известная операция RaaS, появилась в сентябре 2019 года как частная операция, нацеленная на предприятия, а затем наблюдалась Microsoft при атаках на здравоохранение и критически важные службы.

Банда LockBit объединилась с Maze, чтобы создать картель вымогателей для использования одной и той же платформы утечки данных во время атак, а также для обмена тактикой и разведданными.

Злоумышленникам-вымогателям LockBit также требуется всего пять минут для развертывания полезной нагрузки после получения доступа к сети жертвы.

Другие операции RaaS, оставшиеся за пределами уровней Intel 471, - это Ragnarok, CryLock, ProLock, Nefilim и Mount Locker, и все они, как известно, были активны и участвовали в недавних атаках». ***(Sergiu Gatlan. Dozens of ransomware gangs partner with hackers to extort victims // Bleeping Computer®***

(https://www.bleepingcomputer.com/news/security/dozens-of-ransomware-gangs-partner-with-hackers-to-extort-victims/). 16.11.2020).

***

«В начале текущей недели крупный поставщик решений для управляемого веб-хостинга Managed[.]com пострадал от вымогательской атаки. Компания была вынуждена отключить все свои серверы, и инцидент затронул даже клиентские сайты. По данным СМИ, ответственность за эту атаку лежит на операторах вымогателя REvil.

…атака произошла 16 ноября 2020 года, и в этот же день специалисты компании решили отключить все свои системы, включая те, что поддерживают сайты пользователей, чтобы защитить «целостность данных клиентов».

Сначала сообщалось, что вымогатель успел зашифровать лишь некоторые сайты, которые были немедленно изолированы и отключены, но позже в компании предупредили, что атака повлияла на всю хостинговую инфраструктуру, включая управляемые хостинговые решения WordPress и DotNetNuke, почтовые серверы, DNS-серверы, эндпоинты RDP, FTP-серверы и базы данных. В настоящее время ведутся восстановительные работы, а также компания проводит расследование случившегося, совместно с правоохранительными органами.

Журналисты отмечают, что вначале компания и вовсе попыталась выдать эту атаку за внеплановые технические работы, но довольно быстро представители Managed[.]com осознали свою ошибку и сообщили о реальном положении дел.

Теперь обеспокоенные клиенты хостера пишут на форумах компании, что их сайты могут оказаться недоступными на долгие дни или даже недели. Люди ссылаются на похожий инцидент, от которого в мае 2019 года пострадал хостер A2 Hosting. Тогда компании потребовалось более месяца для возвращения к нормальной работе, и многим клиентам пришлось ждать, пока их сайты и данные сайтов будут восстановлены.

По информации издания Bleeping Computer, которое ссылается на собственные источники в ИБ-сообществе, ответственность за эту атаку лежит на операторах вымогателя REvil. Согласно скриншоту, оказавшемуся в распоряжении издания, REvil требует у пострадавшей компании выкуп в размере 500 000 долларов США. При этом пока неясно, сумели ли хакеры похитить у компании какие-то данные, перед тем как зашифровали файлы». ***(Мария Нефёдова. Атака шифровальщика REvil вынудила крупного хостера отключить клиентские сайты // Хакер (https://xakep.ru/2020/11/19/managed-hacked/). 19.11.2020).***

***

«Хотя все компании, атакуемые вымогательским ПО, различны между собой, они все равно могут учиться на опыте друг друга. Пошаговая экспертиза атаки программы-вымогателя может помочь организациям осознать, что они также могут быть уязвимы к подобным атакам, а также пояснить, какие шаги следует предпринять во избежание этих атак.

На проходившей в online-режиме конференции (ISC)² Security Congress глава компания SCADAfence Элад Бен-Мейр (Elad Ben-Meir) представил подробности

расследования атаки вымогательского ПО на крупное европейское промышленное предприятие, имевшей место ранее в нынешнем году. Подробности взлома и другие данные экспертизы представляют большую ценность для команд безопасности организаций.

Описанная SCADAfence кибератака началась ночью. В результате инцидента несколько критически важных сервисов перестали функционировать. IT-команда пострадавшего предприятия обнаружила на многих устройствах в корпоративной сети записку с требованием выкупа. Сначала она намеревалась заплатить выкуп, но после того, как вымогатели повысили цену, изменила свое решение и обратилась за помощью к команде реагирования на инциденты SCADAfence.

В течение первых семи часов атаки более 200 критических серверов были зашифрованы, и вся производственная линия остановилась. До прибытия на место происшествия специалисты проинструктировали IT-команду предприятия, как изолировать угрозу в одном определенном месте сети и тем самым сдержать ее распространение, сократить время простоя затронутых систем и сохранить улики в первоначальном виде.

Специалисты начали сбор доказательств еще до прибытия на место происшествия. Они попросили IT-команду предприятия как можно скорее собрать образы затронутых систем, файлов реестра и конфигурационных файлов, а также другие сведения, которые могли помочь в расследовании.

Прибыв на место происшествия, специалисты изучили инфицированные компьютеры. Они искали устройства с признаками вредоносной активности, например, с инструментами для осуществления атаки, которые могли привести к дальнейшему распространению инфекции. «Это дало нам уникальную картину того, что с чем коммуницирует, и как можно остановить атаку, определив эти связи», - сообщил Бен-Мейр.

Специалисты проверили конфигурацию машин, подозрительные исполняемые файлы, временные метки в файлах, файлы журналов и журналы событий. Подозрительные исполняемые и двоичные файлы были отправлены для дальнейшего анализа экспертам по реверс-инжинирингу. Экспертиза показала источник атаки, использовавшиеся в ней инструменты и индикаторы компрометации собранных двоичных и исполняемых файлов.

Через несколько часов после прибытия на место происшествия исследователи заметили активность сканирования сети с машины, отсутствующей в их списке зараженных устройств. Сканирование не было видно в журналах межсетевого экрана, потому что некоторые сети были соединены мостом с помощью сетевой карты (NIC) на машине, а не маршрутизации через межсетевой экран. IT-команда предприятия не знала об этих конфигурациях и считала, что весь межсегментный трафик маршрутизируется через межсетевой экран.

Для проникновения в корпоративную сеть злоумышленники использовали несколько методов. Во-первых, атакующие отключили обновления Windows и пытались скрыть свою активность, сохраняя исполняемые файлы в легитимных папках. Во-вторых, они отключили защиту конечных точек и в-третьих, заблокировали устройства ввода во время шифрования, чтобы сотрудники предприятия не могли остановить процесс шифрования.

Через 10 часов после прибытия специалистов на место происшествия ситуация была под контролем. Следователи выяснили, что зараженная машина была сторонним устройством, управляемым внешним подрядчиком, а его единственная цель заключалась в обеспечении входа в операционную технологическую сеть для обслуживания и поддержки. У машины был внешний IP-адрес, что затрудняло его поиск в журналах межсетевого экрана, и доступный через интернет открытый RDP-порт. Более того, устройство давно не обновлялось, а его межсетевой экран был отключен.

Во многих компаниях используется хотя бы одно неуправляемое устройство, открывающее доступ ко всей сети. Из-за недостаточной устойчивости такое устройство может позволить угрозе распространиться по всей сети. Для организаций крайне важно знать, кто подключается к их сети, установлены ли на устройстве обновления безопасности и включена ли защита конечных точек.

Бен-Мейр настоятельно рекомендовал компании сегментировать свои сети. «Чем меньше сегменты, тем они жестче и лучше управляемые и тем меньше вероятность распространения угрозы, меньше реальный ущерб инфраструктуре и меньше сбоев в производстве», - сообщил он». ***(Эксперты пошагово представили расследование атаки вымогательского ПО // SecurityLab.ru (https://www.securitylab.ru/news/514117.php). 17.11.2020).***

***

«В 2020 году количество зарегистрированных кибератак на производственные предприятия с использованием вымогательского ПО резко возросло, так как киберпреступники научились срывать производственные процессы, атакуя и IT-сети компании, и использующееся в производстве ПО.

Как сообщается в новом отчете ИБ-компании Dragos, по сравнению с 2019 годом, в 2020 году число кибератак с использованием программ-вымогателей на производственные предприятия увеличилось более чем в три раза (точное количество кибератак в отчете не указано). По словам экспертов, это объясняется двумя факторами. Во-первых, организации стали чаще сообщать о подобных инцидентах, а во-вторых, киберпреступники стали более агрессивными и знают, как выбить компании из колеи.

В частности в отчете Dragos рассматриваются кибератаки на компании Honda и Evraz, которым из-за инцидента пришлось остановить некоторые производственные процессы. Как отметили специалисты, кибератака на Honda указывает на тревожную тенденцию – операторы вымогательского ПО все чаще используют код, способный нарушить работу программного обеспечения, поддерживающего производственные процессы.

Согласно отчету, финансируемые государствами хакерские группы (так называемые APT-группы) редко ограничиваются компаниями одного конкретного сектора. Пять таких групп проявляют интерес к производству, но в то же время атакуют и электроэнергетическую, аэрокосмическую и другие отрасли.

Не исключено, что APT-группы тестируют свои возможности в производственном секторе. На некоторых крупных производствах установлено то

же оборудование, что и на украинских электроэнергетических компаниях, атакованных хакерами в 2016 году.

В отчете утверждается, что такие сложные постоянные угрозы, как часто называют группы, связанные с государством, могут проверить свои возможности в производственном секторе. Некоторые крупные производственные компании имеют на своих объектах электроэнергию, на которой установлено то же оборудование, которое использовалось подозреваемыми российскими хакерами, отключившими электричество в Украине в 2016 году». ***(В 2020 году число атак вымогательского ПО на производства утроилось // SecurityLab.ru (https://www.securitylab.ru/news/514061.php). 13.11.2020).***

***

«Canon наконец публично подтвердила, что кибератака, перенесенная в начале августа, была вызвана программами-вымогателями и что хакеры украли данные с серверов компании.

BleepingComputer первым сообщил об атаке после отслеживания подозрительного сбоя в облачном хранилище фото и видео (image.canon), в результате которого пользователи теряли файлы.

Данные сотрудников украдены

5 августа Canon USA разослала всей компании уведомление, информирующее сотрудников о серьезных системных проблемах, из-за которых несколько приложений, в том числе команды, и электронная почта, были недоступны.

Частичный снимок экрана с запиской о выкупе, полученной BleepingComputer, показал, что сбой был вызван программой-вымогателем Maze, которая обычно крадет данные из взломанных сетей, чтобы заставить жертв заплатить.

Canon начала расследование инцидента и обнаружила доказательства несанкционированной активности в своей сети в период с 20 июля по 6 августа.

Злоумышленник получил доступ к своим файловым серверам, на которых также размещалась «информация о нынешних и бывших сотрудниках с 2005 по 2020 год, а также их бенефициарах и иждивенцах».

В публичном объявлении в среду вечером Canon сообщает, что данные, к которым получил доступ злоумышленник, включали имена сотрудников, номер социального страхования, дату рождения, номер водительского удостоверения или удостоверение личности государственного образца, номер банковского счета для прямых депозитов. от Canon, и их электронная подпись.

Вскоре после атаки программы-вымогатели Maze сообщили BleepingComputer, что они украли у Canon 10 терабайт данных и частных баз данных, а 5 августа взорвали вредоносное ПО для шифрования файлов.

Удивительно, но проблема с image.canon и общий сбой в работе Canon USA, вызванный атакой, никак не связаны. Maze подтвердил, что их действия не распространяются на службу хранения.

Хотя на то, чтобы публично подтвердить атаку программы-вымогателя, потребовалось три месяца, Canon признала характер инцидента безопасности своим сотрудникам в уведомлении внутренней безопасности от 6 августа.

Лабиринта больше нет

Киберпреступная группировка Maze была одним из крупнейших игроков в бизнесе вымогателей. 1 ноября банда прекратила свою деятельность, начатую примерно полтора года назад, в мае 2019 года.

Они несут ответственность за текущую тенденцию к двойному вымогательству, которую сегодня разделяют большинство операторов программ-вымогателей, когда они крадут данные перед их шифрованием и угрожают утечкой файлов, если жертва не заплатит выкуп.

Среди их жертв - крупные компании Allied Universal, Southwire, City of Pensacola, Canon, LG Electronics и Xerox». ***(Ionut Ilascu. Canon publicly confirms August ransomware attack, data theft // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/canon-publicly-confirms-august-ransomware-attack-data-theft/). 26.11.2020).***

***

«Французская многонациональная производственная и дистрибьюторская компания Banijay Group SAS в начале этого месяца подверглась атаке программы-вымогателя DoppelPaymer, и во время инцидента операторы программы-вымогателя похитили конфиденциальную информацию.

Вчера Баниджай публично подтвердил киберинцидент, в результате которого конфиденциальные данные сотрудников и коммерческие данные были потенциально скомпрометированы.

Banijay стала одной из крупнейших, если не крупнейшей международной группой на рынке производства и распространения аудиовизуального контента после приобретения Endemol Shine Group за 2,2 миллиарда долларов в июле 2020 года.

В настоящее время в группе работает более 120 продюсерских компаний на 22 территориях, и она стоит за некоторыми из крупнейших мировых развлекательных брендов, включая контент со сценариями и без сценариев.

Список брендов Banijay включает MasterChef, Survivor, Big Brother, The Kardashians, Mr. Bean, Black Mirror, Extreme Makeover: Home Edition, Deal or No Deal и многие другие.

Только сети Endemol, затронутые атакой

«Баниджай в настоящее время занимается киберинцидентом с уже существующими сетями Endemol Shine Group и Endemol Shine International», - заявили в группе.

«У компании есть основания полагать, что некоторые личные данные нынешних и бывших сотрудников могли быть скомпрометированы, а также коммерческая конфиденциальная информация».

Баниджай сообщил об инциденте местным властям Соединенного Королевства и Нидерландов, где находится имущество, пострадавшее в результате нападения.

Французская группа по производству аудиовизуальных материалов также наняла сторонних экспертов по безопасности для помощи в расследовании атаки.

«Глобальная группа в настоящее время расследует ситуацию с независимыми специалистами и на сегодняшний день сообщила о проблеме соответствующим местным властям как в Нидерландах, так и в Великобритании - территориях, пострадавших от инцидента», - добавил Баниджай.

«Мы продолжаем предпринимать соответствующие шаги и по-прежнему привержены защите наших сотрудников, прошлых и настоящих, поэтому, если мы обнаружим какие-либо случаи получения или неправомерного использования данных, мы свяжемся с затронутыми лицами напрямую».

DoppelPaymer утверждает, что стоит за атакой

В то время как Banijay только сообщил, что они подверглись кибератаке и что некоторые из их данных могли быть скомпрометированы, банда вымогателей DoppelPaymer заявляет о своей ответственности.

В качестве доказательства своей причастности к атаке операторы DoppelPaymer поделились несколькими документами, предположительно украденными из систем Banijay, - тактика, принятая от Maze Ransomware, начиная с февраля 2020 года.

DoppelPaymer также насмехается над французской производственной группой, ссылаясь, в частности, на проблемы соблюдения GDPR и утечка внутреннего документа о соответствии GDPR.

DoppelPaymer - это программа-вымогатель, известная своей способностью поражать корпоративные цели как минимум с середины июня 2019 года, получая доступ к учетным данным администратора и используя их для развертывания полезных данных вымогателя на всех устройствах после компрометации всей сети.

Эта банда вымогателей также известна тем, что требует больших выкупов, поскольку известно, что они шифруют сотни и даже тысячи устройств в сетях своих жертв.

Например, в ноябре 2019 года государственная нефтяная компания Мексики PEMEX пострадала от DoppelPaymer и ее попросили заплатить биткойны на сумму 4,9 миллиона долларов в качестве выкупа.

DoppelPaymer получил свое название от BitPaymer (с которым он делится большими частями кода), но группа также добавила множество обновлений, включая процесс поточного шифрования для более быстрой работы.

