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

№ 8 (серпень)

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– №8 (серпень) . – 150 с.

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

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

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

ЗМІСТ

Національна система кібербезпеки

«При Міністерстві енергетики України запрацював Проектний офіс з кібербезпеки. Відповідний наказ підписала в.о. міністра енергетики Ольга Буславець…

"При Міністерстві енергетики запрацював Проектний офіс з кібербезпеки. В.о. міністра енергетики Ольга Буславець підписала наказ щодо створення Проектного офісу з кібербезпеки для секторальної координації та залучення міжнародної технічної допомоги", - йдеться в повідомленні.

Як вказано, це перший крок, який "свідчить про серйозність ініціатив та намірів Міненерго щодо втілення плану короткострокових заходів для підвищення рівня стійкості кібербезпеки критичної інфраструктури енергетичного сектору".

"Для співпраці та партнерства з Проектним офісом запрошуються експерти у сфері кібербезпеки, представники громадських та експертних організацій, а також представники міжнародних компаній, які зможуть поділитися досвідом та надати технічну підтримку", - зазначили у міністерстві.

Там також нагадали, що перша зустріч підгрупи з кібербезпеки Секторальної робочої групи енергетичного сектору України Міністерства енергетики України відбулася 11 серпня…». ***(Ясамін Мохаммад. При Міненергетики запрацював проектний офіс із кібербезпеки // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1886902-pri-minenergetiki-zapratsyuvav-proektniy-ofis-iz-kiberbezpeki). 19.08.2020).***

***

Правове забезпечення кібербезпеки в Україні

«На экспертном совещании, состоявшемся в Кабинете министров Украины, обсуждались основные положения постановления Кабмина «Об утверждении Порядка отнесения объектов к объектам критической инфраструктуры» и «Об утверждении порядков по вопросам формирования перечня объектов критической информационной инфраструктуры, внесение объектов критической информационной инфраструктуры в государственный реестр объектов критической информационной инфраструктуры, его формирование и обеспечение функционирования».

Председатель Госспецсвязи Юрий Щиголь отметил, что эти два проекта нормативно-правовых актов являются выкристаллизованным единым видением профессионального сообщества на вопросы скоординированной политики в сфере защиты объектов критической и критической информационной инфраструктуры…

В свою очередь Александр Федиенко, заместитель председателя комитета цифровой трансформации Верховной Рады, отметил: “Действующий закон об

основных принципах обеспечения кибербезопасности достаточно рамочный, но не решает много вопросов, о чем мы уже много лет говорим. Хотя в то время он был крайне важным. Постановлени я, разработанные Государственной службой специальной связи и защиты информации Украины на основании указанного Закона, крайне необходимы".

Он, в частности, посоветовал убрать в постановлении критерий «влияние на доверие людей», поскольку такого критерия в соответствующей Директиве ЕС нет. Также, по его мнению, нужно четко понимать критерии региональные и местные. "Если с региональными это более или менее понятно, то вот локализация местных ОКИ и ОКИИ пока вопрос, как определить критерий", - пишет Федиенко.

По его словам, работа рабочей группы по вопросам кибербезопасности и критической инфраструктуры продолжит свою работу с сентября…

Требует пересмотра учет (реестр) таких объектов, чтобы было понятно, на кого будет возложена обязанность формирования реестра объектов критической инфраструктуры. Необходимо также решить формирование перечня информационно-телекоммуникационных систем (ИТС) объектов критической инфраструктуры. Многие другие вопросы уже перезрели и требуют законодательного определения и регулирования». ***(Герман Богапов. Кабмин: без перечня объектов критической инфраструктуры - нет кибербезопасности //Internetua (https://internetua.com/kabmin-bez-perecsnya-ob-ektov-kriticseskoi-infrastruktury-net-kiberbezopastnosti). 22.08.2020).***

***

«…З метою підвищення надійності та ефективності роботи платіжних систем правління Національного банку розробило проєкт постанови про затвердження положення "Про захист інформації та кіберзахист в платіжних системах", що пропонується для громадського обговорення. Зокрема, регулятор має намір встановити чіткі вимоги до учасників платіжного ринку щодо побудови системи захисту інформації та кібербезпеки, порядку дій при виявленні кібератак, що знижують надійність функціонування платіжних систем.

Нові вимоги поширюватимуться на платіжні організації платіжних систем, створені резидентами України, на операторів послуг платіжної інфраструктури, на учасників-резидентів платіжних систем, створених резидентами чи нерезидентами України. Зокрема, передбачається: впровадити ризик-орієнтований підхід до захисту інформації, в залежності від суми можливих збитків (вимоги до ключових учасників платіжного ринку будуть вищими), встановити вимоги до використання засобів захисту інформації, визначити політику управління доступом, створити передумови для мінімізації кількості шахрайських операцій, інцидентів інформаційної безпеки та кіберінцидентів у сфері переказу коштів, унеможливити порушення безперервності діяльності суб'єктів переказу коштів та підвищити захист користувачів платіжних послуг.

Зауваження і пропозиції до проєкту Нацбанк прийматиме до 7 вересня 2020 року». ***(Нацбанк посилить кіберзахист переказу коштів // Укрінформ (https://www.ukrinform.ua/rubric-economy/3079837-nacbank-posilit-kiberzahist-perekazu-kostiv.html). 12.08.2020).***

***

«НКЦК при РНБО України виявив ознаки підготовки до масштабної скоординованої атаки на органи державної влади України та об'єкти критичної інфраструктури напередодні Дня Незалежності. Про це повідомляє УНН із посиланням на пресслужбу Ради національної безпеки та оборони.

"Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України попереджає про активізацію хакерського угруповання Gamaredon, за яким стоять спецслужби Російської Федерації (РФ). Фахівці НКЦК при РНБО України виявили тенденцію до модернізації програмних засобів кібератак з метою підвищення ефективності подолання засобів захисту та приховування своєї діяльності у скомпрометованих системах", - йдеться у повідомленні.

Зазначається, що під час останніх спроб атак використовуються шкідливі вкладення, які імітують документи державних органів влади, зокрема, Служби безпеки України.

"Злочинці розсилають шкідливі документи електронною поштою, і під час їх відкриття хакери отримують доступ до систем та мереж державної установи. Фахівці НКЦК при РНБО України зазначають, що проведений аналіз шкідливих програм виявив ознаки підготовки до масштабної скоординованої атаки на органи державної влади та об'єкти критичної інфраструктури, спрямованої на дестабілізацію ситуації в Україні напередодні Дня Незалежності та під час підготовки до чергових місцевих виборів", - йдеться у повідомленні…». ***(Антоніна Карташева. РНБО виявив ознаки підготовки атаки на органи держвлади України до Дня Незалежності // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1886903-rnbo-viyaviv-oznaki-pidgotovki-ataki-na-organi-derzhvladi-ukrayini-do-dnya-nezalezhnosti). 19.08.2020).***

***

«З 5 по 11 серпня було зафіксовано та заблоковано 3 DDoS-атак, переважна більшість — на веб-ресурси Офісу Президента України. Про це повідомляє УНН із посиланням на пресслужбу Державної служби спеціального зв'язку та захисту інформації України.

"Система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала 64960 підозрілих подій, що на 34% менше, ніж попереднього тижня. Переважна більшість зафіксованих підозрілих подій стосується спроб мережевого сканування (84%) та застосування нестандартних протоколів (14%)", — йдеться в повідомленні.

Повідомляється, що система захищеного доступу державних органів до мережі Інтернет заблокувала 417 965 різних видів атак. Переважна більшість — це мережеві атаки прикладного рівня (99%).

“Також заблоковано 3 DDoS-атаки, переважна більшість — на веб-ресурси Офісу Президента України. Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 1227 кіберінцидентів, що на 63% менше, ніж попереднього тижня”, — зазначається в повідомленні.

Окрім того, переважна більшість опрацьованих інцидентів належить доменній зоні UACOM (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (98% від загальної кількості)…» ***(Анна Мурашко. За тиждень зареєстровано низку кібератак на сайт Офісу Президента // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1885469-za-tizhden-zareyestrovano-nizku-kiberatak-na-sayt-ofisu-prezidenta-ukrayini-2). 12.08.2020).***

***

«В Україні з початку 2020 року зафіксовано близько мільйона випадків, пов’язаних з кіберзагрозами, серед яких спроби WEB-атак, DDoS-атаки, поширення шкідливого програмного забезпечення…

Зокрема, як зазначається в повідомленні, Національний координаційний центр кібербезпеки при РНБО України (НКЦК) збирає інформацію про такі загрози від усіх державних суб’єктів кібербезпеки та аналізує її. Так у 2020 році в Україні було зафіксовано близько мільйона випадків, пов’язаних з кіберзагрозами. Серед них - мережеві атаки прикладного рівня, спроби мережевого сканування, спроби WEB-атак, фішинг, DDoS-атаки, поширення шкідливого програмного забезпечення тощо.

Для оперативного реагування на такі загрози та попередження можливих атак, НКЦК посилює співпрацю з компаніями з приватного сектору, підкреслили в РНБО.

Лише за останній місяць НКЦК підписав меморандуми про співпрацю з трьома десятками приватних іноземних та українських компаній. Такий меморандум передбачає обмін інформацією між НКЦК та окремою конкретною організацією про кіберзагрози та інциденти у сфері кіберзахисту для оперативного інформування, реагування, попередження можливих атак та взаємодопомоги у разі необхідності…» ***(В Україні за рік зафіксували близько мільйона випадків кібератак та кіберзагроз – РНБО // Укрінформ (https://www.ukrinform.ua/rubric-technology/3077451-v-ukraini-za-rik-zafiksuvali-blizko-miljona-vipadkiv-kiberatak-ta-kiberzagroz-rnbo.html). 07.08.2020).***

***

«У Telegram виявили бота, який поширює персональні дані 6 907 українських військовослужбовців. Про це повідомляє Офіс омбудсмена.

Зокрема, в таблиці, яку поширює бот, є інформація про ПІБ, номери військових частин та дати самовільного залишення військових частин.

Офіс омбудсмена звернувся до СБУ та Нацполіції лист, щоб вони відреагували і заблокували бота. Але відомо, що його досі не заблокували і він далі поширює особисті дані військових.

Нацполіція відкрила провадження за ч. 1 ст. 182 ККУ (Порушення недоторканності приватного життя)…». ***(Telegram-бот незаконно поширював особисті дані українських військових // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/25226/2020-08-07-telegram-bot-nezakonno-poshiryuvav-osobisti-dani-ukrainskikh-viiskovikh/). 07.08.2020).***

***

Боротьба з кіберзлочинністю в Україні

«Киберполиция совместно с компанией «Киевстар» заблокировала мошеннический ресурс. Злоумышленники создали фишинговый сайт, который внешне был похож на ресурс телекоммуникационной компании. Мошенники предлагали абонентам установить мобильное приложение для получения определенных бонусов. Однако в случае установления такого приложения они могли получить доступ к телефону и персональным данным пользователей.

Благодаря оперативной реакции киберполицейских и специалистов мобильного оператора указанный фишинговый ресурс заблокирован и приняты меры по недопущению доступа к персональным данным абонентов. Департамент киберполиции Национальной полиции Украины и Киевстар призывают абонентов всех мобильных операторов быть бдительными, чтобы не стать жертвами мошенников…». ***(Герман Богапов. Киберполиция заблокировала мошенническое мобильное приложение // Internetua (https://internetua.com/kiberpoliciya-zablokirovala-moshennicseskoe-mobilnoe-prilojenie). 12.08.2020).***

***

«Киберспециалисты и следователи Службы безопасности Украины разоблачили в Киеве участников организованной группы, которые пытались продать мощное специальное техническое средство негласного получения информации за почти полмиллиона евро.

По предварительным данным следствия, в состав группировки входило несколько жителей столицы, в том числе технические специалисты и специалисты сферы IT. Фигуранты, используя высокотехнологичное оборудование, нелегально разработали для продажи комплекс мониторинга мобильной связи. Устройство дает возможность снимать информацию во всех диапазонах мобильной связи, в частности, «прослушивать» телефонные разговоры и контролировать интернет-трафик.

Подпольную мастерскую они обустроили по месту жительства одного из фигурантов. Заказчика товара они подыскивали через личные связи.

Во время спецоперации оперативники СБУ задержали трех участников группы при получении от заказчика всей суммы денег.

В ходе обысков по месту жительства и работы фигурантов правоохранители изъяли оборудование и другие доказательства противоправной деятельности.

Сейчас всем задержанным сообщено о подозрении по ч. 2 ст. 359 (незаконное приобретение, сбыт или использование специальных технических средств получения информации) Уголовного кодекса Украины.

Продолжаются следственные действия для установления всех обстоятельств правонарушения и привлечения к ответственности других лиц, причастных к деятельности группировки». ***(Артем Сереженок. СБУ разоблачила айтишников, которые собрали и продавали шпионское оборудование // Internetua (https://internetua.com/sbu-razoblacsila-aitishnikov-kotorye-sobrali-i-prodavali-shpionskoe-oborudovanie). 13.08.2020).***

***

«Киберспециалисты Службы безопасности Украины совместно с киберподразделением Городской полиции Лондона и Национальным агентством по борьбе с преступностью (NCA) и другими компетентными органами Великобритании блокировали деятельность международной хакерской группировки.

Установлено, что группировка действовала с 2018 года и специализировалась на похищении персональных данных граждан Великобритании, США, стран Европы и СНГ для продажи на ресурсах «DarkNet».

Оперативники спецслужбы получили от британских партнеров информацию, что один из участников группировки проживает в Украине. Хакер разрабатывал и продавал на специализированных сайтах вирусные программы, которые обеспечивали несанкционированный доступ к компьютерным операционным системам по всему миру. С помощью вредоносной программы злоумышленники получали логины и пароли от Интернет-сайтов, электронных почтовых ящиков, данные кредитных карточек и электронных кошельков граждан. В дальнейшем похищенная информация использовалась для создания бот-сетей, осуществления DDoS-атак, похищения средств и персональной информации граждан.

В ходе следственных действий по месту жительства украинского хакера изъято более 20 терабайт информации с базами данных с компьютеров, которые были взломаны, а также исходные коды разработанного им вируса.

Злоумышленнику сообщено о подозрении по ч. 1 ст. 361-2 (несанкционированные сбыт или распространение информации с ограниченным доступом, которая сохраняется в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или на носителях информации) Уголовного кодекса Украины.

Ранее британские коллеги задержали его сообщника, который уже отбывает тюремное заключение за преступления в сфере кибербезопасности.

Продолжается досудебное следствие.

Разоблачение злоумышленника происходило совместно с Главным следственным управлением Национальной полиции Украины под процессуальным руководством Офиса Генерального прокурора». ***(Артем Сереженок. СБУ совместно с британскими партнерами блокировала деятельность международной хакерской группировки // Internetua (https://internetua.com/sbu-***

sovmestno-s-britanskimi-partnerami-blokirovala-deyatelnost-mejdunarodnoi-hakerskoi-gruppirovki). 19.08.2020).