Представитель Banijay не был немедленно доступен для комментариев, когда сегодня с ним связались представители BleepingComputer». ***(Sergiu Gatlan. MasterChef, Big Brother producer hit by DoppelPaymer ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/masterchef-big-brother-producer-hit-by-doppelpaymer-ransomware/). 27.11.2020).***

***

«Ritzau, крупнейшее независимое информационное агентство в Дании, основанное в 1866 году Эриком Ритцау, заявило в заявлении, что не будет платить выкуп, который потребовала банда вымогателей, поразившая его сеть во вторник утром.

Согласно статистике, предоставленной Gallup и Dansk Online Index за 2015 и 2016 годы, аудитория датского информационного агентства включает 10 миллионов радиослушателей, 8 миллионов телезрителей, 3 миллиона читателей газет и 15 миллионов читателей из цифровых источников новостей.

«Хакеры атаковали Ритцау рано утром во вторник, и, таким образом, информационное агентство подвергалось атакам более суток», - говорится в заявлении информационного агентства. «Атака означала, что редакционные системы были закрыты».

«Информационное агентство, которое доставляет новости практически всем основным средствам массовой информации в Дании, не может транслировать новости в обычном режиме. Вместо этого используется аварийная система, где новости передаются средствам массовой информации страны другим способом».

Сумма выкупа неизвестна

По словам генерального директора Ларса Вестерлокке, Ритцау не будет платить выкуп, который потребовали злоумышленники, стоящие за атакой программы-вымогателя, поразившей сеть информационного агентства.

Хотя группа программ-вымогателей, которая успешно зашифровала системы Ritzau, еще не известна, Вестерлокке назвал атаку «очень профессиональной» согласно опубликованному сегодня заявлению.

«Информационное агентство Ritzau во вторник подверглось масштабной хакерской атаке, и впоследствии хакеры потребовали выкуп за публикацию данных», - сказал Вестерлокке. «Ритцау отказался платить деньги хакерам».

Несмотря на то, что злоумышленники оставили записку о выкупе на зашифрованных компьютерах Ритцау, новостное агентство не выполнило инструкции, необходимые для получения доступа к более подробной информации о требуемой сумме выкупа за дешифратор.

«Они оставили файл с сообщением с более подробной информацией, но мы решили не открывать его после указаний наших консультантов», - добавил Вестерлокке.

Полное выздоровление ожидается в четверг

В ходе атаки группа вымогателей смогла взломать и зашифровать примерно четверть из более чем 100 серверов в сети Ritzau.

ИТ-отдел Ritzau сейчас работает над восстановлением всех затронутых компьютеров и их возвращением в рабочий режим.

Информационному агентству также помогают специалисты, предоставленные его страховой компанией, и оно также наняло внешнюю охранную компанию, специализирующуюся на анализе и предотвращении таких атак.

Информационное агентство рассчитывает возобновить нормальную работу в течение 24 часов, переключившись с системы экстренного распространения,

которая использует шесть живых блогов, на свои обычные каналы выпуска новостей как можно скорее.

«Технический сбой означает, что мы не можем транслировать новости в обычном режиме через службу новостей», - говорится в заявлении информационного агентства. «Мы планируем начать работу не раньше четверга». ***(Sergiu Gatlan. Danish news agency Ritzau refuses to pay after ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/danish-news-agency-ritzau-refuses-to-pay-after-ransomware-attack/). 25.11.2020).***

***

«Французский гигант ИТ-услуг Sopra Steria заявил сегодня в официальном заявлении, что октябрьская атака вымогателя Ryuk приведет к убыткам в размере от 40 до 50 миллионов евро.

Sopra Steria - европейская компания, занимающаяся информационными технологиями, со штатом 46 000 сотрудников в 25 странах, предоставляющая широкий спектр ИТ-услуг, включая консалтинг, системную интеграцию и разработку программного обеспечения.

«Ожидается, что устранение последствий и различные уровни недоступности различных систем с 21 октября окажут серьезное негативное влияние на операционную маржу в размере от 40 до 50 миллионов евро», - сказал Сопра Стерия. «Страховое покрытие Группы от киберрисков составляет 30 миллионов евро».

Атака Октябрьского Рюка

21 октября Sopra Steria опубликовала заявление о кибератаке, обрушившейся на ее сеть вечером 20 октября, но не предоставила подробностей о том, кто стоял за атакой.

Однако у BleepingComputer была информация от источника, знакомого с атакой, что французская компания, предоставляющая ИТ-услуги, была атакована группой вымогателей Ryuk, которая в сентябре также зашифровала системы Universal Health Services.

Когда BleepingComputer обратилась к Sopra Steria за дальнейшими подробностями и подтверждением атаки Ryuk, нам сказали, что у них «нет дополнительных подробностей, которыми можно поделиться».

Неделю спустя Сопра Стерия подтвердила в заявлении, отправленном BleepingComputer, что это действительно была атака Ryuk с использованием новой версии вымогателя Ryuk.

«Более того, также было установлено, что кибератака была начата всего за несколько дней до того, как она была обнаружена», - сказал Сопра Стерия BleepingComputer.

Никаких утечек данных после атаки вымогателя не произошло

Атака программы-вымогателя была заблокирована внутренними службами безопасности и ИТ-специалистами Sopra Steria, которые направили программу-вымогатель на «ограниченную часть инфраструктуры Группы», таким образом защищая данные компании, а также ее клиентов и партнеров.

«На данном этапе Sopra Steria не выявила утечки данных или ущерба, причиненного информационным системам ее клиентов», - сказал Сопра Стерия.

Процесс восстановления, начатый компанией 26 октября, почти завершен: восстановлен доступ почти ко всем «рабочим станциям, серверам НИОКР и производственным серверам, а также внутренним инструментам и приложениям».

«После включения упомянутых выше статей в 2020 финансовом году Sopra Steria ожидает увидеть отрицательный органический рост выручки в размере от 4,5% до 5,0% (ранее« от -2% до -4% »), операционная маржа по деловой активности составит около 6,5% (ранее «от 6% до 7%») и свободный денежный поток от 50 до 100 млн евро (ранее «от 80 до 120 млн евро») », - добавила компания.

Cognizant, одна из крупнейших в мире компаний, предоставляющих управляемые ИТ-услуги, также заявила, что ожидает убытков в размере от 50 до 70 миллионов долларов после атаки вымогателя Maze с апреля 2020 года.

Гигант по производству алюминия Norsk Hydro заявил через неделю после раскрытия информации об атаке программы-вымогателя LockerGoga, в результате которой компания перешла в частичный ручной режим, что «предварительная оценка финансовых последствий в течение первой полной недели» после атаки составляла от 300 до 350 миллионов норвежских крон. (от 33 до 39 миллионов долларов)». ***(Sergiu Gatlan. Sopra Steria expects €50 million loss after Ryuk ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/sopra-steria-expects-50-million-loss-after-ryuk-ransomware-attack/). 25.11.2020).***

***

«US Fertility, крупнейшая сеть центров репродуктивного здоровья в США, сообщает, что некоторые из ее систем были зашифрованы в результате атаки вымогателя, которая затронула компанию два месяца назад, в сентябре 2020 года.

Сеть USF Fertility (USF) состоит из 55 пунктов в 10 штатах, которые в 2018 году прошли почти 25000 циклов ЭКО через свои клиники и более 80 врачей.

В общей сложности более 130 000 детей родились с помощью партнерских практик ЭКО / фертильности в сети USF, включая, помимо прочего, Shady Grove Fertility, Центр репродуктивных наук Сан-Франциско, ЭКО Флориды и Центр фертильности Иллинойса.

Системы не работают более недели

«14 сентября 2020 года в USF произошло событие, связанное с ИТ-безопасностью [..], связанное с недоступностью определенных компьютерных систем в нашей сети в результате заражения вредоносным ПО», - говорится в официальном заявлении USF.

«Посредством нашего немедленного расследования и ответа мы определили, что данные на ряде серверов и рабочих станций, подключенных к нашему домену, были зашифрованы с помощью программы-вымогателя».

Сторонние судебно-медицинские эксперты были привлечены USF сразу после обнаружения атаки, чтобы помочь расследовать инцидент с безопасностью.

USF отключила затронутые серверы и рабочие станции после обнаружения атаки. USF удалось восстановить их с помощью сторонних компьютерных криминалистов и повторно подключить их к сети 20 сентября.

Сеть плодородия также проинформировала федеральные правоохранительные органы об атаке программы-вымогателя и продолжает работать с ними на протяжении всего расследования инцидента.

Защищенная медицинская информация, украденная в результате атаки

«Криминалистическое расследование завершено и подтвердило, что неавторизованный субъект приобрел ограниченное количество файлов в период несанкционированного доступа, который произошел с 12 августа 2020 года по 14 сентября 2020 года, когда была запущена программа-вымогатель», - говорится в уведомлении USF. Детали.

После проверки всех файлов, к которым был получен доступ во время атаки, завершившейся 13 ноября, USF определила, что файлы, отфильтрованные неизвестной группой программ-вымогателей, содержат различные типы информации для каждого пострадавшего человека, включая имена, адреса, даты рождения, номера MPI и социальные сети. Номера безопасности.

«Типы затронутой информации зависят от человека, и мы определили, что для многих людей номера социального страхования не были затронуты», - добавил USF.

«Также обратите внимание, что у нас нет доказательств фактического неправомерного использования информации какого-либо лица в результате Инцидента»…». ***(Sergiu Gatlan. Ransomware hits largest US fertility network, patient data stolen // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ransomware-hits-largest-us-fertility-network-patient-data-stolen/). 26.11.2020).***

***

«Южнокорейский конгломерат моды и розничной торговли E-Land Group заявил в воскресенье, что приостановил работу почти половины своих магазинов в стране из-за атаки программ-вымогателей.

Группа сообщила, что ее корпоративная сетевая система была атакована программой-вымогателем рано утром. Такая атака вредоносного ПО вынудила 23 из 50 ее филиалов NC Department Store и NewCore Outlet прекратить свою деятельность, добавляет E-Land…

Группа заявила, что в настоящее время отключила часть своей корпоративной сетевой системы, чтобы минимизировать ущерб, и попросила полицию расследовать кибератаку». ***(Retail giant E-Land suspends operations at nearly half of stores due to ransomware attack // Yonhap News Agency (https://en.yna.co.kr/view/AEN20201122001900320). 22.11.2020).***

***

«Сегодня государственные школы округа Балтимор подверглись атаке с использованием программ-вымогателей, которая привела к системному отключению их сети из-за количества систем, затронутых атакой.

Школьный округ округа Балтимор управляет всеми государственными школами округа Балтимор, штат Мэриленд, и является 25-й по величине школьной системой США.

Интернет-школы и офисы закрыты

Майкл Дикерсон, глава администрации округа, подтвердил, что атака затронула офисы школьного округа, веб-сайт, систему электронной почты и систему выставления оценок.

Округу также пришлось приостановить все виртуальное обучение и закрыть офисы после атаки программ-вымогателей, поразивших его системы.

«Из-за проблем с нашей сетью все государственные школы округа Балтимор будут закрыты сегодня, в среду, 25 ноября 2020 года», - сказал он.

«Государственные школы округа Балтимор теперь могут подтвердить, что мы стали жертвой кибератаки программ-вымогателей [sic]», - добавил позже Дикерсон.

«Это вызвало системное прерывание работы наших сетевых информационных систем. Наша технологическая группа BCPS работает над исправлением ситуации. Обновления по мере возможности».

В зависимости от банды вымогателей, которая зашифровала системы школьного округа, эта атака также может привести к утечке данных, если информация о сотрудниках и учениках была украдена с компьютеров школьного округа.

Прямо сейчас более 20 операций программ-вымогателей крадут конфиденциальные документы с серверов своих жертв до того, как зашифруют сетевые системы.

Студентов из Балтимора призвали использовать только устройства, выданные округом

Округ государственных школ города Балтимора также опубликовал на своем веб-сайте предупреждение, призывающее учащихся использовать только выданные школой устройства для виртуального обучения.

«Учащиеся, участвующие в виртуальном обучении, должны использовать только ноутбуки или устройства, выданные городскими школами», - говорится в уведомлении.

«Не используйте устройства, выданные школами округа Балтимор, или ваш личный ноутбук или компьютер. Учащимся, не имеющим доступа к устройству, выданному городскими школами, будет предоставлено освобождение от занятий».

На этот раз никакие государственные системы не пострадали

Округ Балтимор сообщил WMAR, что не обнаружил доказательств того, что правительственные системы были скомпрометированы во время атаки вымогателя.

Однако в мае 2019 года мэрии Балтимора не повезло, так как некоторые из ее правительственных серверов были зашифрованы в результате атаки вымогателя RobbinHood.

В то время городу пришлось отключить большинство своих серверов, чтобы предотвратить распространение вредоносного ПО и шифрование других систем.

Сегодняшняя атака программ-вымогателей - третья за последние три года после того, как в марте 2018 года была нарушена работа системы экстренного вызова Балтимора, когда персоналу пришлось переключиться на ручные операции

для обработки всех входящих вызовов экстренной помощи, согласно NBC NEWS». ***(Sergiu Gatlan. Baltimore County Public Schools hit by ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/baltimore-county-public-schools-hit-by-ransomware-attack/). 25.11.2020).***

***

Програми-трояни

«Злоумышленники воспользовались сохраняющейся неопределенностью вокруг выборов в США в 2020 году, чтобы развернуть новую кампанию по распространению вредоносного спама, направленную на распространение трояна Qbot.

По словам новых исследователей, преступники, стоящие за Qbot, снова появились на следующий день после выборов с волной спама в электронных письмах, которые пытаются заманить жертв сообщениями, в которых содержится информация о вмешательстве в выборы.

«Выборы в США в 2020 году были предметом пристального внимания и эмоций, хотя происходили в разгар глобальной пандемии», - сообщили исследователи из Malwarebytes Labs в среду. «В этом случае мы начали наблюдать за новой кампанией по рассылке спама, рассылающей вредоносные вложения, которые используют сомнения относительно избирательного процесса». Qbot, постоянно развивающийся троян для кражи информации, который существует с 2008 года, снова появился в этом году после перерыва, нацелившись на клиентов финансовых учреждений США с новыми возможностями, чтобы помочь ему оставаться незамеченным. Его нынешнее воплощение превратилось в «швейцарский армейский нож» вредоносного ПО, которое может красть информацию, устанавливать программы-вымогатели и совершать несанкционированные банковские транзакции.

Последние сообщения электронной почты, обнаруженные командой MalwareBytes Labs, включают в себя вложения в формате ZIP с именем «ElectionInterference_ [от 8 до 9 цифр] .zip» с просьбой к получателю «Прочитать документ и сообщить мне, что вы думаете».

Если жертва клюнет на приманку, она нажимает на электронную таблицу Excel, созданную так, как если бы это был защищенный файл DocuSign. «Пользователи обманываются, позволяя макросам «расшифровать» документ», - говорят исследователи.

После включения макроса загружает вредоносную полезную нагрузку, содержащую трояна Qbot, URL-адрес которого закодирован в ячейке листа с кириллицей «Лист3». После выполнения троян связывается со своим сервером управления и контроля, чтобы запросить инструкции для его гнусной деятельности. В этом случае Qbot крадет и эксфильтрует данные о жертвах, а также собирает электронные письма, которые могут быть использованы в будущих кампаниях по распространению вредоносного спама, говорят исследователи.

Последняя кампания Qbot использует уловку, которую команда разработчиков трояна Emotet, которую правительство США считает одной из наиболее распространенных существующих киберугроз, также использовала, чтобы «повысить легитимность и усложнить обнаружение», - отметили Сегура и Джази. Эта тактика заключается в том, чтобы электронные письма приходили в виде ответов цепочки, чтобы попытаться обмануть потенциальных жертв, чтобы они думали, что сообщение было частью предыдущего электронного письма.

Действительно, Qbot ранее был связан с Emotet, запуская вредоносное ПО в рамках метода распространения, использованного в кампании в начале этого года. Qbot также был одним из вредоносных программ, распространяемых в ходе связанной с выборами кампании целевого фишинга Emotet в начале октября, в ходе которой были отправлены тысячи вредоносных электронных писем, якобы от Национального комитета Демократической партии, для набора потенциальных добровольцев-демократов.