***

«За допомогою «вірусу» фігурант отримував право керування закордонними інтернет-серверами. За такі дії зловмиснику загрожує до п'яти років ув'язнення.

Співробітники кіберполіції у Львівській області спільно зі слідчими поліції регіону та батальйоном поліції особливого призначення, під процесуальним керівництвом місцевої прокуратури, викрили 33-річного місцевого мешканця у розповсюдженні шкідливого програмного забезпечення.

Кіберполіція встановила місце знаходження сервера, з якого здійснювалося розповсюдження шкідливого програмного забезпечення. Захоплення здійснювалося шляхом підбору паролів та давало можливість зловмиснику отримати конфіденційну інформацію, що зберігалася на серверах.

Правоохоронці провели ряд обшуків та вилучили комп'ютерну техніку і мережеве обладнання. За результатами комп'ютерно-технічної експертизи на вилученій техніці виявлено шкідливе програмне забезпечення.

Фігуранту оголошено підозру у вчиненні правопорушення, передбаченого ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України. Максимальне покарання, яке загрожує зловмиснику – позбавлення волі на строк до п'яти років. Вирішується питання щодо обрання чоловіку запобіжного заходу.

Наразі кіберполіція встановлює можливих спільників фігуранта. Слідчі дії тривають». ***(Жителю Львівщини оголошено підозру у розповсюдженні шкідливого програмного забезпечення // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/zhytelyu-lvivshhyny-ogolosheno-pidozru-u-rozpovsyudzhenni-shkidlyvogo-programnogo-zabezpechennya-4881/). 19.08.2020).***

***

«19-річний хакер за допомогою створеного вірусу викрадав персональну інформацію користувачів Інтернету. Після розміщував цю інформацію на тематичних форумах. Таким чином фігурант хизувався технічними знаннями серед «однодумців».

Співробітники кіберполіції у Львівській області спільно зі слідчими поліції області та спецпризначенцями, під процесуальним керівництвом місцевої прокуратури, викрили чоловіка, який створював та розповсюджував шкідливе програмне забезпечення.

Кіберполіція встановила, що підозрюваний має відповідні технічні навички та володіє п'ятьма мовами програмування. Фігурант розробляв та поширював шкідливе програмне забезпечення, яке призначене для злому серверів, комп'ютерів та мобільних пристроїв.

Основною метою був збір персональних даних користувачів. Вірус фігурант маскував під файли, програми й розповсюджував його у месенджерах та соціальних мережах. Отриманими персональними даними він вихвалявся на хакерських форумах, де мав десятки облікових записів.

Правоохоронці провели обшук за місцем мешкання фігуранта та вилучили комп'ютерну техніку. Усі речові докази було направлено на експертні дослідження. За результатами експертизи виявлено зразки шкідливого програмного забезпечення.

Наразі чоловіку вже повідомлено про підозру за ч.1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України. Досудове розслідування триває». ***(Кіберполіція викрила хлопця у створенні та розповсюдженні шкідливого програмного забезпечення // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-xlopczya-u-stvorenni-ta-rozpovsyudzhenni-shkidlyvogo-programnogo-zabezpechennya-419/). 25.08.2020).***

***

«Служба безопасности Украины блокировала на Львовщине незаконную деятельность группы лиц, осуществлявших DDos-атаки на информационные ресурсы.

Специалисты по кибербезопасности СБУ установили, что хакеры разрабатывали и использовали вредоносное программное обеспечение для поражения компьютеров граждан для получения персональных данных. Злоумышленники в мессенджере «Телеграмм» через закрытые онлайн-каналы систематически размещали информацию, которую похищали у пользователей сети Интернет во время несанкционированного вмешательства в работу компьютеров и мобильных устройств.

Во время проведения следственных действий по месту жительства фигурантов дела правоохранители обнаружили и изъяли компьютерную технику и образцы вредоносного программного обеспечения.

В рамках уголовного производства по ч. 2 ст. 361 (несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи) и ч. 2 ст. 361-1 (создание с целью использования, распространения или сбыта вредоносных программных или технических средств, а также их распространение или сбыт) Уголовного кодекса Украины нескольким фигурантам сообщено о подозрении в совершении преступления.

Продолжаются следственные действия». ***(Артем Сереженок. СБУ блокировала деятельность группировки, которая занималась похищением персональных данных с помощью вирусов // Internetua (https://internetua.com/sbu-blokirovala-deyatelnost-gruppirovki-kotoraya-zanimalas-pohisxeniem-personalnyh-dannyh-s-pomosxua-virusov). 25.08.2020).***

***

«Секретар Ради національної безпеки і оборони України Олексій Данілов ознайомив надзвичайного і повноважного посла Королівства Нідерландів в Україні Йеннеса де Мола з роботою Національного координаційного центру кібербезпеки при РНБО України…

"Під час зустрічі Олексій Данілов повідомив Йеннессу де Молу, що з 2016 року НКЦК є ключовою державною структурою з виявлення, запобігання та реагування на кіберінциденти, а Указом Президента України... було суттєво посилено спроможності та покращено формат діяльності Центру", - йдеться у повідомленні.

За словами Данілова, НКЦК ефективно координує та контролює діяльність суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку у різних сферах – Держспецзв'язку, СБУ, Національної поліції, Національного банку, Генерального штабу ЗСУ та інших, а також залучає до діяльності кіберфахівців з приватного сектору.

"У цьому контексті, на думку Секретаря РНБО України, "спільні зусилля партнерів у кіберпросторі дають колосальний результат", тому поглиблення практичного співробітництва між Україною та Нідерландами у сфері протидії кіберзагрозам та відбиття кібератак, зокрема, з боку РФ, є вкрай нагальним та перспективним", - зазначається у повідомленні.

Окрім того, Данілов висловив подяку нідерландській стороні за незмінну і стійку підтримку України на її шляху до відновлення територіальної цілісності та суверенітету над тимчасово окупованими територіями.

"Своєю чергою, надзвичайний і повноважний посол Нідерландів в Україні відзначив прогрес та досягнення України у напрямі побудови потужної системи кібербезпеки. Пан де Мол підтримав позицію секретаря РНБО України щодо того, що гібридні загрози, зокрема, кібератаки на критичну інфраструкутру та цифрова пропаганда, сьогодні виходять на перший план, і взаємодія держав у цьому напрямку є важливою та необхідною", - йдеться у повідомленні…». ***(Анна Мурашко. Данілов обговорив із послом Нідерландів співпрацю в сфері кібербезпеки // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1886666-danilov-obgovoriv-iz-poslom-niderlandiv-spivpratsyu-v-sferi-kiberbezpeki). 18.08.2020).***

***

«Варшава буде одним з основних партнерів Києва щодо узагальнення досвіду і розробки інструментів стійкості для протидії гібридним загрозам, що здійснюватиметься у рамках Програми розширених можливостей НАТО.

Про це в інтерв'ю Укрінформу заявила віцепрем'єр-міністр з питань європейської та євроатлантичної інтеграції України Ольга Стефанішина.

За її словами, справді унікальна роль України як учасника Програми розширених можливостей має полягати в тому, щоб органічно структурувати

досвід України у боротьбі з гібридними загрозами. Це стосується інформаційних атак, кібербезпеки, захисту та обміну даними, протидії ворожим інформаційним кампаніям, пропаганді тощо.

“У взаємодії з РНБО України ми хочемо побудувати інституції, які узагальнюватимуть цей досвід і, відповідно, розробляти інструменти стійкості щодо цих гібридних загроз. Думаю, що Польща буде одним із наших головних союзників з накопичення цього досвіду і його реалізації в рамках Програми розширених можливостей”, - заявила Стефанішина.

Вона наголосила, що обговорила питання боротьби з гібридними загрозами з головою Бюро національної безпеки Польщі Павелом Солохом…». ***(Стефанішина: Польща буде одним із головних партнерів України з протидії гібридним загрозам // Укрінформ (https://www.ukrinform.ua/rubric-world/3082887-stefanisina-polsa-bude-odnim-iz-golovnih-partneriv-ukraini-z-protidii-gibridnim-zagrozam.html). 17.08.2020).***

***

«Секретар РНБО Олексій Данілов ознайомив послів Швеції та Фінляндії в Україні Тобіаса Тиберга та Пяйві Лайне з роботою Національного координаційного центру кібербезпеки (НКЦК) при РНБО.

Як передає Укрінформ, про це повідомляє пресслужба Радбезу.

Данілов наголосив, що у сучасному світі кібернетична та біологічна загрози стають страшнішими та небезпечнішими за ядерну зброю. "Сьогодні ми спостерігаємо за першою світовою біологічною війною, наслідки якої відчуває весь світ", - заявив він.

Сторони обговорили безпекову ситуацію в регіоні, зокрема в контексті врегулювання ситуації на Сході України, а також події в Білорусі.

Іноземні дипломати запевнили очільника РНБО у незмінності підтримки України на шляху до відновлення територіальної цілісності та суверенітету та висловили готовність до розширення співпраці у сфері кібербезпеки…» ***(Швеція і Фінляндія готові розширювати співпрацю з Україною у кібербезпеці — РНБО // Укрінформ (https://www.ukrinform.ua/rubric-society/3088191-svecia-i-finlandia-gotovi-rozsiruvati-spivpracu-z-ukrainou-u-kiberbezpeci-rnbo.html). 27.08.2020).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Исследователи компании Check Point Software Technologies фиксируют новую тенденцию атак – теперь хакеры все активнее используют тему вакцины от коронавируса. Основной вектор – электронная почта, 82% атак за последние 30 дней происходили через нее. Практически в каждом письме с подобными темами содержатся вредоносные ссылки. После перехода по ним жертвы загружают вредоносный файл, обычно в формате .EXE, .XLS или .DOC. С их помощью злоумышленники пытаются завладеть конфиденциальными данными пользователей – логины, пароли и т.п.

Количество новых доменов, связанных с коронавирусом и с вакцинами от него, удвоилось в июне и июле. При этом в целом количество атак, связанных с коронавирусом, значительно снизилось на общем фоне. В июле специалисты Check Point за неделю фиксировали в среднем около 61 тыс. атак, связанных с коронавирусом, что на 50% меньше, чем в июне». ***(Вместо коронавируса хакеры все активнее используют тему вакцины от него // Компьютерное Обозрение (https://ko.com.ua/vmesto_koronavirusa_hakery_vse_aktivnee_ispolzuyut_temu_vakciny_ot_nego_134135). 14.08.2020).***

***

«Согласно отчету Интерпола о влиянии пандемии COVID-19 на киберпреступность во всем мире, американские компании среднего размера активно становятся мишенью операторов программ-вымогателей LockBit.

Отчет был подготовлен Управлением по борьбе с киберпреступностью Интерпола и включает данные 48 стран-членов Интерпола и 4 частных партнеров, а также информацию и анализ отдела реагирования на киберпреступность (CTR) Интерпола и его Cyber Fusion Center (CFC).

«Полученный в результате анализ был дополнен информацией, предоставленной партнерами из частного сектора и региональными рабочими группами Интерпола по киберпреступности», - сообщает Интерпол.

Американские малые и средние предприятия на линии огня LockBit

В рамках краткого обзора региональных тенденций киберпреступности Международная организация уголовной полиции (Интерпол) сообщает [PDF], что «кампания вымогателей, проводимая в основном с помощью вредоносного ПО LOCKBIT, в настоящее время затрагивает средние компании в некоторых странах этого региона».

LockBit - это управляемая человеком операция «Программа-вымогатель как услуга» (RaaS), которая в сентябре 2019 года стала частной операцией, нацеленной на предприятия, а затем наблюдалась Microsoft при нацеливании на здравоохранение и критически важные службы.

Операторы этого штамма вымогателей используют общедоступный инструмент CrackMapExec для тестирования на проникновение, чтобы действовать горизонтально, как только они закрепляются в сети жертвы.

Два месяца назад LockBit объединился с операторами программ-вымогателей Maze, чтобы создать картель вымогателей, который позволяет им использовать одну и ту же платформу утечки данных во время своих операций и обмениваться тактиками и разведданными.

Позже Мейз сказал BleepingComputer, что другие группы программ-вымогателей могут присоединиться к этим совместным усилиям, чтобы генерировать выкуп.

Наиболее активные штаммы программ-вымогателей во время пандемии

Интерпол также внимательно изучил данные, предоставленные частными партнерами, чтобы получить обзор наиболее агрессивных банд вымогателей во время пандемии.

Согласно их анализу, CERBER, NetWalker и Ryuk были основными семействами программ-вымогателей, недавно обнаруженных частными партнерами Интерпола, и они рассматриваются как «постоянно развивающиеся, чтобы максимизировать потенциальный ущерб от одной атаки, а также финансовую прибыль для ее исполнителей».

«В первые две недели апреля 2020 года наблюдался всплеск атак с использованием программ-вымогателей со стороны нескольких групп угроз, которые были относительно бездействующими в течение последних нескольких месяцев», - добавил Интерпол.

«Это означает, что все еще могут быть организации, которые были заражены, но где программа-вымогатель еще не была активирована».

В связи с этим Интерпол упомянул ботнет Emotet (известный как вектор заражения программ-вымогателей) в части отчета, посвященной сбору данных о вредоносных программах, причем 13% организаций во всем мире затронуты этим вредоносным ПО.

Согласно отчету Интерпола, операторы программ-вымогателей также нацелены на европейские медицинские учреждения и критическую инфраструктуру, участвующие в реагировании на COVID-19.

Международная полицейская организация ранее предупреждала в апреле о всплеске атак с использованием программ-вымогателей, нацеленных на больницы и попыток заблокировать их доступ к критическим системам, хотя большинство из них уже были подавлены наплывом пациентов, вызванным продолжающейся пандемией.

Меры защиты от программ-вымогателей

Интерпол рекомендует организациям, подвергающимся атакам программ-вымогателей, поддерживать свое программное и аппаратное обеспечение в актуальном состоянии, а также выполнять резервное копирование данных с помощью автономных запоминающих устройств, чтобы блокировать доступ операторов программ-вымогателей и их шифрование…» ***(Sergiu Gatlan. Interpol: Lockbit ransomware attacks affecting American SMBs // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/interpol-lockbit-ransomware-attacks-affecting-american-smbs/). 04.08.2020).***

***

«Лаборатория Касперского» обнаружила новый Android-имплант, который известная группа кибершпионажа Transparent Tribe распространяет под видом приложения с контентом для взрослых, а также приложения о Covid-19 в Индии.

По мнению экспертов компании, это говорит о расширении поля деятельности Transparent Tribe и её актуальном курсе на пользователей мобильных устройств.

Первое приложение представляет собой видеоплеер, который при установке проигрывает ролики эротического характера. Другое, Aarogya Setu, имитирует мобильную программу для отслеживания COVID-19, разработанную Национальным центром информатики при правительстве Индии.