То, что субъекты угрозы используют неопределенность выборов 2020 года, официальный исход которых остается неизвестным, не вызывает удивления. Исследователи безопасности давно ожидали, что день выборов и его последствия будут сорваны киберугрозами.

Действительно, нынешний сценарий выборов 2020 года является идеальной пищей для схем социальной инженерии, часто используемых злоумышленниками для массового распространения вредоносных программ через вредоносные электронные письма, отметили Сегура и Джази.

«Субъектам угроз необходимо заставить жертв выполнить определенный набор действий, чтобы скомпрометировать их», - написали они. «Мировые события, такие как пандемия Covid или выборы в США, предоставляют идеальный материал для разработки эффективных схем, приводящих к высокому уровню инфицирования». ***(Elizabeth Montalbano. Malspam Campaign Milks Election Uncertainty // Threatpost (https://threatpost.com/malspam-campaign-milks-election-uncertainty/160983/). 05.11.2020).***

***

«Кампания недавно обнаруженного троянского вредоносного ПО нацелена на предприятия и высшее образование, что, как представляется, является попыткой украсть имена пользователей, пароли и другую личную информацию, а также создать постоянный бэкдор для скомпрометированных систем.

Инфостилер Jupyter был подробно описан компанией по кибербезопасности Morphisec, которая обнаружила его в сети неназванного высшего учебного заведения в США. Считается, что троян активен с мая этого года.

Атака в первую очередь нацелена на данные браузера Chromium, Firefox и Chrome, но также имеет дополнительные возможности для открытия бэкдора на скомпрометированных системах, позволяя злоумышленникам выполнять сценарии и команды PowerShell, а также возможность загружать и выполнять дополнительные вредоносные программы.

SEE: выигрышная стратегия кибербезопасности (специальный отчет ZDNet) | Скачать отчет в формате PDF (TechRepublic)

Установщик Jupyter замаскирован в виде заархивированного файла, часто с использованием значков Microsoft Word и имен файлов, которые выглядят так, как будто их нужно срочно открыть, связанных с важными документами, данными о поездках или повышением заработной платы.

Если программа установки запущена, она установит легальные инструменты, чтобы скрыть реальную цель установки - загрузку и запуск вредоносной программы установки во временные папки в фоновом режиме.

После полной установки в системе Jupyter крадет информацию, включая имена пользователей, пароли, автозаполнение, историю просмотров и файлы cookie, и отправляет их на сервер управления и контроля. Анализ вредоносного ПО показал, что тот, кто его создал, постоянно изменяет код, чтобы собирать больше информации, а также усложняет обнаружение жертв.

Неясно, каков точный мотив кражи информации, но киберпреступники могут использовать ее для получения дополнительного доступа к сетям для дальнейших атак - и потенциально кражи очень конфиденциальных данных - или они могут продавать учетные данные для входа и черный доступ к системам для другие преступники, которые имеют доступ.

Исследователи считают, что Jupyter происходит из России. Анализ вредоносного ПО не только показал, что он связан с управляющими серверами в России, но и обратный поиск изображения планеты Юпитер в админ-панели инфостилера показал, что оригинал взят с русскоязычного форума. На этом изображении также написано Jupyter, вероятно, неправильное написание названия планеты с русского на английский.

Хотя многие командные серверы сейчас неактивны, панель администратора все еще работает, что говорит о том, что кампании Jupyter, возможно, еще не завершены». ***(Danny Palmer. Jupyter trojan: Newly discovered malware stealthily steals usernames and passwords // ZDNet (https://www.zdnet.com/article/jupyter-trojan-newly-discovered-trojan-malware-stealthily-steals-usernames-and-passwords/). 16.11.2020).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«В четверг румынские полицейские арестовали двух человек, подозреваемых в использовании трех онлайн-сервисов, предназначенных для помощи в разработке и распространении вредоносных программ.

Аресты являются частью совместной операции, в которой участвовали ФБР, Европол, австралийская и норвежская полиция.

Следователи заявили, что двое румынских подозреваемых считаются создателями трех сервисов под названием CyberSeal, DataProtector и CyberScan.

Первые два - это так называемые «криптографические» сервисы. Эти типы инструментов позволяют разработчикам вредоносных программ шифровать код своих вредоносных программ, чтобы обойти антивирусное программное обеспечение и избежать его.

Третий сервис, названный CyberScan, работал как клон сервиса Google VirusTotal. Это позволило авторам вредоносных программ загружать и сканировать свои новые выпуски вредоносных программ и проверять, будут ли они обнаружены антивирусным ПО.

Разница между CyberScan и VirusTotal заключалась в том, что CyberScan не делился результатами сканирования с поставщиками антивирусных программ, что позволяло авторам вредоносных программ проверять обнаруживаемость своих полезных нагрузок, не опасаясь, что «предупреждение об обнаружении» будет отправлено обратно в антивирусную компанию и вызовет расследование.

Два подозреваемых были активны в области распространения вредоносных программ по крайней мере с 2014 года, когда они впервые начали рекламировать CyberSeal. Два других сервиса были запущены в 2015 году (DataProtector) и 2019 году (CyberScan).

Все три были рекламированы на нескольких хакерских форумах по цене от 40 до 150 долларов.

Европол сообщил, что эти три инструмента часто использовались для шифрования и тестирования различных типов вредоносных программ, таких как RAT (трояны удаленного доступа), кражи информации и программы-вымогатели.

Более 1560 авторов вредоносных программ использовали две службы шифрования для шифрования кода более 3000 разновидностей вредоносных программ.

Власти расправились с бандой вчера, в четверг, 19 ноября, когда они обыскали четыре места в городах Бухарест и Крайова на юге Румынии и произвели два ареста.

По данным Управления по расследованию организованной преступности и терроризма Румынии (DIICOT), были также допрошены два других человека, которые предположительно входили в группу.

Следователи также отключили серверы в Румынии, Норвегии и США. Домены cyber-seal.org и cyberscan.org, используемые для размещения двух сервисов, теперь отключены». ***(Catalin Cimpanu. Two Romanians arrested for running three malware services // ZDNet (https://www.zdnet.com/article/two-romanians-arrested-for-running-multiple-malware-services/). 20.11.2020).***

***

Технічні аспекти кібербезпеки

«Исследователи обозначили слабые места безопасности в Tesla Backup Gateway и способы их использования.

Во вторник Rapid7 описал риски безопасности, связанные с подключением Tesla Backup Gateway к Интернету; в частности, способы использования открытых подключений для нарушения конфиденциальности и безопасности пользователей.

Tesla Backup Gateway (.PDF) - это платформа, разработанная автопроизводителем для управления солнечными батареями и установками Powerwall. Система может напрямую подключаться к сети, отслеживать отключения и дает пользователям возможность отслеживать и контролировать запасы энергии через подключенное мобильное приложение. Соединения могут быть установлены через Wi-Fi, кабель Ethernet или мобильный телефон.

Чтобы получить доступ к шлюзу, пользователи подключаются к сети Wi-Fi программного обеспечения, вводят его серийный номер, который действует как пароль, и получают доступ к Tesla Backup Gateway из интернет-браузера. Каждый шлюз использует самоподписанный сертификат SSL.

При первом входе пользователя в систему используются его адрес электронной почты и пароль - последние пять цифр пароля шлюза.

Согласно Rapid7 и прошлому исследованию, проведенному Винсом Лоскьяво, такая практика связана с риском использования слабых учетных данных.

В худшем случае, пять цифр для первого входа в систему приводят к 60,4 миллионам комбинаций паролей, и команда говорит, что, похоже, нет ограничений, чтобы остановить попытки перебора. Однако есть способы обойти проблему опробования миллионов комбинаций, поскольку простой проездной для записи точки доступа Wi-Fi может уменьшить этот объем.

SSID точки доступа использует последние три символа серийного номера, оставив только два символа для предположения.

Rapid7 также отмечает, что многие округа публикуют в Интернете разрешения на установку бытовых систем Tesla Solar и Powerwall, что дает злоумышленникам направление к потенциальным целям.

Когда шлюз подключен к локальной сети, его имя хоста транслируется с использованием полного серийного номера.

Также было обнаружено, открыто и доступно в Интернете несколько установок Tesla Backup Gateway. С января исследователи задокументировали 379 открытых установок в США и Европе, некоторые из которых представляют собой коммерческие блоки питания Tesla.

Платформа включает в себя API-интерфейсы, документирующие использование энергии, рисование и некоторую информацию о владельце, но есть также скрытые API-интерфейсы, которые можно использовать для дополнительной статистики.

«Теоретически напряжение, цикл и другие параметры энергии, которыми управляет Backup Gateway, и подключенные к нему батареи можно настраивать», - говорит Rapid7. «Если эти настройки могут быть изменены, возможно повреждение аккумулятора или даже электросети. Хотя размещение Tesla Backup Gateway или Tesla Powerpack в Интернете может показаться заманчивым, мы должны помнить, что Интернет шумный по своей природе, когда большое количество нежелательного трафика регулярно проходит через различные порты ".

Rapid7 связалась с Tesla перед публикацией, и компания заявила, что предстоящие обновления безопасности будут включать усиление и устранение упомянутых проблем.

Кроме того, по словам Теслы, «предсказуемые пароли установщика были зафиксированы в течение некоторого времени на недавно введенных в эксплуатацию устройствах Backup Gateway V1, но некоторые ранее введенные в эксплуатацию устройства все еще имели их, и все онлайн-устройства Backup Gateway V1 имели свои пароли установщика случайным образом». Устройства Backup Gateway V2 теперь также поставляются со случайными паролями…» ***(Charlie Osborne. Researchers warn of internet security risks connected to Tesla Backup Gateway // ZDNet (https://www.zdnet.com/article/researchers-warn-of-internet-security-risks-connected-to-tesla-backup-gateway/). 17.11.2020).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«У Windows виявили критичну вразливість, яку використовують для злому комп'ютерів. Про це повідомляється на сайті Google Project Zero.

Фахівці заявили, що баг відноситься до вразливості нульового дня (zero day), тобто до шкідливих систем, проти яких ще не розроблені захисні механізми. За допомогою бага хакери можуть підвищити привілеї певних процесів в системі для її злому. Експерти розповіли, що злом відбувається через взаємодію з функцією Windows Kernel Cryptography Driver (cng.sys), через що відбувається переповнення буфера.

У дослідженні Google Project Zero йдеться, що нова уразливість використовується разом з уразливістю CVE-2020-15999 в браузері Chrome, яку фахівці виявили кілька днів тому. За допомогою системного пролому хакерам вдається запускати шкідливий код всередині браузера.

Експерти Google підсумували, що знайдена уразливість нульового дня вже використовується зловмисниками. Злом з її допомогою було організовано на останній версії Windows 10, проте експлойт вдалося запустити і на більш старих версіях ОС, зокрема, Windows 7…». ***(Лужна Софія. У Windows знайшли критичну уразливість // TechnoPortal.com.ua (https://technoportal.com.ua/noviny/52942). 02.11.2020).***

***

«NVIDIA выпустила обновление безопасности для приложения для облачных игр GeForce Now для Windows, чтобы устранить уязвимость, которая может позволить злоумышленникам выполнить произвольный код или повысить привилегии в системах, на которых запущено неустановленное программное обеспечение.

GeForce Now - это облачный сервис потоковой передачи игр, который позволяет пользователям из более чем 80 стран с платной подпиской транслировать бесплатные игры или игры, которыми они владеют, в режиме реального времени из библиотеки из сотен наименований, размещенных на серверах NVIDIA.

Облачный игровой сервис NVIDIA может использоваться клиентами, которые владеют NVIDIA Shield, настольными (macOS, Microsoft Windows и ChromeOS) или мобильными (Android) устройствами через специальные приложения.

В приложении для Windows исправлена ошибка высокой степени серьезности

Сегодня NVIDIA устранила уязвимость с высокой степенью серьезности (CVE - 2020-5992) во всех версиях приложения Windows GeForce Now до 2.0.25.119, чтобы локальные злоумышленники не могли повысить свои привилегии или выполнить код после успешной эксплуатации.

Об уязвимости сообщил Hou JingYi из Qihoo 360 CERT, и она была обнаружена в библиотеке OpenSSL, одной из зависимостей программного обеспечения GeForce Now с открытым исходным кодом.

Хотя эта уязвимость требует от злоумышленников доступа локального пользователя и, следовательно, ее нельзя использовать удаленно, ею все же можно злоупотреблять с помощью вредоносных инструментов, развернутых в системах с уязвимыми версиями приложений, как объясняет NVIDIA в опубликованном сегодня рекомендации по безопасности…

Атаки, использующие эту ошибку, имеют низкую сложность и требуют низких привилегий, обеспечивающих базовые возможности пользователя.

К счастью, любые атаки, направленные на злоупотребление уязвимостью CVE - 2020-5992, также требуют взаимодействия с пользователем для успешной эксплуатации.

NVIDIA заявляет, что «оценка риска основана на среднем риске для разнообразного набора установленных систем и может не отражать истинный риск вашей локальной установки».

Компания также рекомендует «проконсультироваться со специалистом по безопасности или ИТ-специалистом для оценки риска для вашей конкретной конфигурации».

Применение обновления безопасности GeForce Now

Чтобы применить обновление для системы безопасности и защитить вашу систему, вам необходимо открыть приложение Windows GeForce Now, чтобы оно было загружено автоматически, а затем следуйте инструкциям по его установке (приложение требует прав администратора для обновления).

Если вы не можете запустить приложение от имени администратора, вы также можете обновить его вручную, удалив, используя эти инструкции, а затем установив последнюю версию программного обеспечения (например, 2.0.25.119)…». ***(Sergiu Gatlan. NVIDIA fixes severe flaw in GeForce NOW cloud gaming service // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/nvidia-fixes-severe-flaw-in-geforce-now-cloud-gaming-service/). 11.11.2020).***

***

«На выходных Oracle выпустила обновление для системы безопасности по дополнительному каналу, чтобы устранить критическую уязвимость удаленного выполнения кода (RCE), затрагивающую несколько версий Oracle WebLogic Server.

Уязвимость системы безопасности, отслеживаемая как CVE-2020-14750, получила базовую оценку серьезности 9,8 от Oracle из максимальной оценки 10.

Oracle благодарит 20 организаций и людей в рекомендациях по безопасности за предоставление информации, которая позволила компании обратиться к CVE-2020-14750.

Без авторизации RCE

Злоумышленники, не прошедшие проверку подлинности, могут удаленно использовать этот недостаток RCE без аутентификации в компоненте консоли сервера через HTTP, без взаимодействия с пользователем, как часть атак низкой сложности для потенциального захвата целевых серверов.

«Его можно использовать удаленно без аутентификации, т. е. его можно использовать по сети без необходимости вводить имя пользователя и пароль», - поясняется в сообщении Oracle.

«Из-за серьезности этой уязвимости и публикации кода эксплойта на различных сайтах Oracle настоятельно рекомендует клиентам как можно скорее применить обновления, предоставленные этим предупреждением безопасности».

Поддерживаемые версии Oracle WebLogic Server, на которые влияет CVE-2020-14750, включают 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 и 14.1.1.0.0.

Эрик Морис, директор по обеспечению безопасности в Oracle, также поделился ссылкой на инструкции по усилению защиты WebLogic Server в сообщении в блоге, опубликованном в воскресенье, с объявлением о внешнем обновлении безопасности.

Ранее сегодня Агентство по кибербезопасности и безопасности инфраструктуры (CISA) также призвало пользователей и администраторов применить обновление безопасности для блокировки потенциальных атак.

Относится к активно нацеленной на CVE-2020-14882

Oracle также сообщает, что уязвимость связана с CVE-2020-14882, еще одной критической ошибкой WebLogic Server, 9,8 из 10, которая была устранена в обновлении Critical Patch за октябрь 2020 года две недели назад.

Как сообщил BleepingComputer в четверг, злоумышленники начали сканирование уязвимых и уязвимых экземпляров Oracle WebLogic на предмет эксплойтов CVE-2020-14882 через неделю после того, как это было во время критического обновления исправлений в этом месяце, согласно данным SANS Technology Institute.