После скачивания оба приложения пытаются установить пакет Android с модифицированной версией AhMyth Android Remote Access Tool (RAT) — троянца с открытым исходным кодом для удалённого доступа к гаджету. Надо отметить, что модифицированная версия этого вредоноса отличается от стандартной: она включает в себя более продвинутые функции для кражи данных, однако исключает доступ к камере. В остальном троянец также позволяет атакующим производить на заражённых устройствах многочисленные действия: читать СМС-сообщения, просматривать журнал вызовов, манипулировать файлами на дисках, создавать скриншоты, прослушивать разговоры через встроенный микрофон и т.д.

«Эта активность подчеркивает усилия Transparent Tribe по добавлению в свой арсенал новых инструментов, открывающих перед ними ещё более широкие горизонты для атак. Мы также видим, что группа непрерывно совершенствует свои техники, — комментирует Юрий Наместников, руководитель российского исследовательского центра «Лаборатории Касперского». — В такой ситуации пользователям нужно быть предельно осторожными при оценке источников, из которых они загружают контент. В особенности это касается тех, кто знает, что может стать жертвой таргетированной атаки».

Группа Transparent Tribe также известна как PROJECTM и MYTHIC LEOPARD. Она проводит масштабные кампании кибершпионажа с 2013 года, а «Лаборатория Касперского» следит за её деятельностью с 2016 года. Подробная информация об индикаторах компрометации, относящихся к этой группе, включая хеши файлов и серверы C2, доступна на портале Kaspersky Threat Intelligence Portal». ***(Шпионское ПО для Android распространяется под видом контента для взрослых и приложения о Covid-19 // ООО "ИКС-МЕДИА (http://www.iksmedia.ru/news/5688401-Shpionskoe-PO-dlya-Android-rasprost.html). 27.08.2020).***

***

«ИТ-командам пришлось научиться быть динамичными, поскольку сотрудники продолжают менять стратегии, а COVID-19 затягивается.

Если вам кажется, что в наши дни вы постоянно пересматриваете черновик своей инструкции по кибербезопасности, это потому, что вы, вероятно, так и делаете.

До пандемии было достаточно сложно реализовать тщательный подход к кибербезопасности. Затем появился COVID-19 и заставил всех ваших сотрудников покинуть офис и вернуться в свои дома, вероятно, работая на личных устройствах и домашних сетях, которые - давайте посмотрим правде в глаза - вероятно, не видели смены пароля с момента первоначальной настройки. Теперь, когда многие из нас привыкли к рутине работы на дому, мы внезапно планируем вернуться в офис, в зависимости от вашей отрасли и вашего положения в мире. Пытаться придумать разумные меры безопасности, которые также помогут людям оставаться продуктивными, где бы они ни работали, - непростой подвиг.

Как профессионалы в области безопасности, наша задача - помогать пользователям - включая сотрудников, клиентов, поставщиков, поставщиков и партнеров - беспрепятственно получать доступ к ресурсам, необходимым им для

выполнения своей работы, будь то настольные компьютеры в офисе или мобильные устройства. COVID-19 ничего из этого не изменил, он просто усложнил задачу.

Итак, хотя первоначальная паника утихла, срыв продолжается. И, конечно же, мы всегда можем рассчитывать на киберпреступников, которые воспользуются ситуациями, когда наша защита наиболее уязвима. Еще в апреле Министерство внутренней безопасности (DHS) предупредило, что «группы APT используют пандемию COVID-19 в рамках своих кибероперациий. Эти субъекты киберугроз часто маскируются под доверенные лица. Их деятельность включает использование фишинговых сообщений на тему коронавируса или вредоносных приложений, часто маскирующихся под доверенные лица, которые могли быть ранее скомпрометированы».

Хорошая новость в том, что вы можете перестать сомневаться в каждом проекте своей инструкции по кибербезопасности, потому что мир и то, как мы к нему приспосабливаемся, меняется каждый день. Независимо от того, сколько сотрудников работает в офисе, дома или (возможно, когда-нибудь) в аэропортах и отелях, вот несколько эффективных и долгосрочных мер, которые вы можете сделать прямо сейчас, чтобы защитить свою организацию от фишинга и других кибератак (конечно, эти важны, даже если нет пандемии).

Перестаньте полагаться на пароли. В 2020 году сложно поверить, что украденные и ненадежные учетные данные по- прежнему являются причиной 80% утечек корпоративных данных, связанных с взломом. Если вы еще не начали, сейчас самое время применить многофакторную аутентификацию (MFA) для всех учетных записей пользователей. Подумайте о добавлении физического фактора, такого как YubiKey или надежных биометрических данных, которые устраняют необходимость в паролях и их намного сложнее подделать, чем одноразовые пароли (OTP).

Устраните пробелы в VPN и других инструментах удаленной работы. Увеличилась ли ваша мобильная инфраструктура с нескольких сотен до нескольких тысяч VPN-подключений за считанные дни (или часы)? Если это так, то хакеры использовали известные уязвимости в этих и других инструментах удаленной работы, таких как решения для удаленного рабочего стола и приложения для видеоконференцсвязи. В эпоху COVID-19 многие организации с меньшей вероятностью обновят свои VPN последними обновлениями безопасности и исправлениями, подвергая приложения и данные еще большему риску взлома.

Обучайте пользователей. Специалисты по безопасности все время говорят, что не следует полагаться на конечных пользователей в защите ваших ценных данных, и это все еще правда. Но обучение ваших мобильных сотрудников распознаванию некоторых из новейших методов фишинга может иметь большое значение для предотвращения следующей атаки на вашу организацию. Люди чувствуют себя особенно уязвимыми во время пандемии и, следовательно, более уязвимы для шквала фишинговых схем, связанных с пандемией. Используйте онлайн-тренинг по безопасности, чтобы научить мобильных пользователей, как избежать этих мошенников, особенно сейчас. Вот краткое руководство, чтобы начать работу.

Пусть все говорят. Легко захотеть использовать технологические решения для решения сложных проблем, и мобильная безопасность определенно может облегчить некоторые из наших самых больших головных болей, таких как угрозы устройств и сети. Но автоматизация не заменяет общение. Учтите, что только 51 процент технических специалистов и руководителей полностью уверены в том, что их группы по кибербезопасности готовы обнаруживать и реагировать на растущие атаки кибербезопасности во время COVID-19. Если вы один из тех профессионалов в области безопасности, которые сомневаются в способности вашей компании отражать кибератаки, особенно когда все работают удаленно, сейчас самое время высказаться. Ваша компания полагается на вашу команду по кибербезопасности, чтобы оставаться продуктивной, организованной и бдительной сейчас как никогда.

По мере того как мы все движемся вперед в неизведанное, мы должны планировать как на настоящее, так и на будущее. Единственный способ добиться этого - оставаться гибким, внимательным и постоянно пересматривать правила кибербезопасности, чтобы соответствовать беспрецедентным требованиям этого нового момента». ***(Brian Foster. How to Write a Cybersecurity Playbook During a Pandemic // Threatpost (https://threatpost.com/cybersecurity-playbook-during-pandemic/158538/). 26.08.2020).***

***

Світові тенденції в галузі кібербезпеки

«За последние несколько лет учебные заведения дополнительного образования вкладывают больше средств в обучение, продукты и услуги по кибербезопасности. Все больше колледжей используют сторонние сервисы для помощи в обнаружении угроз и управлении ими, и увеличилось количество тех, кто получил сертификаты Cyber Essentials.

Однако данные из центра безопасности Jisc (SOC) и Национального центра кибербезопасности NCSC) показали, что колледжи по-прежнему подвергаются атакам, и обеспокоенность по поводу растущей угрозы кибератак усилилась.