Несмотря на то, что компания не предоставила никаких дополнительных сведений о связи между двумя уязвимостями, это внеполосное обновление безопасности может быть прямым результатом того, что в пятницу был обнаружен обход исправления CVE-2020-14882.

BleepingComputer связался с Oracle для получения дополнительных сведений и подтверждения того, что CVE-2020-14750 действительно был выпущен для

обхода обхода CVE-2020-14882 на прошлой неделе, но на момент публикации не получил ответа». ***(Sergiu Gatlan. Oracle issues emergency patch for critical WebLogic Server flaw // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/oracle-issues-emergency-patch-for-critical-weblogic-server-flaw/). 02.11.2020).***

***

«Unity Orchestrator от Silver Peak, программно определяемая платформа управления WAN (SD-WAN), страдает от трех ошибок безопасности удаленного выполнения кода, которые могут быть объединены в цепочку, чтобы позволить захват сети неаутентифицированными злоумышленниками.

SD-WAN - это облачный сетевой подход, используемый предприятиями и многопрофильными предприятиями любого размера. Он позволяет подключать местоположения и облачные экземпляры друг к другу и к ресурсам компании через любой тип подключения. И он применяет программный контроль к управлению этим процессом, включая оркестровку ресурсов и узлов. Эта оркестровка обычно централизована через платформу единого представления - в данном случае Unity Orchestrator, который, по словам Silver Peak, имеет около 2000 развертываний.

По словам исследователей из Realmode Labs, тремя ошибками являются обход аутентификации, обход пути удаления файла и выполнение произвольного SQL-запроса, которые можно комбинировать для выполнения произвольного кода.

Фирма отметила, что злоумышленники сначала будут обходить аутентификацию, чтобы войти на платформу, а затем искать файл, запускаемый веб-сервером. Затем они могут удалить его, используя проблему обхода пути удаления файла, заменив его одним по своему выбору с помощью выполнения SQL-запроса. Тогда все, что нужно, - это запустить файл, чтобы запустить любой код или вредоносную программу, которая им нужна.

«В лучшем случае злоумышленник может использовать эти уязвимости для перехвата или направления трафика», - сказал Ариэль Темпельхоф, соучредитель и генеральный директор Realmode, в своем посте на Medium на этой неделе. «Однако при желании злоумышленник может вместо этого отключить всю международную сеть компании».

Детали ошибки

Проблемы присутствуют в версиях Silver Peak Unity Orchestrator до 8.9.11+, 8.10.11+ или 9.0.1+. По словам Сильвер Пик, это затрагивает экземпляры Orchestrator, которые размещаются у клиентов - локально или у поставщика общедоступного облака. Доступны патчи.

Что касается технических особенностей, обход аутентификации (CVE-2020–12145) существует в способе обработки Unity вызовов API.

«[Затронутые платформы используют] заголовки HTTP для аутентификации вызовов REST API с localhost», - говорится в рекомендациях Silver Peak по безопасности. «Это позволяет войти в Orchestrator, введя заголовок HTTP HOST, установленный на 127.0.0.1 или localhost.

По сути, это означает, что, по словам Темпельхофа, значимая аутентификация не выполняется, когда вызовы исходят от localhost.

«Проверка localhost выполняется [примерно так]: request.getBaseUri (). GetHost (). Equals (« localhost »)», - пояснил он. «Любые запросы с« localhost »в качестве заголовка HTTP-хоста удовлетворяют этой проверке. Конечно, это можно легко подделать в удаленных запросах ».

Проблема с обходом пути (CVE-2020–12146) тем временем существует, потому что при удалении локально размещенного файла проверка обхода пути не выполняется.

«Авторизованный пользователь может получать доступ, изменять и удалять файлы с ограниченным доступом на сервере Orchestrator с помощью REST API / debugFiles», - говорит Silver Peak.

Темпельхоф пояснил: «Некоторые конечные точки API, которые теперь доступны благодаря обходу аутентификации, позволяют выгружать журналы отладки в корзину S3 для проверки Silver Peak. Этот механизм подготавливает журналы, загружает их, а затем удаляет локально размещенный файл. Конечная точка / gms / rest / debugFiles / delete, выполняющая удаление, не проверяет обход пути, создавая возможность удалить любой файл в системе (если позволяют разрешения)».

И последняя проблема, ошибка выполнения SQL-запроса (CVE-2020–12147), позволяет аутентифицированному пользователю делать несанкционированные запросы MySQL к базе данных Orchestrator, используя / sqlExecution REST API, согласно Silver Peak. Эти произвольные запросы SQL возможны благодаря специальной конечной точке API, которая использовалась для внутреннего тестирования.

«Конечная точка / gms / rest / sqlExecution может быть использована для произвольной записи файла с помощью предложения INTO DUMPFILE», - пояснил Темпельхоф, добавив, что, хотя INTO DUMPFILE не позволяет перезаписывать файл напрямую, злоумышленники могут использовать ошибку обхода пути для сначала удалите файл, а затем перепишите его.

Realmode сообщила об уязвимостях 9 августа, а Silver Peak выпустила исправления 30 октября. Оценки серьезности CVSS еще не присвоены.

Темпельхоф сказал, что его команда обнаружила аналогичные недостатки в трех других компаниях SD-WAN (все в настоящее время исправлены), которые будут вскоре раскрыты.

«Мы исследовали четыре основных продукта SD-WAN на рынке и обнаружили серьезные уязвимости удаленного выполнения кода», - написал он. «Для использования уязвимостей не требуется никакой аутентификации».

У ведущих поставщиков SD-WAN были проблемы в прошлом. Например, в марте Cisco Systems устранила три уязвимости высокой степени серьезности, которые могли позволить локальным злоумышленникам, прошедшим проверку подлинности, выполнять команды с привилегиями root. Похожая ошибка была обнаружена месяцем позже в Cisco IOS XE, версии межсетевой операционной системы Cisco (IOS) на базе Linux, используемой в развертываниях SD-WAN.

А в декабре прошлого года критическая ошибка нулевого дня была обнаружена в различных версиях продуктов Citrix Application Delivery Controller (ADC) и Citrix Gateway, которые позволяли перехват устройств и RCE,

используемые в реализациях SD-WAN. После того, как об этом было объявлено, количество атак и публичных эксплойтов быстро накапливалось». ***(Tara Seals. Silver Peak SD-WAN Bugs Allow for Network Takeover // Threatpost (https://threatpost.com/silver-peak-sd-wan-bugs-network-takeover/161142/). 11.11.2020).***

***

«Спустя полтора года после того, как Microsoft раскрыла уязвимость BlueKeep, влияющую на службу Windows RDP, более 245000 систем Windows по-прежнему не исправлены и уязвимы для атак.

Это число составляет около 25% из 950 000 систем, которые были первоначально обнаружены уязвимыми для атак BlueKeep во время первого сканирования в мае 2019 года.

Точно так же более 103000 систем Windows также остаются уязвимыми для SMBGhost, уязвимости в протоколе Server Message Block v3 (SMB), который поставляется с последними версиями Windows, раскрытым в марте 2020 года.

Обе уязвимости позволяют злоумышленникам удаленно управлять системами Windows и считаются одними из самых серьезных ошибок, обнаруженных в Windows за последние несколько лет.

Однако, несмотря на их серьезность, многие системы так и не получили исправлений, согласно исследованию, проведенному за последние несколько недель обработчиком SANS ISC Яном Копривой [1, 2].

Коприва говорит, что BlueKeep и SMBGhost - не единственные крупные уязвимости, которые можно использовать удаленно, которые в наши дни широко распространены в сети, подвергая системы атакам.

По словам чешского исследователя безопасности, до сих пор существуют миллионы доступных из Интернета систем, которые администраторам не удалось исправить и которые уязвимы для удаленного захвата. К ним относятся такие системы, как серверы IIS, почтовые агенты Exim, клиенты OpenSSL и сайты WordPress…

Причины, по которым эти системы остались без исправлений, остаются неизвестными, но даже недавние предупреждения правительственных агентств кибербезопасности США не помогли.

Это включает в себя два предупреждения Агентства национальной безопасности США (АНБ), одно из которых было выпущено в мае (для ошибки Exim CVE-2019-10149, использованной российскими государственными хакерами), а второе - в октябре (для ошибки BlueKeep, которая была использована китайскими государственными хакерами).

Тем не менее, несмотря на эти предупреждения, более 268 000 серверов Exim все еще не исправлены для ошибки Exim и более 245 000 не исправлены для BlueKeep.

Коприва говорит, что цифры показывают, что «даже очень известные уязвимости иногда остаются не исправленными в течение многих лет».

«Учитывая, насколько опасен и хорошо известен BlueKeep, скорее всего, возникает вопрос, сколько других, менее известных критических уязвимостей все

еще не исправлено на аналогичном количестве систем», - добавляет Коприва». ***(Catalin Cimpanu. More than 245,000 Windows systems still remain vulnerable to BlueKeep RDP bug // ZDNet (https://www.zdnet.com/article/more-than-245000-windows-systems-still-remain-vulnerable-to-bluekeep-rdp-bug/). 17.11.2020).***

***

«VMware выпустила обновления безопасности для исправления критических уязвимостей высокой степени серьезности в VMware ESXi, Workstation, Fusion и Cloud Foundation, что позволяет выполнять код и повышать привилегии.

Сяо Вэй и Тяньвен Тан из Qihoo 360 Vulcan Team успешно воспользовались этими двумя уязвимостями в первый день конкурса Pwn Contest 2020 Tianfu Cup.

Прикован к эскалации привилегий

Одна из ошибок безопасности с рейтингом критической серьезности, отслеживаемая как CVE-2020-4004, позволяет злоумышленникам с локальными административными привилегиями на виртуальной машине злоупотреблять уязвимостью использования после освобождения в USB-контроллере XHCI для VMware ESXi, Workstation, и Fusion.

Успешная эксплуатация позволяет выполнять код как процесс VMX виртуальной машины, запущенный на узле, процесс, используемый для настройки и размещения экземпляров виртуальных машин.

Вторая уязвимость, обозначенная как CVE-2020-4005 и оцененная как высокая степень серьезности, позволяет злоумышленникам злоупотреблять высокозащищенной ошибкой повышения привилегий VMware ESXi в способе управления системными вызовами для повышения привилегий.

«Злоумышленник с привилегиями только в рамках процесса VMX может повысить свои привилегии в уязвимой системе», - заявляет VMware.

Однако для успешной эксплуатации CVE-2020-4005 требуется изменить ошибку в USB-контроллере XHCI с использованием ошибки после освобождения.

Обходной путь для блокировки цепочки эксплойтов

VMware выпустила обновления безопасности для CVE-2020-4004, но также предлагает обходной путь, который включает удаление контроллера XHCI (USB 3.x) с потенциально целевых виртуальных машин, если они не используются.

VMware также выпустила обновления безопасности для защиты от CVE-2020-4005 во всех уязвимых версиях VMware ESXi.

Компания все еще работает над выпуском фиксированных версий ESXi для VMware Cloud Foundation в ближайшие дни.

Два дня назад VMware также устранила несколько уязвимостей средней и высокой степени серьезности в облачной и многопользовательской службе управления SD-WAN Orchestrator, которая могла привести к выполнению кода, несанкционированному доступу к данным, атакам с использованием метода Pass-the-Hash и повышению привилегий». ***(Sergiu Gatlan. VMWare releases fix for critical ESXi, Workstation vulnerability // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/vmware-releases-fix-for-critical-esxi-workstation-vulnerability/). 20.11.2020).***

***

«Сегодня Cisco устранила три уязвимости безопасности Webex Meetings, которые позволили бы удаленным злоумышленникам, не прошедшим проверку подлинности, присоединиться к текущим совещаниям в качестве призрачных участников.

Cisco Webex - это программное обеспечение для онлайн-встреч и видеоконференций, которое можно использовать для планирования совещаний и присоединения к ним. Он также предоставляет пользователям возможности презентации, совместного использования экрана и записи.

Платформа удаленных встреч Cisco за четыре месяца увеличилась на 451% из-за текущей пандемии COVID-19, при этом на пике популярности за один день проводится около 4 миллионов встреч для 324 миллионов пользователей.

Злоумышленники-призраки на вашей встрече Webex

Злоумышленники, злоупотребляющие исправленными недостатками, могут стать «призрачными» пользователями, способными присоединиться к собранию, не будучи обнаруженными, как обнаружили исследователи IBM, анализируя инструмент совместной работы Cisco на предмет уязвимостей.

«Призрачные» пользователи - это участники встречи, которых нельзя увидеть в списке пользователей и которые не были приглашены на встречу, но они могут слышать, говорить и обмениваться медиафайлами внутри собрания.

Эти три ошибки также позволили злоумышленникам оставаться на совещании Webex и поддерживать двунаправленное аудиосоединение даже после того, как администраторы удаляли их и получали доступ к информации пользователей Webex, такой как адреса электронной почты и IP-адреса, из вестибюля конференц-зала.

Уязвимости существуют в Cisco Webex Meetings и Cisco Webex Meetings Server, и они «работают, используя процесс подтверждения связи, который Webex использует для установления соединения между участниками собрания».

Исследователи IBM заявили, что в случае успешного использования злоумышленников злоумышленники могут:

Присоединяйтесь к совещанию Webex как призрак, чтобы вас не видели в списке участников, с полным доступом к функциям аудио, видео, чата и совместного использования экрана (CVE-2020-3419)

Оставаться на совещании Webex как призрак после исключения из него, сохраняя аудиосвязь (CVE-2020-3471)

Получите доступ к информации о посетителях встречи, включая полные имена, адреса электронной почты и IP-адреса, из вестибюля конференц-зала, даже если вас не допустили к звонку (CVE-2020-3441)

Доступны обновления безопасности

Исследователям удалось успешно продемонстрировать атаки с использованием этих ошибок Webex в Windows, macOS и версии приложений Webex Meetings для iOS и устройстве Webex Room Kit.

Cisco устранила уязвимости, установив исправления на облачных сайтах Cisco Webex Meetings и выпустив обновления безопасности для локального

программного обеспечения, такого как мобильное приложение Cisco Webex Meetings и программное обеспечение Cisco Webex Meetings Server.

Пользователям рекомендуется немедленно обновить Webex до последней версии, чтобы защитить собрания от злоумышленников, которые попытаются использовать их и присоединиться в качестве пользователей-призраков.

Исследовательская группа IBM также подготовила видео-демонстрацию с подробностями об уязвимостях и советами о том, что Webex Meetings может сделать, чтобы защитить себя от атак.

Cisco также устранила несколько критических уязвимостей в своих продуктах Cisco IoT Field Network Director (CVE-2020-3531), Cisco DNA Spaces Connector (CVE-2020-3586), Cisco Integrated Management Controller (CVE-2020-3470).

После успешной эксплуатации неаутентифицированные удаленные злоумышленники могут выполнять произвольные команды (в некоторых случаях с привилегиями root) и получать доступ к внутренней базе данных скомпрометированных систем». ***(Sergiu Gatlan. Cisco fixes WebEx bugs allowing 'ghost' attackers in meetings // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/cisco-fixes-webex-bugs-allowing-ghost-attackers-in-meetings/). 18.11.2020).***

***

«В мессенджере исправили баг, который позволял хакерам присоединяться к звонкам без ведома или одобрения пользователя.

Наталья Сильванович, исследовательница команды безопасности Google Project Zero, обнаружила уязвимость в процессе аудита безопасности. Баг шпионил за пользователями платформы Android.

Согласно докладу Сильванович, баг находился в протоколе WebRTC, который использовался для поддержки аудио- и видеозвонков.

Более того, Сильванович уточнила в своем докладе, что уязвимость обнаружили в SDP (Session Description Protocol), составной части WebRTC. SDP содержит данные сессий для соединений WebRTC. Сильванович обнаружила, что сообщения SDP могут быть использованы для автоматического подтверждения соединений WebRTC без вмешательства пользователя.