Атаки - факты

За последние несколько лет группа реагирования на инциденты компьютерной безопасности (CSIRT) Jisc, которая охватывает национальную исследовательскую и образовательную сеть, Джанет, обрабатывала от 5000 до 6000 инцидентов и запросов в год. График ниже показывает разбивку типов инцидентов, затрагивающих членов Jisc.

Эти статистические данные помогают проиллюстрировать широкий спектр инцидентов, произошедших в секторе образования; на реальные цифры сильно повлияла деятельность ДжанетCSIRTи обнаружение событий, а не их фактическая частота возникновения. Например, успешное расследование ботнета приведет к увеличению числа вредоносных программ за этот месяц, даже если вредоносное ПО могло быть активным, но не обнаруженным в предыдущие месяцы.

Хотя переход к удаленной работе для сотрудников и студентов изменил модель угроз, с которой сталкиваются колледжи, он не изменил того факта, что

безопасность остается приоритетной задачей. Преступники печально известны тем, что пользуются новостями и совмещают возникающие и актуальные проблемы, и текущая ситуация с COVID-19 ничем не отличается.

Фишинг

Вскоре после появления новостей о кризисе атаки начали адаптироваться, чтобы использовать преимущества нового контекста. Фишинговые электронные письма всегда были проблемой, и тем более, поскольку преступники используют электронные письма, связанные с коронавирусом, чтобы побудить жертв переходить по ссылкам или загружать вредоносное ПО.

NCSC предупредил общественность об этом в апреле этого года. Хотя Джанет не связана с COVID-19CSIRTнедавно пришлось отреагировать на несколько чрезвычайно серьезных инцидентов с программами-вымогателями. Это включало один колледж, которому пришлось закрыть все свои системы более чем на неделю. Со всеми инцидентами, и особенно примерами, разрушающими бизнес, как этот, Джанет раньшеCSIRT свяжется, может быть более эффективной цифровой криминалистической экспертизы, и более быстрое может быть возобновлено нормальное обслуживание.

Атаки отказа в обслуживании

За последние 12 месяцев Jisc обнаружил 569 атак типа «отказ в обслуживании» (DDoS) против колледжей в Англии, что более чем на 10% выше, чем за предыдущий 12-месячный период. Однако, глядя на статистику с начала блокировки до момента написания (с 20 марта по 20 мая 2020 г.), мы обнаружили 26DDoS атак на 15 колледжей Великобритании, что меньше, чем за тот же период в 2019 г. (100 DDoS нападения на 33 колледжа Великобритании).

Номер DDoS атаки в марте и апреле в течение обоих лет были довольно схожими, но в мае наблюдалось значительное снижение: с 1 по 20 мая 2019 года было зарегистрировано 47 атак и всего пять за тот же период в этом году.

Джанет CSIRT сильно подозревает, что большая часть DDoS атаки происходят изнутри колледжей.

Еще слишком рано определять, связано ли это с изоляцией, изменяющей способ работы всех (включая преступников), или это аномалия. Судя по предыдущему анализу атак, и когда нам удалось поработать с колледжами для выявления преступников, ДжанетCSIRT сильно подозревает, что большая частьDDoS атаки происходят изнутри колледжей.

Поскольку многие системы размещены в облаке, а не в университетском городке, а ресурсы и системы доступны непосредственно из домашних сетей, потенциально меньше пользы от запуска атаки отказа в обслуживании против сети колледжа во время блокировки.

В одном примере аналитики безопасности Jisc смягчали атаку в колледже, которая была запущена примерно в 09:00. Он закончился в 12:00, а затем снова заработал в 13:00 и закончился во второй половине дня. Это наводило на мысль, что злоумышленник был кем-то в университетском городке, который хотел выйти в Интернет в обеденное время. Jisc SOC также обнаружил доступ из колледжей к веб-сайтам, которые предоставляют «атаки как услугу»: так называемые сайты

Booter и Stresser позволяют злоумышленникам запускатьDDoS нападения на любую организацию всего за несколько фунтов.

Профилактика

Если другие колледжи подпишутся на службу распознавания сети Janet Network (JNRS) Jisc, то мы сможем предотвратить доступ к таким сайтам из сети колледжа. JNRS также может помочь снизить риск того, что веб-запросы пользователей будут направлены на взломанные или опасные веб-сайты (например, в результате фишинга или связанных атак).

Также важно, чтобы колледжи вели соответствующие журналы в своих системах, чтобы помочь идентифицировать злоумышленников и определить, чем они занимались. Когда в колледже происходит киберинцидент, его сотрудники могут позвонить Джанет.CSIRTдля оказания помощи. Это может включать в себя предоставление рекомендаций и рекомендаций по электронной почте или по телефону, но довольно часто влечет за собой подробное расследование. Это может включать в себя цифровую криминалистику, чтобы определить, что именно произошло, и, например, как злоумышленник смог получить доступ.

Эта команда помогает сотрудникам учреждений восстановить работу систем, чтобы преподавание и обучение продолжались. BCSIRT team также проактивно связывается с колледжами при обнаружении инцидентов или при получении предупреждений о конкретной угрозе.

Отношение к риску

70% респондентов (до COVID-19) AoC/ Jisc College IT-опрос показал, что они либо согласны, либо полностью согласны с тем, что их колледж способен справиться с риском кибербезопасности. Это даже более уверенный ответ, чем было отмечено в обзоре состояния кибербезопасности Jisc за 2019 год, где средний балл 6,6 / 10 был дан в ответ на вопрос по шкале от 1 (совсем плохо) до 10 (очень хорошо защищен). насколько хорошо вы считаете, что ваша организация защищена? ' Почти четверть респондентов дали оценку 8/10 и выше.

Хотя Jisc был свидетелем передовой практики в некоторых колледжах, такой как хорошие процессы и политики, включая политики исправлений, как и во всех организациях, есть выбор, который следует сделать в отношении того, что является приоритетом.

Есть некоторые опасения, что не все колледжи осведомлены о спектре угроз и что об инцидентах не сообщается.

Существует некоторая обеспокоенность тем, что не все колледжи осведомлены о спектре угроз и что об инцидентах не сообщается: более половины колледжей заявили в опросе 2019 года, что они не сообщали об инцидентах кибербезопасности в предыдущие 12 месяцев. вAoC/ Jisc IT-опрос: 11% колледжей сообщили, что столкнулись как минимум с одним инцидентом кибербезопасности, который привел к серьезным сбоям в работе, и почти все (96%) испытали хотя бы один незначительный инцидент.

Ресурсы и экспертиза

В очень немногих колледжах есть специализированный персонал по кибербезопасности. Фактически, только 11% респондентов опроса 2019 года заявили, что у них есть определенные роли в сфере безопасности. У многих есть

небольшие команды с широким кругом обязанностей, что означает, что они не могут делать все, поэтому им приходится расставлять приоритеты. Это может означать, что игнорируются важные векторы атаки.

Хорошее использование технологий или работа с надежным партнером могут помочь. Хотя внедрение систем безопасности информации и управления событиями (SIEM) находится на низком уровнеFEв настоящее время (4% согласно опросу 2019 года) наличие централизованного места для регистрации информации из разрозненных систем помогает сэкономить время при ручном поиске признаков атаки и может предупреждать команды при обнаружении чего-то подозрительного. Точно так же, если уже известно, какие активы подключены к сети, легче эффективно управлять угрозами.

Из результатов опроса Jisc 2019 года мы знаем, что все большее количество колледжей обеспечивают наличие базовых средств контроля безопасности, получая правительственный сертификат Cyber Essentials . Результаты опроса 2019 года показали значительный скачок с 4% колледжей в 2018 году до 31%. Мы ожидаем, что эта цифра еще больше увеличится в опросе этого года, поскольку колледжи стремятся выполнять требования к безопасности данных в финансовых соглашениях Агентства по финансированию образования и повышения квалификации.

Культура и обучение

Кибербезопасность - это одновременно технологический и культурный вопрос. Наличие технических средств контроля для обеспечения актуальности систем, исправлений, сканирования уязвимостей и т. Д. Является ключевым моментом, равно как и обучение и осведомленность пользователей. Обнадеживает то, что все больше колледжей обучают своих сотрудников: с июня 2019 года 55% сообщили об обязательном обучении для некоторых или всех своих сотрудников, до 67% вAoC/ Jisc IT-опрос в декабре.

Обеспечение осведомленности сотрудников и учащихся об опасности фишинга и вредоносных программ, а также о необходимости резервного копирования их данных становится еще более важным при нынешних способах работы.

Однако число учащихся, сообщивших об обучении, не столь положительно: с чуть менее четверти в июньском опросе до 27% в декабре. Обеспечение осведомленности сотрудников и учащихся об опасности фишинга и вредоносных программ, а также о необходимости резервного копирования их данных становится еще более важным при нынешних способах работы.

Обучение осведомленности о кибербезопасности должно проводиться для всех сотрудников организации; Очень важно убедить совет и директоров поддержать стратегию кибербезопасности колледжа и внедрить ее во всей организации.

Постройте сильную оборону

Удаленная работа из-за COVID-19 изменила ландшафт угроз, но по-прежнему означает, что необходимо проводить базовые меры безопасности и обучение. Злоумышленникам нужно найти только одну уязвимость, чтобы воспользоваться ею, поэтому чем больше внимания будет уделяться сети, тем

больше шансов заблокировать эти уязвимости до того, как злоумышленники войдут в нее или очень скоро.

Злоумышленникам нужно найти только одно слабое место, чтобы использовать его, поэтому чем больше внимания будет уделяться сети, тем больше шансов заблокировать эти слабые места до того, как злоумышленники проникнут внутрь.

Хотя ни одно учреждение не застраховано от кибератак, необходимо принять ряд мер, чтобы сделать колледжи более сложной целью и минимизировать воздействие атаки или взлома. Колледжи должны гарантировать, что системы исправлены и поддерживаются в актуальном состоянии; сети должны быть сегментированы; все пользователи должны пройти обучение по вопросам информационной безопасности; и следует рассмотреть возможность внедрения SIEM либо внутри компании, либо через управляемую службу, чтобы обеспечить максимальную прозрачность.

Jisc очень заинтересован в сотрудничестве с учреждениями, чтобы улучшить их положение в области кибербезопасности и гарантировать, что ни один колледж или их студенты не останутся без внимания, когда дело доходит до передовых методов безопасности». ***(John Chapman. Cyber security in FE: what are the threats and how do we deal with them? // Joint Information Systems Committee (https://www.jisc.ac.uk/news/cyber-security-in-fe-what-are-the-threats-and-how-do-we-deal-with-them-05-aug-2020). 05.08.2020).***

***

«…Незважаючи на те, що горизонти цифрових загроз постійно розширюються, ключовим елементом пазлу кібербезпеки залишаються кінцеві точки (endpoints). Це пристрої користувачів, приєднані до мережі компанії, кожен з яких може бути використаним для розкриття даних організації. Якщо проаналізувати типові офісні конфігурації, виявиться, що кінцеві точки досить легко відстежити – це комп'ютери, мобільні пристрої, сервери, смарт-пристрої тощо. З усіма цими пристроями під одним дахом та за допомогою IT відділів в офісі організації можуть забезпечити належні практики щодо кіберзахисту, залишаючись поза ризиками.

Але небачене збільшення кількості віддалених робітників руйнує цей баланс. Чим більше кінцевих точок, тим складнішим повинен бути підхід до безпеки. Разом з мільйонами працівників, які підключають ноутбуки та мобільні пристрої до своїх мереж, за експонентною зростають і кіберризики. Більшість персональних пристроїв не мають тих засобів захисту, якими оснащені пристрої компанії. Крім того, багато компаній навіть не підозрюють, які пристрої підключені до їхніх систем. Обізнаність щодо наявності та місцезнаходження ваших активів, а також щодо захисту, якого вони потребують, – це основа захищеності компанії. Великий ризик для компанії становить і те, що деякі працівники не розуміють природу кіберзагроз й не усвідомлюють, що певні їхні дії можуть створити одну з них.

У міру того, як компанії пристосовуються до цього безпрецедентного виклику, їхні керівники повинні відповісти на три основні питання:

– чи може моя компанія виявляти та реагувати на кіберзагрози, а також відновлюватися після кіберінцидентів, і як кожна з цих здатностей змінюється щодо загроз, пов'язаних з віддаленою роботою;

– які активи є критичними для нашої компанії (що нам потрібно захистити – інформацію клієнтів, інтелектуальну власність, важливі апаратні системі тощо);

– чи є в моїй компанії культура кіберзахисту і чи навчені наші співробітники розпізнавати кіберінциденти й запобігати їм незалежно від їхнього робочого місця.

Підвищення рівня кіберобізнаності серед працівників

Багато організацій мають політики безпеки та можливості керувати популярними загрозами, тому більшість піде простим шляхом підтримки вже наявних систем. Однак цього може бути недостатньо для стримування ризиків, перелік яких постійно поповнюється. Приміром, з 13 по 26 березня цього року було виявлено понад 400 тис. фішингових листів на тему COVID-19 (PDF, EN). У відповідь на таку статистику американські й британськи органи розвідки опублікували спільне повідомлення, в якому попереджають про дії кіберзлочинців, які, використовуючи пандемію, націлили на компанії та окремих користувачів своє зловмисне програмне забезпечення.

Один клік працівника може становити загрозу для даних усієї компанії, тому організаціям вкрай необхідно переоцінити всі існуючі кінцеві точки на предмет вразливостей. Також належним чином повинні бути захищені всі нещодавно прийняті хмарні рішення та інструменти для відеоконференцій. Без ефективного контролю (PDF, EN) безпеки кіберзлочинці можуть приєднуватися до ділових зустрічей та/чи мати доступ до конфіденційної інформації, що зберігається у хмарних сервісах.

Ключовим фактором успішної екосистеми віддаленої роботи є розуміння працівників їхньої ролі у забезпеченні кібербезпеки. Особиста відповідальність та обізнаність – важливі складники програми кіберризиків кожної організації. Командам, що спеціалізуються на кіберзахисті, потрібно співпрацювати з керівництвом для заохочення комунікації та навчання кращих практик і політик кібербезпеки компанії, а також планів щодо реагування на інциденти. Щоб мати можливість швидше і стійкіше реагувати на кібератаки, необхідно:

– розробити й застосовувати план реагування на кіберінциденти для навчання і тренування працівників. Це допоможе запобігти кібер-інцидентам та уникненню поширення дезінформації;

– підвищити обізнаність працівників про кіберзагрози від фішинг-кампаній в електронних листах, де можуть вимагати гроші;

– вимкнути непідтверджені персональні пристрої з корпоративних мереж і переконатися, що програмне забезпечення корпоративного захисту встановлено на затверджених пристроях до їх підключення у мережу.