Исследовательница Google доложила об инциденте в прошлом месяце, а на днях Facebook исправил сбой, выпустив новую версию для Android». ***(Баг в мессенджере Facebook мог позволить хакерам шпионить за пользователями // SecureNews (https://securenews.ru/a-bug-in-the-facebook-messenger-could-allow-hackers-to-spy-on-users/). 20.11.2020).***

***

«Уязвимая версия приложения, у которой 100 миллионов пользователей, использует легко предсказуемые URL-адреса для ссылки на частный контент.

По мнению исследователей, уязвимость в системе безопасности, обнаруженная в приложении GO SMS Pro для Android, может быть использована для публичного раскрытия медиафайлов, отправленных с помощью приложения.

Приложение GO SMS Pro - популярное приложение для обмена сообщениями, которое скачали более 100 миллионов раз из магазина Google Play. Исследователи из Trustwave SpiderLabs заявили, что личные голосовые сообщения, видеосообщения и фотографии могут быть скомпрометированы из-за уязвимости в версии 7.91, которую можно легко использовать.

Когда пользователь отправляет мультимедийное сообщение, получатель может получить его, даже если у него нет установленного GO SMS Pro. В этом случае медиафайл отправляется получателю в виде URL-адреса через SMS, поэтому человек может щелкнуть ссылку, чтобы просмотреть медиафайл в окне браузера.

«SpiderLabs обнаружила, что доступ к ссылке возможен без какой-либо аутентификации или авторизации, что означает, что любой пользователь, имеющий ссылку, может просматривать контент», - пояснили исследователи в публикации в четверг.

Само по себе это может быть использовано с помощью вредоносного ПО для анализа SMS или браузера для кражи информации. Но исследователи также обнаружили, что URL-адреса, используемые для медиа, являются последовательными и предсказуемыми.

Таким образом, предсказывая следующий URL-адрес в шестнадцатеричной последовательности, злоумышленник может просматривать любое количество медиафайлов пользователей без согласия.

«[Они могут] потенциально получить доступ к любым медиафайлам, отправленным через эту службу, а также к любым, которые будут отправлены в будущем», - отметили исследователи. «Увеличивая значение в URL-адресе, можно просматривать или слушать другие мультимедийные сообщения, которыми обмениваются другие пользователи».

С помощью простого сценария bash можно сгенерировать примерный список URL-адресов, используя предсказуемые изменения в добавленных адресах, которые можно просто вставить в расширение с несколькими вкладками в Chrome или Firefox для удобного просмотра.

Изящество экономии состоит в том, что злоумышленник не сможет связать носитель с конкретным пользователем, если только сам медиафайл не утекнет личность человека.

«Например, изображение профиля можно искать с помощью обратного поиска изображений, изображение водительского удостоверения или юридические документы будут содержать личную информацию (PII), которая может быть использована для привязки изображения к конкретным людям и т. Д.», - Карл Сиглер, Старший менеджер по исследованиям в области безопасности в SpiderLabs сообщил Threatpost. «Однако случайное изображение заката, скорее всего, нелегко связать с человеком».

Тем не менее, это серьезная ошибка, добавил Сиглер. Он сказал, что, поскольку злоумышленник не может напрямую нацеливаться на конкретных пользователей, «я бы не стал считать это критической степенью серьезности... но широкая сеть, которая может быть брошена вокруг потенциально конфиденциальных данных, безусловно, оправдывает высокую серьезность».

Эта слабость была подтверждена в GO SMS Pro v7.91, как уже упоминалось, но разработчик выпустил новую версию (v.7.93) в среду. Исследователи заявили, что SpiderLabs еще не тестировал эту новую версию приложения (но Сиглер сказал, что планирует это сделать), и разработчик никогда не признавал ошибку, несмотря на многочисленные попытки связаться с ней, начиная с середины августа.

По словам Сиглера, исправление будет включать добавление надлежащих элементов управления доступом в экземпляр облака, внедрение более длинных уникальных идентификаторов в URL-адрес, которые предотвратят последовательный просмотр данных, или просто полное отключение экземпляра облака до тех пор, пока проблема не будет решена.

Пользователи должны обновиться до последней версии, если она устраняет ошибку, но для обеспечения конфиденциальности содержимого «настоятельно рекомендуется избегать отправки мультимедийных файлов через приложение, которое, как вы ожидаете, останется конфиденциальным или которое может содержать конфиденциальные данные, используя этот популярный мессенджера, по крайней мере, до тех пор, пока поставщик не признает эту уязвимость и не устранит ее», - говорится в сообщении SpiderLabs.

Threatpost обратился к разработчику за дополнительной информацией о том, решает ли новая версия проблему - все почтовые ящики были заполнены.

«Это не должно быть обычным явлением, но неопытные разработчики могут легко упустить что-то подобное», - сказал Сиглер. «Вот почему важно добавлять тестирование безопасности в любой жизненный цикл разработки приложений». ***(Tara Seals. GO SMS Pro Android App Exposes Private Photos, Videos and Messages // Threatpost (https://threatpost.com/go-sms-pro-android-app-exposes-private-photos/161407/). 19.11.2020).***

***

«Каждый из четырех поставщиков промышленных систем управления объявил об уязвимостях от критических до особо серьезных.

Во вторник компании, производящие системы управления производством, Real Time Automation и Paradox предупредили о критических уязвимостях, которые открывают системы для удаленных атак злоумышленников.

Согласно отраслевому стандарту Common Vulnerability Scoring System, уязвимости получают оценку 9,8 из 10 по серьезности. Ошибка Real Time Automation восходит к уязвимости компонента, опубликованной Claroty.

«Уязвимость переполнения стека была обнаружена в стеке RTA 499ES ENIP, всех версиях до 2.28, одном из наиболее широко используемых протоколов OT», - написал Claroty, который во вторник публично раскрыл ошибку. Сторонний код, используемый в проприетарном компоненте автоматизации в реальном времени (RTA), 499ES EtherNet / IP (ENIP), может запускаться для создания условий для атаки типа «отказ в обслуживании».

Исследователи Claroty заявили, что они идентифицировали 11 устройств, использующих стек RTA ENIP от шести различных поставщиков, которые могут быть уязвимы для атак. Этих других поставщиков он не идентифицировал. Шарон

Бризинов из Claroty, отслеживаемый как CVE-2020-25159, сообщил об этой уязвимости в CISA в прошлом месяце.

Компания RTA, которая позиционирует себя как поставщик промышленных систем управления для автоматизации производства и зданий, опубликовала информацию об уязвимости 27 октября.

Джон Ринальди, главный стратег, менеджер по развитию бизнеса и генеральный директор RTA, сказал в октябре, что «старый код в устройстве RTA пытался уменьшить использование оперативной памяти, ограничивая размер конкретного буфера, используемого в запросе прямого открытия EtherNet / IP. Ограничивая оперативную память, злоумышленник мог попытаться переполнить буфер и использовать его, чтобы попытаться получить контроль над устройством. Эта строка кода была изменена несколько уровней назад и не является проблемой для текущих версий программного обеспечения EtherNet / IP ».

Система безопасности ICS Paradox

Производитель устройств безопасности Paradox также объявил о критической ошибке (CVE-2020-25189), влияющей на его интернет-модуль IP150, которая создала условия для атаки на переполнение буфера на основе стека.

«Успешное использование этих уязвимостей может позволить злоумышленнику удаленно выполнить произвольный код, что может привести к прекращению работы системы физической безопасности», - написало агентство Cybersecurity Infrastructure Security Agency (CISA) в бюллетене, опубликованном во вторник.

Согласно Paradox, затронутый интернет-модуль IP150 представляет собой «коммуникационный модуль на базе локальной сети, который позволяет вам контролировать и контролировать вашу систему безопасности Paradox через локальную сеть или Интернет через любой веб-браузер».

Вторая ошибка высокой степени серьезности, отслеживаемая как CVE-2020-25185 с рейтингом CVSS 8,8, открывает Интернет-модуль IP150 для «пяти переполнений буфера после аутентификации, что может позволить зарегистрированному пользователю удаленно выполнить произвольный код».

Хотя Paradox указал на отсутствие известных общедоступных эксплойтов, нацеленных на эти уязвимости, компания также не предложила никаких конкретных исправлений для каждой ошибки.

Запросы в Paradox не возвращались.

Вместо исправлений Paradox предложил ряд рекомендаций по снижению риска, включая обеспечение соблюдения принципа минимальных привилегий и «минимизацию воздействия сети на все устройства и / или системы системы управления, а также обеспечение того, чтобы они были недоступны из Интернета».

Напряженный день для исправлений ICS

Помимо ошибок RTA и Paradox, серьезные недостатки были обнародованы Sensormatic Electronics, дочерней компанией Johnson Controls, и гигантом ICS Schneider Electric.

Schneider сообщил о девяти серьезных ошибках в своей интерактивной графической системе SCADA. К уязвимостям относятся: неправильное

ограничение операций в пределах буфера памяти, запись за пределами границ и ошибки чтения за пределами.

Ошибка Sensormatic (CVE-2020-9049) влияет на оборудование: веб-клиент American Dynamics victor и веб-клиент CURE CURE.

«Успешное использование этой уязвимости может позволить неаутентифицированному злоумышленнику в сети создать и подписать свой собственный веб-токен JSON и использовать его для выполнения метода HTTP API без необходимости действительной аутентификации / авторизации. При определенных обстоятельствах это может быть использовано злоумышленником, чтобы повлиять на доступность системы путем проведения атаки типа «отказ в обслуживании», - предупреждает CISA в своем бюллетене по безопасности, опубликованном во вторник». ***(Tom Spring. Multiple Industrial Control System Vendors Warn of Critical Bugs // Threatpost (https://threatpost.com/ics-vendors-warn-critical-bugs/161333/). 17.11.2020).***

***

Проблемы безопасности в программируемых логических контроллерах Schneider Electric допускают компрометацию оборудования, отвечающего за физические операции предприятия.

Две уязвимости в системе безопасности программируемых логических контроллеров (ПЛК) Schneider Electric могут позволить злоумышленникам взломать ПЛК и перейти к более сложным атакам на критически важную инфраструктуру.

ПЛК являются ключевыми элементами оборудования в таких средах, как электроэнергетика и фабрики. Они контролируют площадь физического оборудования на заводских сборочных линиях и в других промышленных средах и являются ключевой частью сетей операционных технологий (OT).

По словам исследователей из Trustwave, проблемы присутствуют в программном обеспечении для управления ПЛК EcoStruxure Machine Expert v1.0 и в прошивке для ПЛК M221 версии 1.10.2.2 соответственно.

CVE и оценки серьезности ожидаются, и доступны исправления.

Взлом шифрования пароля

Первая уязвимость, уязвимость малого размера, позволяет обнаруживать ключи шифрования, используемые EcoStruxure Machine-Expert Basic для защиты приложений. Доступны два типа защиты приложений: защита от чтения защищает приложение контроллера от чтения неуполномоченным персоналом на рабочей станции инженера; а защита от записи защищает приложение контроллера от несанкционированных изменений.

«Мы можем провести исчерпывающий поиск ключей, чтобы определить ключ шифрования, который используется для шифрования хешированного пароля, используемого для защиты приложения на ПЛК», - пояснили исследователи Trustwave в своем сообщении в четверг. «Злоумышленник может использовать этот ключ шифрования для расшифровки зашифрованного хеш-пароля, который отправляется контроллеру для разблокировки защиты от чтения / записи».

Исследователи отметили, что перебор стал возможным благодаря двум недостаткам: во-первых, случайный одноразовый номер и секретный ключ, используемые в процессе шифрования, обмениваются открытым текстом.

«Следовательно, мы можем перехватить и получить секретный ключ из сетевых пакетов», - заявили они.

А во-вторых, семя, которое используется для генерации ключей, имеет длину всего два байта. Это означает, что существует только 65 535 возможных комбинаций семян.

«Как только мы получили начальное число, мы можем использовать его и одноразовый номер, извлеченные из сетевого пакета, для генерации ключа шифрования», - сказали исследователи. «Этот ключ шифрования можно использовать для расшифровки зашифрованного хешированного пароля, который мы извлекли из сетевого пакета с помощью алгоритма XOR».

Более сложные атаки

Вторая ошибка - проблема обхода безопасности для механизма защиты приложений, которая может открыть дверь для гораздо более серьезных атак. Исследователи обнаружили альтернативный канал для обхода функции защиты от чтения на контроллере.

«Эта функция защиты от чтения предназначена для защиты приложения, развернутого на контроллере, от загрузки неавторизованным персоналом», - заявили в компании. «[Обход] может использоваться злоумышленником для обхода защиты и загрузки приложения с контроллера M221».

Альтернативный канал - это возможность отправлять запросы данных приложения от третьего лица напрямую контроллеру.

«Эти полезные данные могут быть успешно использованы контроллером без какой-либо аутентификации, тем самым обходя любую существующую защиту от чтения», - сообщает Trustwave. «В ходе нашего анализа мы также поняли, что передаваемые данные приложения будут отправляться в открытом виде, а не в зашифрованном виде».

Это, в свою очередь, позволит злоумышленнику провести разведку основного приложения M221, проложив путь для более сложных последующих атак, говорят исследователи Trustwave. Это потому, что приложение содержит управляющую логику, развернутую на контроллере. Эта логика использует так называемые «теги» в промышленных системах управления (ICS) для связи через сеть операционных технологий (OT).

По словам Trustwave, «понять функцию этих тегов в сети - нетривиальная задача. «Для того, чтобы злоумышленник провел целевую атаку, ему необходимо выяснить контекст тегов, которые используются в логике управления. Один из способов упростить этот процесс - загрузить логику управления из контроллера и прочитать теги, которые настроены для получения полного понимания процесса, развернутого на контроллере ».

Schneider Electric рекомендует исправлять инженерное программное обеспечение, обновлять прошивку контроллера и блокировать порты на межсетевом экране. Trustwave добавила, что клиенты также должны использовать два разных сложных пароля для различных средств защиты приложений и принять

меры, чтобы только рабочая станция и авторизованные клиенты могли напрямую связываться с ПЛК.

ICS в центре внимания

ICS привлекает все больше внимания исследователей безопасности и федерального правительства. Например, критическая инфраструктура стала главной темой для отдела кибербезопасности и инфраструктуры Агентства внутренней безопасности безопасности (CISA) в этом году, он объявил.

И действительно, по мере того, как усиливается этот фокус, в оборудовании ICS обнаруживается все больше и больше ошибок. Например, хакерские соревнования, такие как Pwn2Own, начали фокусироваться на ICS.

Эти усилия приносят плоды: в марте были обнаружены критические ошибки, затрагивающие ПЛК и физические системы контроля доступа от Rockwell Automation и Johnson Controls.

А в июле, сразу после ужасного предупреждения от CISA о надвигающихся атаках на критически важную инфраструктуру, ICS-CERT выпустила уведомление о критической ошибке безопасности в Schneider Electric Triconex TriStation и модуле связи Tricon. Эти контроллеры инструментальных систем безопасности (SIS) отвечают за остановку работы предприятия в случае возникновения проблемы и действуют как автоматизированная защита безопасности промышленных объектов, предназначенная для предотвращения отказа оборудования и катастрофических инцидентов, таких как взрывы или пожар.

В прошлом они подвергались атаке TRITON в 2017 году». ***(Tara Seals. Bugs in Critical Infrastructure Gear Allow Sophisticated Cyberattacks // Threatpost (https://threatpost.com/bugs-critical-infrastructure-gear-attacks/161164/). 12.11.2020).***

***

«Ошибки, отслеживаемые как CVE-2020–8271, CVE-2020–8272 и CVE-2020–8273, существуют в Citrix SD-WAN Center.

По мнению исследователей, три ошибки безопасности в программно-определяемой (SD) -WAN платформе Citrix позволили бы удаленное выполнение кода и захват сети.

Недостатки затрагивают Citrix SD-WAN Center (в версиях до 11.2.2, 11.1.2b и 10.2.8). Они состоят из неаутентифицированного обхода пути и проблемы внедрения оболочки в stop_ping (CVE-2020–8271); обход аутентификации ConfigEditor (CVE-2020–8272); и проблема внедрения оболочки CreateAzureDeployment (CVE-2020–8273). Баллы серьезности еще не выставлены.

В первых двух случаях злоумышленник должен иметь возможность связываться с IP-адресом управления SD-WAN Center или полным доменным именем (FQDN), согласно рекомендациям Citrix, выпущенным на прошлой неделе. В третьем случае злоумышленник должен пройти аутентификацию.

Согласно Citrix, первая уязвимость позволяет неаутентифицированному RCE с привилегиями root в Citrix SD-WAN Center. В отчете Realmode Labs в понедельник более подробно рассказывается о том, где он существует.

По словам исследователя Realmode Ариэля Темпельхофа, для CVE-2020–8271 «конечная точка / collector / diagnostics / stop_ping читает файл / tmp / pid_». «$

Req_id и использует его содержимое в вызове shell_exec. Никакая дезинфекция не выполняется для предоставленного пользователем $ req_id, что позволяет обход пути. Можно перетащить файл с управляемым пользователем содержимым куда угодно (например, с помощью / collector / licensing / upload) и запустить произвольную команду оболочки».

Вторая ошибка связана с тем, как CakePHP переводит URI в параметры функции конечной точки. Это может привести к раскрытию функций SD-WAN без проверки подлинности.

Инфраструктура Citrix SD-WAN работает на Apache с CakePHP2 в качестве основы. Исследователи из Realmode обнаружили дыру в том, как фреймворк CakePHP2 обрабатывает URL-адреса. Для этого Citrix использует функцию «_url в CakeRequest.php».

«Если наш REQUEST_URI содержит? после: // начало URI будет удалено», - говорится в сообщении Темпельхофа в понедельник. «Это вызовет несоответствие между тем, как Apache видит URI, и тем, как CakePHP анализирует его, что, в свою очередь, позволяет нам обойти проверку сертификата клиента для конечной точки Collector».

Например, URI в форме «aaaaaaaaaaaaaaaa /: //? / Collector / diagnostics / stop_ping» будет преобразован в / collector / diagnostics / stop_ping и не потребует ни сертификата клиента, ни аутентификации, сказал он. Это позволяет неаутентифицированному злоумышленнику получить доступ к функциям ConfigEditor.

Что касается третьей ошибки, данные, предоставленные пользователем, кодируются в формате JSON и объединяются с вызовом exec с использованием кода, сказал Темпельхоф.

«В защиту Citrix мы признаем, что трудно ожидать, что CakePHP будет обрабатывать URL-адреса так, как он это делает», - сказал Темпельхоф. «Вот почему так важно проводить специальные аудиты безопасности ваших продуктов».

На прошлой неделе Realmode обнаружила три ошибки безопасности удаленного выполнения кода в Silver Peak Unity Orchestrator для SD-WAN. Их можно объединить в цепочку, чтобы обеспечить захват сети злоумышленниками, не прошедшими проверку подлинности.

Темпельхоф сказал, что его команда обнаружила аналогичные недостатки еще в двух платформах SD-WAN (все теперь исправлены), о которых скоро будет сообщено.

SD-WAN - это облачный сетевой подход, используемый предприятиями и многопрофильными предприятиями любого размера. Он позволяет подключать местоположения и облачные экземпляры друг к другу и к ресурсам компании через любой тип подключения и применяет программный контроль для управления этим процессом, включая оркестровку ресурсов и узлов.

Это растущий сегмент рынка, который представляет интерес для киберпреступников. К сожалению, в прошлом у ведущих поставщиков SD-WAN были проблемы.

Например, в марте Cisco Systems устранила три уязвимости высокой степени серьезности, которые могли позволить локальным, прошедшим проверку

подлинности злоумышленникам выполнять команды с привилегиями root. Похожая ошибка была обнаружена месяцем позже в Cisco IOS XE, версии межсетевой операционной системы Cisco (IOS) на базе Linux, используемой в развертываниях SD-WAN.

А в декабре прошлого года критическая ошибка нулевого дня была обнаружена в различных версиях продуктов Citrix Application Delivery Controller (ADC) и Citrix Gateway, которые позволяли перехват устройств и RCE, используемые в реализациях SD-WAN. После того, как об этом было объявлено, количество атак и публичных эксплойтов быстро накапливалось». ***(Tara Seals. Citrix SD-WAN Bugs Allow Remote Code Execution // Threatpost (https://threatpost.com/citrix-sd-wan-bugs-remote-code-execution/161274/). 16.11.2020).***

***

«Разработчики Mozilla и Google исправили критические уязвимости в браузерах Firefox и Chrome, которые недавно были продемонстрированы хакерами на китайском соревновании Tianfu Cup…

Равно как и во время Pwn2Own, обо всех использованных эксплоитах и найденных багах сообщают разработчикам скомпрометированных продуктов, и патчи выходят вскоре после завершения мероприятия. Так как в этом году участникам удалось скомпрометировать iOS, Windows 10, Safari, Chrome, Firefox и другие продукты, исправления и подробная информация о найденных багах не заставили себя ждать.

Уязвимость в Firefox, получившая идентификатор CVE-2020-26950, описывается разработчиками браузера как проблема, связанная с use-after-free багом в MCallGetProperty. Недостаток был исправлен в составе Firefox 82.0.3, Firefox ESR 78.4.1 и Thunderbird 78.4.2

В свою очередь, уязвимость в Chrome, обнаруженная на Tianfu Cup, отслеживается как CVE-2020-16016. В Google ее описывают как некорректную имплементацию в компоненте base. Инженеры компании исправили баг обновлении для Chrome 86, которое было выпущено в начале текущей недели.

Эксплуатация уязвимостей CVE-2020-26950 и CVE-2020-16016 была продемонстрирована на Tianfu Cup командой китайского технологического гиганта Qihoo 360. Именно эта команда в итоге стала победителем соревнований и забрала с собой 744 500 долларов, то есть почти и две трети всего призового фонда мероприятия, который в этом году составлял 1 210 000 долларов. Так, уязвимость в Firefox принесла специалистам 40 000 долларов, а проблема в Chrome, которая позволила добиться удаленного выполнения кода с выходом из песочницы, была оценена в 100 000 долларов». ***(Мария Нефёдова. В Firefox и Chrome исправлены уязвимости, выявленные в ходе Tianfu Cup // Xakep (https://xakep.ru/2020/11/13/ff-chrome-bugs/). 13.11.2020).***

***

«Drupal выпустила экстренные обновления безопасности для устранения критической уязвимости с известными эксплойтами, которые могут допускать выполнение произвольного кода PHP в некоторых версиях CMS.

«Согласно расписанию регулярных окон выпуска безопасности, 25 ноября обычно не является основным периодом безопасности», - сказал Drupal.

«Однако этот выпуск необходим, потому что есть известные эксплойты для одной из зависимостей ядра, а некоторые конфигурации Drupal уязвимы».

Прямо сейчас более 944 000 веб-сайтов используют уязвимые версии Drupal из общего числа 1 120 941, согласно официальной статистике. «Эта статистика является неполной; в данные включаются только веб-сайты Drupal, использующие модуль Update Status», - сообщает Drupal.

Drupal также используется 2,5% всех веб-сайтов с системами управления контентом, что делает его четвертым по популярности CMS в Интернете после WordPress (63,8%), Shopify (5,1%) и Joomla (3,6%).

Обновления безопасности для всех уязвимых версий

Согласно рекомендациям по безопасности Drupal, уязвимость вызвана двумя ошибками в библиотеке PEAR Archive_Tar, используемой системой управления контентом (CMS), которые отслеживаются как CVE-2020-28948 и CVE-2020-28949.

Критическая уязвимость выполнения кода Drupal может быть использована, если CMS настроена на разрешение и обработку загрузки файлов .tar, .tar.gz, .bz2 или .tlz.

Было выпущено несколько обновлений безопасности Drupal, чтобы исправить ошибку и позволить администраторам быстро исправлять свои серверы, чтобы защитить их от потенциальных атак.

Drupal рекомендует установить следующие обновления на уязвимых серверах:

Пользователи Drupal 9.0 должны обновиться до Drupal 9.0.9

Пользователи Drupal 8.9 должны обновиться до Drupal 8.9.10

Пользователи Drupal 8.8 или более ранней версии должны обновиться до Drupal 8.8.12.

Пользователи Drupal 7 должны обновиться до Drupal 7.75

«Версии Drupal 8 до 8.8.x являются устаревшими и не получают защиты», - заявили в команде безопасности Drupal.

Также доступны меры по смягчению последствий

Меры по смягчению также доступны для администраторов, которые не могут сразу обновить установку Drupal на своих серверах.

Для этого администраторам сайта рекомендуется заблокировать ненадежным пользователям возможность загрузки файлов .tar, .tar.gz, .bz2 или .tlz, чтобы временно устранить проблему.

Агентство кибербезопасности и безопасности инфраструктуры (CISA) Министерства национальной безопасности также выпустило сегодня предупреждение, призывающее администраторов и пользователей перейти на исправленные версии Drupal.

На прошлой неделе Drupal устранил еще одну критическую уязвимость удаленного выполнения кода, которая была отмечена как CVE-2020-13671 и вызвана неправильной очисткой имен загруженных файлов.

«Обратите особое внимание на следующие расширения файлов, которые следует считать опасными, даже если за ними следует одно или несколько дополнительных расширений: phar, PHP, pl, py, cgi, asp, js, HTML, htm и phtml», - заявили в компании.

«Этот список не является исчерпывающим, поэтому оценивайте проблемы безопасности для других включенных расширений в индивидуальном порядке». ***(Sergiu Gatlan. Drupal issues emergency fix for critical bug with known exploits // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/drupal-issues-emergency-fix-for-critical-bug-with-known-exploits/). 27.11.2020).***

***

«TikTok устранил две уязвимости, которые могли позволить злоумышленникам захватить учетные записи одним щелчком мыши при объединении в цепочку для пользователей, которые зарегистрировались через сторонние приложения.

Платформа социальных сетей, принадлежащая базирующейся в Пекине ByteDance, используется для обмена короткими зацикленными мобильными видео продолжительностью от 3 до 60 секунд.

Согласно официальной статистике Google Play Store, Android-приложение TikTok в настоящее время имеет более 1 миллиарда установок и в апреле 2020 года превысило отметку в 2 миллиарда установок на всех мобильных платформах, согласно оценкам Sensor Tower Store Intelligence.

Найдено с помощью нечеткого тестирования

Немецкий охотник за вознаграждением Мухаммед Таскиран обнаружил ошибку безопасности, связанную с межсайтовым скриптингом (XSS), также известную как непостоянный XSS, в параметре URL TikTok, отражающем его значение без надлежащей очистки.

Таскиран обнаружил отраженный XSS, который также мог привести к утечке данных при нечетком тестировании доменов компании www.tiktok.com и m.tiktok.com.

Он также обнаружил, что конечная точка API TikTok уязвима для атак с подделкой межсайтовых запросов (CSRF), которые позволяют изменять пароли учетных записей для пользователей, которые зарегистрировались с помощью сторонних приложений.

«Конечная точка позволила мне установить новый пароль для учетных записей, которые использовали сторонние приложения для регистрации», - сказал Таскиран.

«Я объединил обе уязвимости, создав простую полезную нагрузку JavaScript, запускающую CSRF, которую я ранее вставил в параметр уязвимого URL, чтобы заархивировать «захват учетной записи в один клик».

Таскиран сообщил TikTok о цепочке атак по захвату учетной записи 26 августа 2020 года, когда компания решила проблемы и 18 сентября наградила охотника за ошибками наградой в размере 3860 долларов.

В прошлом году исправлено больше ошибок для взлома аккаунтов

TikTok также устранил ряд уязвимостей в своей инфраструктуре, что позволило потенциальным злоумышленникам захватить учетные записи, манипулировать видео пользователей и украсть их информацию.

Проблемы безопасности были раскрыты ByteDance исследователями Check Point в конце ноября 2019 года, и компания исправила ошибки в течение одного месяца.

Злоумышленники могли использовать SMS-систему TikTok, чтобы использовать уязвимости для загрузки несанкционированных и удаленных видео, перемещения видео пользователей из частных в общедоступные и кражи конфиденциальных личных данных.

«TikTok стремится защищать пользовательские данные», - сказал в то время инженер по безопасности TikTok Люк Дешотелс. «Как и многие организации, мы поощряем ответственных исследователей в области безопасности раскрывать нам уязвимости нулевого дня в частном порядке». ***(Sergiu Gatlan. TikTok fixes bugs allowing account takeover with one click // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/tiktok-fixes-bugs-allowing-account-takeover-with-one-click/). 23.11.2020).***

***

«Вчера Национальный центр кибербезопасности Великобритании (NCSC) опубликовал предупреждение, в котором всем организациям было предложено исправить критическую уязвимость CVE-2020-15505 удаленного выполнения кода (RCE) в системах управления мобильными устройствами MobileIron (MDM).

MDM - это программная платформа, которая позволяет администраторам удаленно управлять мобильными устройствами в своей организации, включая удаление приложений, обновлений и возможность изменять настройки. Все это управление осуществляется из централизованного места, такого как консоль администратора, работающая на сервере организации, что делает ее основной целью для злоумышленников.

NCSC предупреждает, что им известно о хакерских группах, активно использующих уязвимость MobileIron CVE-2020-1550 для взлома сетей в здравоохранении, местных органах власти, логистике и юридическом секторе.

«NCSC осведомлен о том, что национальные группы Advanced Persistent Threat (APT) и киберпреступники сейчас активно пытаются использовать эту уязвимость [T1190] для компрометации сетей британских организаций», - говорится в сообщении.

Агентство кибербезопасности и инфраструктуры США (CISA) также предупредило, что хакерские группы APT активно используют эту уязвимость для получения доступа к сетям. Агентство национальной безопасности США (NSA)

заявляет, что CVE-2020-15505 входит в число 25 основных уязвимостей, используемых китайскими хакерами, спонсируемыми государством.

Доступны экспериментальные эксплойты

Уязвимость MobileIron CVE-2020-15505 позволяет злоумышленнику удаленно выполнять команды на сервере MDM без необходимости аутентификации.

Поскольку серверы MDM должны быть общедоступными для удаленного управления мобильными устройствами, это делает их привлекательной мишенью для злоумышленников.

Обнаруженная и ответственно раскрытая исследователем безопасности Orange Tsai в марте, MobileIron выпустила исправления и рекомендации в июне. Orange Tsai также опубликовал видео, демонстрирующее, как уязвимость использовалась для получения доступа к серверу Facebook MDM, как показано ниже.

Вскоре после этого исследователи выпустили экспериментальный эксплойт (PoC) для уязвимости, который позволяет удаленным злоумышленникам выполнять команды на уязвимых устройствах.

APT-группы и хакерские группы, спонсируемые государством, вскоре начали использовать эту уязвимость для взлома сетей, включая сеть, используемую системами поддержки выборов в США.

В связи с этим NCSC Великобритании настоятельно призывает все организации, использующие уязвимое программное обеспечение, незамедлительно применить исправления.

Версии MobileIron, уязвимые для CVE-2020-15505:

10.3.0.3 и ранее

10.4.0.0, 10.4.0.1, 10.4.0.2, 10.4.0.3, 10.5.1.0, 10.5.2.0 и 10.6.0.0

Sentry версии 9.7.2 и ранее

9.8.0

База данных мониторинга и отчетности (RDB) версии 2.0.0.1 или более ранней

Информацию о доступных исправлениях можно найти в уведомлении MobileIron». ***(Lawrence Abrams. UK urges orgs to patch critical MobileIron CVE-2020-15505 RCE bug // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/uk-urges-orgs-to-patch-critical-mobileiron-cve-2020-15505-rce-bug/). 24.11.2020).***

***

«Для исправления уязвимостей и добавления новых функций в свою систему бесключевого доступа в автомобилях Tesla Model X компания Tesla использует обновления «по воздуху». Однако, по словам специалиста Левенского католического университета (Бельгия) Леннерта Ваутерса (Lennert Wouters), с помощью этого механизма доставки обновлений можно в считанные минуты угнать автомобиль.

Ваутерс обнаружил как в системе бесключевого доступа Tesla Model X так и в самом автомобиле уязвимости, позволившие ему через Bluetooth-подключение

переписать прошивку брелока, снять код разблокировки и угнать автомобиль. По словам исследователя, угонщик, которому удастся прочитать идентификационный номер (обычно он виден на приборной панели автомобиля через лобовое стекло) и приблизиться к брелоку жертвы на расстояние 4,6 м, сможет проэксплуатировать эти уязвимости. Необходимое для этого оборудование обойдется в $300, его спокойно можно уместить в рюкзак, а управление осуществляется с помощью смартфона.

Всего за 90 секунд представленное Ваутерсом устройство способно извлечь радиокод для разблокировки Tesla Model X. Оказавшись внутри автомобиля, угонщик может проэксплуатировать вторую уязвимость и всего за минуту завести машину с помощью собственного брелока.

«По сути, комбинация из двух уязвимостей позволяет хакеру угнать Model X за несколько минут. Если их скомбинировать, атака получится гораздо мощнее», - сообщил исследователь.

Ваутерс уведомил Tesla о проблеме в августе нынешнего года, и компания пообещала выпустить исправления для брелоков (и, возможно, для компонентов автомобиля) на этой неделе. По словам производителя, рассылка обновлений всем уязвимым Tesla Model X может занять до одного месяца, поэтому владельцы должны устанавливать все доступные обновления, чтобы защитить себя от вышеописанной атаки. Со своей стороны, исследователь пообещал не публиковать раньше времени никаких кодов и подробностей об уязвимостях во избежание их возможной эксплуатации хакерами». ***(Новая Bluetooth-атака позволяет в считанные минуты угнать Tesla Model X // SecurityLab.ru (https://www.securitylab.ru/news/514263.php). 23.11.2020).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Задача Digital Security by Design (DSbD) получила две новые финансовые награды, которые помогут предотвратить атаки с помощью систем кибербезопасности.

Задача Digital Security by Design (DSbD), возглавляемая UK Research and Innovation, направлена на предотвращение удаленного доступа хакеров к управлению цифровыми системами, такими как автономные автомобили, личные устройства, системы безопасности умного дома, а также кибератаки и утечки данных в Интернете Мир.

Последние награды. Демонстратор работы с технологией Arm

5,8 миллиона фунтов стерлингов были присуждены консорциуму, возглавляемому компанией THG Holdings plc (THG), занимающейся глобальной технологической платформой, работающей с Манчестерским и Оксфордским университетами.

В рамках партнерства будет разработан важнейший демонстрационный элемент для работы с ведущей технологической фирмой, прототипом платформы Arm, проектом Morello, который ранее получил финансирование UKRI.

Этот демонстратор протестирует преимущества технологии DSbD для повышения безопасности электронной коммерции и обеспечения повышения производительности и развития будущих мировых услуг и продуктов.

2,8 миллиона фунтов стерлингов будут инвестированы THG в набор персонала и специализированное оборудование для исследований, а оставшаяся часть будет распределена между университетами-партнерами.

Преодоление разрыва между безопасностью и обществом

Также было профинансировано новое сотрудничество в области исследований в Университете Бата стоимостью 3,5 миллиона фунтов стерлингов под названием DiScriBe. Министерство культуры, средств массовой информации и спорта выделило 1,2 миллиона фунтов стерлингов, а проект «Цифровая безопасность посредством дизайна» Фонда «Промышленная стратегия» профинансировал оставшиеся 2,3 миллиона фунтов стерлингов.

Этот исследовательский центр будет сосредоточен на социальной науке о цифровой безопасности, преодолевая разрыв между проблемами инженерной безопасности и предприятиями и людьми, которые будут их реализовывать.

Министр цифровой инфраструктуры Мэтт Уорман сказал:

«Эти проекты являются прекрасным примером того, как наши университеты мирового уровня работают с ведущими британскими предприятиями над разработкой передовых продуктов для кибербезопасности, обеспечивающих безопасность людей в Интернете.

«Мы предоставляем дополнительное финансирование, чтобы продолжать разрабатывать инновационные кибер-решения, вселять в потребителей и промышленность уверенность и стимулировать растущую цифровую экономику».

Директор конкурса Digital Security by Design Challenge профессор Джон Гудакр сказал:

«Значение этих двух важных наград - это импульс, который они придадут всей запланированной программе работы.

«Проект Soteria, возглавляемый THG, занимает лидирующие позиции в этом начинании и представляет собой решающую демонстрацию преимуществ безопасности, которые технология DSbD может принести все более важной отрасли электронной коммерции».

Исполнительный председатель ESRC профессор Дженнифер Рубин сказала:

«Премия DiScriBe Hub + позволит продвигать цифровую безопасность за счет комбинированного подхода, который включает понимание и устранение экономических и социальных факторов, которые в противном случае могут помешать техническим решениям.

«Обеспечивая тесное сотрудничество экономических и социальных исследователей и инженеров, мы сможем поддержать исследователей и предприятия в преодолении кражи данных и кибератак, которые представляют собой значительный глобальный риск»…». ***(R&D investments spearhead cyber security defence // Open Access Government***

(https://www.openaccessgovernment.org/rd-investments-spearhead-cyber-security-defence/96958/). 04.11.2020).

***

«Ставший очень популярным на волне карантинных ограничений сервис видеоконференций Zoom поначалу имел немало проблем с обеспечением конфиденциальности и безопасности пользователей. И вот наконец-то начато внедрение сквозного шифрования E2EE в платной и бесплатной версиях сервиса, сообщает Softprom, авторизованный партнер Zoom Video Communications. Благодаря этому пользователи во всем мире смогут осуществлять видеоконференции с количеством участников до 200 человек в режиме повышенной безопасности.

В мае компания объявила, что планирует внедрение механизма сквозного шифрования в свою платформу и сейчас заявляет о завершении первой фазы этой работы. Шифрование End-to-end encryption (E2EE) обеспечивает надёжную защиту от перехвата ключей дешифрования, которые могут быть использованы для мониторинга содержания видеоконференции.

Zoom E2EE использует то же 256-битное шифрование AES-GCM, которое по умолчанию защищает видеоконференции Zoom. Администраторы учётных записей могут включить эту функцию на веб-панели управления на уровне учётной записи, группы и пользователя, а участники также должны включить эту функцию, чтобы присоединиться к собранию со сквозным шифрованием.

В тоже время компания предупредила, что, по крайней мере, на первом этапе развёртывания E2EE будет блокировать некоторые функции Zoom, включая облачную запись, потоковую передачу, транскрипцию в реальном времени, комнаты для обсуждения, опрос, частный чат тет-а-тет и реакции на встречи. Всего этапов внедрения будет четыре.

E2EE от Zoom уже доступен для ознакомления, чтобы использовать его, клиенты должны включить собрания E2EE на уровне учетной записи и подписаться на E2EE для каждого собрания. Его участники могут найти зеленый логотип в виде щита в верхнем левом углу экрана собрания с замком посередине, чтобы указать, что их собрание использует E2EE. Он похож на символ использующегося сейчас шифрования GCM, но галочка заменена на замок.

Zoom планирует улучшить управление идентификацией и интеграцию E2EE SSO в рамках второго этапа, который ориентировочно намечен на 2021 г.» ***(Сервис видеоконференций Zoom наконец-то начал внедрение сквозного шифрования // Компьютерное Обозрение (https://ko.com.ua/servis_videokonferencij_zoom_nakonec-to_nachal_vnedrenie_skvoznogo_shifrovaniya_135104). 02.11.2020).***

***

«Производители веб-браузеров планируют заблокировать новую технику атаки, которая позволит злоумышленникам обойти NAT, брандмауэр или маршрутизатор жертвы, чтобы получить доступ к любой службе TCP / UDP, размещенной на их устройствах.

Метод атаки, получивший название NAT Slipstreaming, был обнаружен исследователем безопасности Сами Камкаром и требует, чтобы жертвы посетили вредоносный веб-сайт злоумышленника (или сайт со злонамеренно созданной рекламой).

Чтобы раскрыть размещенные службы, атака злоупотребляет определенными устройствами NAT, сканирующими порт 5060, чтобы создать правила переадресации портов при обнаружении злонамеренно созданных HTTP-запросов, замаскированных под действительные SIP-запросы.

Kamkar также предоставляет проверочный код эксплойта, чтобы продемонстрировать достоверность этой недавно раскрытой техники обхода NAT / firewal / маршрутизатора.

"Эта атака использует преимущество произвольного управления частью данных некоторых пакетов TCP и UDP без включения HTTP или других заголовков; атака использует этот новый метод внедрения пакетов во всех основных современных (и более старых) браузерах и является модернизированной версией моего оригинальная технология NAT Pinning 2010 года (представленная на DEFCON 18 + Black Hat 2010). Кроме того, включены новые методы обнаружения локальных IP-адресов», - пояснил Камкар.

«Эта атака требует, чтобы NAT / брандмауэр поддерживал ALG (шлюзы уровня приложений), которые являются обязательными для протоколов, которые могут использовать несколько портов (канал управления + канал данных), таких как SIP и H323 (протоколы VoIP), FTP, IRC DCC и т. Д.. "

Браузеры будут блокировать атаки со смещением

Чтобы заблокировать такие атаки, поставщики веб-браузеров планируют заблокировать TCP-порты 5060 и 5061, используемые в этой атаке, добавив их в ограниченный список.

«В качестве обходного пути для обхода NAT« Slipstream »мы будем блокировать соединения HTTP и HTTPS с портами SIP 5060 и 5061», - говорит разработчик Chromium Адам Райс. «Это будет означать, что подключение к серверам на этих портах не будет выполнено».

Как только порты будут добавлены в список ограниченных портов, Райс ожидает, что пользователи браузера заметят некоторое влияние, включая:

Соединения с серверами на этих портах, например http://example.com:5060/ или https://example.com:5061/, больше не будут работать. Ожидается, что это будет редко.

Тесты, которые запускают сервер на произвольном порту, а затем ожидают возможности подключения к нему, будут немного более нестабильными, чем они есть.

На данный момент команды разработчиков Firefox, Safari и Blink (движок рендеринга Chromium) выразили намерение реализовать меры, необходимые для блокирования атак NAT Slipstreaming.

Ошибки реализации также были поданы трекер ошибки Chrome и Safari 4 ноября, с изменением позже слились в канал выпуска Chrome Canary и предлагаемый патчем, совершенное для посадки команды разработчиков браузера Safari». ***(Sergiu Gatlan. New Slipstream NAT bypass attacks to be blocked by browsers***

// BleepingComputer.com (https://www.bleepingcomputer.com/news/security/new-slipstream-nat-bypass-attacks-to-be-blocked-by-browsers/). 09.11.2020).

***

«Корпорация Microsoft сообщила, что разработала технологию безопасности, которую производители микросхем Intel и Advanced Micro Devices планируют внедрить в процессоры персональных компьютеров, чтобы повысить их способность защиты от хакеров и кибератак.

Intel и AMD заявили, что чипы с новой технологией, которую Microsoft называет Pluton, будут готовы в течение следующих нескольких лет. Qualcomm выразила поддержку этому подходу, но отказалась сообщить, будет ли она включать этот инструмент в свои чипы. Microsoft и компании-производители микросхем в течение многих лет искали способы усилить защиту компьютера, блокируя важную информацию, такую как пароли и сертификаты безопасности, в оборудовании, что усложняет хакерам использование уязвимостей в одной компьютерной программе или части устройства и использование этих "дыр" для взлома всего ПК.

Защитный инструмент Microsoft будет встроен непосредственно в основной процессор компьютера, что затруднит взлом ПК и ноутбуков, а также обеспечит большую последовательность в обеспечении безопасности ПК, если эта технология будет широко использоваться. Преимущество встроенной защиты по сравнению с программной защитой заключается в том, что для взлома обычно требуется физический доступ к машине, по сравнению с риском удаленной атаки через Интернет. Это стало еще более важным во время пандемии Covid-19, потому что многие сотрудники компании работают удаленно на домашнем оборудовании, а не за корпоративными брандмауэрами.

«Сейчас есть всего несколько людей в мире, у которых есть инструменты и опыт», чтобы взломать систему с использованием новой технологии Microsoft, - сказал Дэвид Уэстон, директор по работе с партнерами, работающий над корпоративной безопасностью и безопасностью операционных систем в Microsoft.

Даже когда в настоящее время для защиты паролей и другой важной информации используются микросхемы, они часто отделены от центрального процессора или ЦП ПК. Связь между этими двумя чипами была определена хакерами как потенциальная уязвимость. Благодаря встраиванию схемы безопасности в сам ЦП это соединение не требуется, а это означает, что на одну область меньше, открытую для незаконного доступа.

Microsoft пытается перепрофилировать технологию, используемую в ее игровых консолях Xbox, которая защищает от взлома оборудование и игры за которые не заплатили, чтобы усложнить атаки на персональные компьютеры на базе Windows. Технология была разработана собственными инженерами микросхем Microsoft, командой, которая выросла по мере того, как производитель программного обеспечения занимался более индивидуальным проектированием и разработкой процессоров для таких продуктов, как Xbox и очков дополненной реальности HoloLens компании. Microsoft планирует продолжить внедрение микросхем, но вряд ли сосредоточится на микросхемах общего назначения, таких

как Intel, AMD и Qualcomm, заявил главный директор по продуктам Microsoft Панос Панай.

«Если мы думаем, что нам нужно инвестировать в кремний, мы обязательно сделаем это», - сказал Панай…». ***(Романов Роман. Microsoft объединяется с производителями микросхем для внедрения технологии защиты от хакерских атак в процессор ПК // Internetua (http://internetua.com/microsoft-ob-edinyaetsya-s-proizvoditelyami-mikroshem-dlya-vnedreniya-tehnologii-zasxity-ot-hakerskih-atak-v-processor-pk). 18.11.2020).***

***

«Microsoft запустила приоритетную защиту Office 365 для учетных записей высокопоставленных сотрудников, таких как руководители высшего звена, которые чаще всего становятся объектами атак злоумышленников.

Новая функция была добавлена в Microsoft Defender для Office 365 (ранее известный как Office 365 ATP), который обеспечивает корпоративные учетные записи с защитой от угроз электронной почты от сложных угроз, включая компрометацию корпоративной электронной почты и фишинг учетных данных, а также автоматическое устранение обнаруженных атак.

Приоритетная защита учетной записи позволяет группе безопасности организации предоставлять критически важные учетные записи с индивидуальными мерами защиты для блокирования целевых атак, таких как фишинг, которые могут привести к серьезным нарушениям безопасности из-за их доступа к высокочувствительным данным компании.

Это позволяет приоритизировать предупреждения и расследования угроз с участием наиболее целевых или видимых пользователей высшего звена организации.

Команды безопасности предприятия также могут легко выявлять атаки, нацеленные на критически важные учетные записи Office 365, и быстро переключать свои усилия на расследования кампаний с участием пользователей C-Suite.

«Эти теги и фильтры приоритетных учетных записей будут отображаться во всем продукте, в том числе в предупреждениях, обозревателе угроз, представлениях кампании и отчетах», - заявляла ранее Microsoft в прошлом месяце, когда функция еще находилась в разработке.

Как объяснил менеджер по маркетингу Microsoft 365 Скотт Шнолл, приоритетную защиту учетной записи можно настроить, зайдя в Центр безопасности и соответствия требованиям.

Чтобы получить доступ к этой новой функции, у клиентов должны быть подписки на Защитник для Office 365 (план 2), в том числе с Office 365 E5, Microsoft 365 E5 или Microsoft 365 E5 Security.

Ранее в этом месяце Microsoft также объявила об общедоступности защиты от фишинга согласия Office 365, включая проверку издателя приложений OAuth и политики согласия приложений.

Redmond также планирует добавить поддержку SMTP MTA Strict Transport Security (MTA-STS) в Exchange Online для обеспечения целостности и

безопасности сообщений электронной почты клиентов Office 365, начиная со следующего месяца.

После запуска поддержка MTA-STS поможет защитить электронную почту пользователей Exchange Online от перехвата электронной почты, перехода на более раннюю версию или атак типа «человек посередине». ***(Sergiu Gatlan. Microsoft rolls out protection for critical accounts in Office 365 // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/microsoft-rolls-out-protection-for-critical-accounts-in-office-365/). 19.11.2020).***

***

«Zoom объявила сегодня о внедрении новых усовершенствований безопасности, призванных помочь организаторам встреч блокировать попытки зумомбирования, а участникам - сообщать о ненадлежащем поведении пользователей.

Программное обеспечение для видеоконференцсвязи Zoom стало чрезвычайно популярным способом поддерживать связь с семьей и друзьями с начала пандемии: в апреле компания сообщила, что ее платформу ежедневно используют 300 миллионов пользователей.

Зомомбирование происходит, когда к собраниям Zoom присоединяются неавторизованные третьи стороны с целью нарушить текущие сеансы и беспокоить участников.

Новые улучшения безопасности

Первая новая функция безопасности, добавленная Zoom, получившая название «Приостановить действия участников» и включенная по умолчанию для всех пользователей Zoom, позволяет организаторам и соорганизаторам временно приостанавливать собрания и быстро удалять всех участников, мешающих работе.

Нажав кнопку «Приостановить действия участников» под значком «Безопасность», организаторы смогут немедленно прекратить все видео, аудио, чат во время собрания, аннотации, совместное использование экрана, запись и действия в комнатах обсуждения.

«Организаторов или соведущих спросят, хотят ли они сообщить о пользователе со своей встречи, поделиться любыми подробностями и, при желании, включить снимок экрана», - пояснил Zoom. «После того, как они нажмут «Отправить», заявленный пользователь будет удален со встречи, и команда Zoom по обеспечению доверия и безопасности получит уведомление».

Вторая функция, известная как «Отчет участников», также позволяет участникам собрания сообщать о троллях-зомомберах, щелкая значок «Безопасность» в верхнем левом углу окна клиента Zoom.

Хотя он не включен по умолчанию, «Отчет по участникам» может быть включен администраторами и владельцами учетных записей в веб-настройках.

Новые улучшения безопасности сразу же доступны для всех пользователей настольных клиентов Zoom для macOS, Windows, Linux и мобильных приложений, а пользователи веб-клиента и VDI получат доступ позже в этом году.

Начиная с этой осени, недавно развернутая программа Zoom «Уведомление о встречах с риском» также будет автоматически уведомлять владельцев учетных

записей по электронной почте о ссылках на встречи Zoom с высоким риском сбоя…». ***(Sergiu Gatlan. Zoom rolls out security enhancements to stop zoombombing trolls // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/zoom-rolls-out-security-enhancements-to-stop-zoombombing-trolls/). 16.11.2020).***

***

«Браузер Firefox 83 стал расходовать на 8% меньше оперативной памяти и загружать страницы на 15% быстрее, чем это делал Firefox 82. Mozilla добилась этого за счет оптимизации поддержки JavaScript, попутно добавив в свой браузер массу других нововведений.

Новая версия браузера Mozilla Firefox 83 также получит функцию безопасности под названием HTTPS-Only Mode. В таком режиме не будут открываться небезопасные сайты.

Активировать опцию можно на странице Firefox Options в разделе Privacy & Security. Браузер в режиме HTTPS-Only Mode будет пытаться найти HTTPS-версию любого сайта, даже если пользователь кликает на ссылку HTTP. Если это не удастся, программа предупредит об опасности. Впрочем, он всё равно сможет открыть сайт на свой страх и риск». ***(В браузере Mozilla Firefox появился режим только https // SecurityLab.ru (https://www.securitylab.ru/news/514166.php). 19.11.2020).***

***

«Group-IB раскрыла результаты многолетней разработки собственных высокотехнологичных продуктов для исследования киберугроз и охоты за атакующими. Group-IB первой в мире создала систему нового класса Threat Intelligence & Attribution, способную гибко формировать карту угроз под конкретную компанию, динамически выстраивая связи между разрозненными событиями и атрибутируя атаку до конкретной хакерской группы.

Еще одной инновационной премьерой стала комплексная система Threat Hunting Framework, предназначенная для защиты ИТ и технологических сетей от неизвестных ранее угроз и целевых атак, поиска угроз как внутри, так вне сети, а также расследования инцидентов кибербезопасности и немедленного реагирования на них в целях минимизации последствий.

«Умная» экосистема Group-IB, объединившая инновационные технологии компании сфере кибербезопасности, впервые была представлена в рамках международной конференции CyberCrimeCon 2020.

По данным аналитического отчета Hi-Tech Crime Trends 2020-2021, посвященного исследованию высокотехнологичных преступлений в мире, сращивание разных слоев киберкриминального андеграунда привело к появлению новых угроз, следствием которых стало увеличение ущерба от атак. Так, по самым минимальным подсчетам аналитиков, суммарный ущерб, причиненный компаниям в 45 странах от публично известных атак программ-шифровальщиков составил свыше $1 млрд. Взрывными темпами рос рынок продажи доступов в скомпрометированную инфраструктуру компаний: за год он увеличился в 4 раза и достиг $6 189 388. Количество «продавцов» взлетело до 63, среди них — как

представители киберкриминала, так и прогосударственные атакующие. Объем рынка кардинга, связанного с кражей данный банковских карт, вырос на 116% по сравнению с прошлым периодом и вплотную приблизился к $2 млрд. В этих условиях коммерческий сектор и государственные предприятия вынуждены переоценить свои стратегии защиты, делая упор на хантинг за угрозами, релевантными для своей сферы деятельности.

Сегодня Group-IB впервые представила результаты эволюционного развития собственных продуктов для расследования высокотехнологичных преступлений и предотвращения кибератак Threat Hunting Framework и Threat Intelligence & Attribution. Сложные инженерные разработки Group-IB интегрированы между собой и объединены в «умную» технологическую экосистему, способную полностью автоматизировано останавливать целевые атаки на организацию, давая команде безопасности инструменты соединения разрозненных событий вокруг атаки, атрибуции угроз, анализа вредоносного кода и реагирования на инцидент.

«Динамика развития киберпреступности сигнализирует рынку о том, что основную массу угроз вы должны уметь отражать автоматически, но этого мало, — сказал Дмитрий Волков, CTO Group-IB, — Злоумышленники, располагающие деньгами, умом и ресурсами, со временем научатся обходить любую автоматизированную систему обнаружения. Нужно быть готовым к этому, наращивая опыт хантинга за угрозами с помощью «заточенных» под это инструментов. В этой борьбе недопустима простая блокировка: завтра вас атакуют с учетом того, как вы остановили угрозу сегодня. Хантинг – это постоянный процесс, построенный на умении использовать огромные массивы данных, начиная от системных событий и мета-данных трафика и заканчивая доменами, хостами и профайлами атакующих группировок. Уметь работать с этим – значит обладать профессией «третхантера» — охотника за киберугрозами и хакерами. Это и есть будущее кибербезопасности».

Инженерная команда Group-IB руководствуется несколькими принципами при создании технологий. Во-первых, системы и алгоритмы обнаружения должны «знать» злоумышленников, а специалисты по кибербезопасности — получать либо качественное техническое обоснование, либо полный разведывательный контекст об угрозе: кто атакует, какова мотивация атакующих, какова их тактика, какими инструментами пользуются и что потенциально будут использовать при дальнейших попытках атак. Система защиты должна эффективно обнаруживать и немедленно блокировать угрозы, но сегодня этого недостаточно. Для построения работающих стратегий кибербезопасности — детектирование лишь начало работы.

Во-вторых, процесс обогащения данными систем защиты должен быть автоматизирован. Для этого механизм анализа выходит за рамки простого обнаружения угрозы: крайне важно извлечь и полностью запустить вредоносный код в безопасной изолированной среде, собрав «урожай» из индикаторов, который помогут в дальнейшем хантинге за угрозами в сети. В-третьих, хантинг приходит на смену поиска угроз для того, чтобы найти то, что могло быть упущено в прошлом и потенциально может быть использовано злоумышленниками в будущем.

Group-IB Threat Hunting Framework – универсальное решение для ИТ и технологических сетей, основными задачами которого являются обнаружение неизвестных ранее угроз и целевых атак, поиск угроз как внутри, так и за пределами защищенного периметра, а также расследование инцидентов кибербезопасности и реагирование на них. Архитектура Threat Hunting Framework включает несколько основных функциональных модулей.

Для выявления угроз на сетевом уровне за счет глубокого анализа сетевого трафика используется Sensor. Технологическую сеть от целевых атак защищает отдельный модуль Sensor Industrial. Он обеспечивает контроль целостности программного обеспечения и прошивок узлов АСУ ТП за счет анализа промышленных протоколов и комплексной защиты сети, детектируя угрозы гибко настраиваемыми политиками и специальным классификатором, использующим машинное обучение. Еще одна инновация Group-IB — Polygon. Эта платформа создана для «детонации» вредоносного кода. Она детектирует угрозы за счет поведенческого анализа электронных писем, файлов и содержимого ссылок и запускает вредоносный код в изолированной среде, вызывая его «детонацию», то есть максимально полное выполнение, позволяющее получить обогащенные индикаторы атаки и выполнить атрибуцию обнаруженной угрозы.

Также Group-IB представила инновационную защиту для рабочих станций пользователей — Huntpoint. Этот модуль фиксирует полную хронологию событий на компьютере сотрудника, обеспечивая обнаружение аномального поведения, блокировку вредоносных файлов, мгновенную изоляцию атакованных хостов и сбор криминалистически значимых данных для дальнейшего исследования.

За полностью автоматизированный анализ и корреляцию событий в сети отвечает Huntbox. Этот модуль предоставляет полную картину происходящего внутри и вне сети, помогая проактивно охотиться за угрозами и выявлять действия атакующих группировок, направленных конкретно на компанию. Также возможности комплексной платформы Group-IB Threat Hunting Framework усилены за счет функционала модуля Decryptor для расшифровки TLS/SSL-трафика в защищаемой инфраструктуре. Реализована поддержка российских протоколов шифрования по ГОСТ.

Одна из самых высоконагруженных систем Group-IB, оперирующая данными о хакерских группах, их инструментах и инфраструктуре, Threat Intelligence & Attribution, шагнула на несколько уровней вверх. Появление на рынке TI&A знаменует собой открытие нового класса решений для сбора данных об угрозах и атакующих, релевантных для конкретной организации, с целью исследования, проактивной охоты за хакерами и защиты сетевой инфраструктуры.

Объединяя в себе уникальные источники данных, опыт расследования высокотехнологичных преступлений и реагирования на сложные многоступенчатые атаки по всему миру, именно TI&A во многом «накачивает» данными для хантинга за атакующими и угрозами все остальные продукты Group-IB. Система «хранит» данные о хакерах и их связях, доменах, IP, инфраструктуре за 15 лет, включая те, что преступники пытались удалить. Обширный функционал позволяет настраивать ее под ландшафт угроз не только отдельной отрасли, но и отдельной компании в конкретной стране.

В центре внимания новой TI&A — атакующие. Вокруг них выстроена вся идеология системы: выявить не только угрозу, но того, кто за ней стоит. Массивы данных, которыми она оперирует, помогают оперативно связывать атаку с группировкой или конкретными персоналиями. TI&A «умеет» анализировать и атрибутировать угрозы, с которыми уже столкнулась компания, обнаруживать утечки и компрометацию пользователей, идентифицировать инсайдеров, торгующих данными компании на андеграудных ресурсах, выявлять и блокировать атаки, нацеленные на компанию и ее клиентов, независимо от отрасли.

Вывод на рынок TI&A открывает доступ к внутренним инструментам Group-IB до этого времени использовавшимся исключительно командами реагирования, хантинга и киберразведки компании. Теперь каждому специалисту, использующему TI&A, доступен поиск по крупнейшей коллекции данных даркнета, продвинутая модель профилирования хакерских групп, а также полностью автоматизированный графовый анализ, который за секунды помогает провести корреляцию данных и атрибутировать угрозы до конкретной преступной группировки или физического лица.

TI&A позволяет обнаруживать атаки, не покрываемые традиционными средствами защиты, глубже понимать методы работы продвинутых атакующих, а также оценивать, может ли им противостоять защищаемая инфраструктура. Такой подход помогает мотивировать и совершенствовать внутренние команды кибербезопасности, а также усиливать их экспертизу за счет глубокого понимания ландшафта угроз для защищаемой инфраструктуры». ***(Владимир Бахур. Group-IB вывела на рынок новый класс решений для охоты за хакерами и предотвращения кибератак // CNews (https://safe.cnews.ru/news/line/2020-11-26_groupib_vyvela_na_rynok_novyj). 26.11.2020).***

***

«Компания Zyxel Networks выпустила два межсетевых экрана USG Flex 100W и USG Flex 700 с версией микропрограммы ZLD 4.60, улучшающей возможности и быстродействие всей линейки шлюзов безопасности. Межсетевые экраны и версия микропрограммы улучшают возможности компаний среднего и малого бизнеса по внедрению гибкой системы безопасности для защиты от самых разнообразных киберугроз и непрерывного функционирования бизнеса в условиях пандемии.

Согласно недавно опубликованную отчету 2020 Threat Landscape report by Enisa, число кибератак продолжает увеличиваться по мере перехода компаний к новому этапу цифровой трансформации бизнеса. Пандемия Covid-19 ускорила цифровизацию, так как многим компаниям пришлось для продолжения бизнес-операций срочно переводить персонал на удаленный режим работы. Такая резкая смена практики ведения бизнеса значительно усложнила обеспечение защиты сетей компаний SMB, поскольку у большинства из них сильно ограничен бюджет на ИТ и ресурсы.

В качестве расширения модельного ряда, доступного для SMB, Zyxel представила два межсетевых шлюза безопасности из серии USG Flex: межсетевой экрана начального уровня со встроенной беспроводной точкой доступа USG Flex

100W и межсетевой экран старшего класса USG Flex 700, способный одновременно обслуживать до 800 подключенных клиентов. Межсетевые экраны серии USG Flex – это универсальные решения для бизнеса, которые не только обеспечивают надежную и масштабируемую систему защиты для сети предприятия, но и удаленный VPN доступ, управление точками доступа Wi-Fi и широкие возможности управления хот-спотами.

Микропрограмма ZLD 4.60, выпущенная Zyxel, обеспечивает увеличение производительности инспекции трафика SSL в 3-5 раз по сравнению с предыдущей версий прошивки. Такие показатели достигнуты в полевом тестировании межсетевых экранов Zyxel при использовании протокола HTTPS с настройками устройство по умолчанию: включенными функциями маршрутизации межсетевого экрана, NAT и ADP.

Это означает, что, используя уже имеющееся оборудование USG Flex, можно значительно ускорить шифрование/ дешифрование трафика и сократить задержки, связанные с генерацией сертификатов.

Усовершенствованная инспекция SSL также поддерживает новейшую версию протокола Transport Layer Security (TLS), используемого для защиты трафика между серверами и их клиентами. Поддержка протокола TLS 1.3 поможет пользователям Zyxel более эффективно отражать наиболее опасные кибератаки.

В дополнение к уже имеющимся сервисам репутации IP-адресов и URL-адресов в микропрограмме ZLD 4.60 реализован сервис репутации DNS на базе технологий McAfee. Эти три сервиса, используемые в продуктах серии Zyxel ATP, предоставляют комплексное надежное решение, которое предотвращает посещение пользователями скомпрометированных доменов, содержащих опасный контент, и блокирует доступ к определенным сайтам. Данные анализа от сервисов репутации можно легко просматривать в консоли Zyxel SecuReporter, поэтому сетевые администраторы всегда могут контролировать посещение пользователями подозрительных доменов, риски и типы запросов к поисковым службам». ***(Zyxel расширила линейку шлюзов безопасности для предприятий SMB // Компьютерное Обозрение (https://ko.com.ua/zyxel_rasshirila_linejku_shlyuzov_bezopasnosti_dlya_predpriyatij_smb_135376). 23.11.2020).***

***