Прийняття «кіберреальності»

Криза COVID-19 спричинила кризу в багатьох компаніях, і тепер вони змушені переключитися на режим 'new normal'. Оскільки мільйони співробітників працюють з дому, керівники підприємств хочуть зосередитися виключно на підтримці операційної спроможності та функціональності за будь-яку ціну. Однак, якщо кібербезпека не буде вбудована у їхні плани відновлення після COVID-19,

організації можуть бути серйозно скомпрометовані в короткостроковій перспективі й мають ризик не встояти у світі, де всі готові до нових викликів чи можливостей. Зараз організаціям як ніколи важливо зрозуміти, що кібертехнології скрізь, тому треба розглядати їх як ланцюг, що об'єднує їх організацію, клієнтів, постачальників та громади, дозволяючи інтегрувати кібераспекти у стратегічні рішення, які організації приймають щодня.

У своїй більшості вимушене застосування політик роботи з дому підштовхнуло до цифрового перетворення. Можливо, цей період спричинить нову епоху роботи, де кордони між роботою в офісі та з дому зітруться остаточно. Організації, для яких кібербезпека є одним із пріоритетів, будують для себе хороший фундамент на місяці й навіть роки вперед». ***(Емілі Моссбург. Нові аспекти кібербезпеки в умовах віддаленої роботи // Компьютерное Обозрение (https://ko.com.ua/novi_aspekti_kiberbezpeki_v_umovah_viddalenoyi_roboti_133984). 04.08.2020).***

***

«Microsoft провела исследование крупных компаний в Индии, Германии, Великобритании и США для того, чтобы выявить изменения, произошедшие в первые два месяца пандемии в области цифровой трансформации и информационной безопасности.

Результаты исследования отразили пять основных трендов в области кибербезопасности:

Безопасность - основа для обеспечения продуктивности в эпоху цифровых технологий. Повышение производительности во время удаленной работы является основным приоритетом руководителей бизнес-подразделений по обеспечению ИБ (41%), а “распространение технологий защиты данных на большее количество приложений для удаленной работы” респонденты назвали самым положительным явлением для пользователей в этой области. Неудивительно, но “предоставление безопасного удаленного доступа к ресурсам, приложениям и данным” одновременно является и самой сложной задачей. Большинство опрошенных компаний в качестве первого шага на пути к этой цели назвали внедрение системы многофакторной аутентификации.

Все находятся на пути к концепции «Никому не доверяй» (Zero Trust). Концепция в первые же дни пандемии из интересной возможности превратилась в бизнес-приоритет. В свете перехода на удаленную работу 51% руководителей в сфере ИБ ускоряют развертывание архитектуры Zero Trust. В результате концепция может стать отраслевым стандартом, поскольку 94% компаний сообщают, что они в той или иной степени уже внедряют элементы Zero Trust.

Больше различных наборов данных - больше информации о возможных угрозах. Пандемия позволила оценить возможности облачных технологий. Компания Microsoft ежедневно отслеживает более 8 триллионов сигналов об угрозах из самых разных источников (продуктов, сервисов, подписок на индикаторы компрометации и т.д.) по всему миру. Автоматизированные инструменты помогли специалистам по безопасности выявлять новые угрозы до того, как они достигнут клиентов - иногда за доли секунды. Облачные фильтры и

средства обнаружения угроз также позволили предупреждать службы безопасности о подозрительном поведении, что было крайне актуальным для бизнеса, поскольку 54% руководителей служб безопасности сообщили об увеличении количества фишинговых атак с начала пандемии. Об успешных фишинговых атаках значительно чаще сообщали компании, которые описали свои ресурсы как преимущественно локальные (36%), по сравнению с 26% в компаниях, которые опираются на облачную инфраструктуру.

Кибербезопасность является основой для операционной отказоустойчивости. Поскольку все больше организаций предоставляют сотрудникам решения безопасной удаленной работы. Облачные технологии упрощают разработку комплексной стратегии обеспечения защиты и непрерывности бизнеса в условиях активных киберугроз (киберустойчивости) и подготовку к широкому спектру непредвиденных обстоятельств. Более половины компаний, использующих облачные или гибридные технологии, сообщают о наличии стратегии киберустойчивости для большинства сценариев, по сравнению с 40% организаций, опирающихся на локальную инфраструктуру, из которых 19% вообще не имеют такого плана в документированном виде.

Облако является необходимым условием эффективного обеспечения безопасности. В то время как специалисты часто думали о безопасности как наборе решений для развертывания поверх существующей инфраструктуры, такие события, как масштабный переход на удаленную работу, демонстрируют необходимость внедрения систем интегрированной безопасности для компаний любого размера.

Помимо этого, с момента начала пандемии более 80% компаний нанимали специалистов в сфере безопасности. Большинство руководителей служб информационной безопасности сообщили об увеличении бюджета на ИБ (58%) и соответствие нормативным требованиям (65%), чтобы адаптироваться к многочисленным последствиям пандемии для бизнеса.

В то же время 81% из них также сообщили о необходимости снизить затраты на ИБ компании в целом. Чтобы сократить расходы в краткосрочной перспективе, руководители работают над улучшением систем интегрированной защиты от угроз для значительного снижения риска ущерба от кибератак. Почти 40% предприятий заявляют, что в долгосрочной перспективе отдают предпочтение инвестициям в облачную безопасность, за которыми следуют безопасность данных и информации (28%) и антифишинговые инструменты (26%)». ***(Глобальные тренды в сфере кибербезопасности в первые месяцы пандемии // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5687222-Globalnye-trendy-v-sfere-kiberbezop.html). 20.08.2020).***

***

«Один из крупнейших регистраторов доменов в мире, Namecheap, сегодня пострадал от серии загадочных сбоев, и непонятно почему.

Компания с более чем 11 миллионами зарегистрированных пользователей и 10 миллионами доменов предлагает регистрацию доменов, хостинг, частные

почтовые услуги и сертификаты TLS / SSL и стала одним из самых узнаваемых имен в отрасли.

Я заметил это еще в 2:00 утра по восточному времени (7:00 утра по британскому времени), когда безуспешно пытался зайти на свой веб-сайт через смартфон. «Может быть, плохой сигнал WiFi, - подумал я сначала.

Учитывая, что большинство услуг виртуального хостинга обеспечивают не более 99,9% гарантии безотказной работы, я списал это на очередное плановое обслуживание.

Множественные загадочные отключения

При переходе на страницу статуса сервиса Namecheap мы видим 4 сообщения с сегодняшнего дня, только 30 августа.

1. Регистрация доменов: самое первое предупреждение о сбое в работе службы. получившее название «внеплановое обслуживание», было выпущено сегодня в 3:41 утра по восточному времени в отношении регистрации доменов. Пользователи, пытающиеся зарегистрировать определенные домены TLD, испытывали проблемы. В 6:00 утра по восточному времени компания объявила в том же предупреждении, что они устранили проблему, только чтобы повторно открыть предупреждение в 7:05 из-за постоянных ошибок, которые все еще действуют.

«Невыполненные заказы будут возвращены источнику оплаты или на баланс вашего аккаунта Namecheap, чтобы вы могли повторно отправить заказ».

2. Регистрация доменов ccTLD . Второе предупреждение было отправлено в 6:59 по восточноевропейскому времени и касалось регистрации доменов для конкретных стран для TLD .me, .cc и .tv .

В 7:30 утра по восточному времени предупреждение гласило:

«Проблема с доменами .cc и .tv решена. Мы все еще ждем обновлений от нашего вышестоящего партнера относительно доменных имен .me ».

3. Частная электронная почта и веб-сайт Namecheap. Примерно в 8:27 по восточноевропейскому времени перерыв в работе самого домена Namecheap.com и его частных почтовых служб. Это предупреждение было закрыто в 9:20 по восточному времени, но без разрешения. Он был объединен с четвертым предупреждением:

4. Общий хостинг, личная электронная почта, VPS-серверы, инфраструктура WordPress ... в основном все не работает: последнее предупреждение, выпущенное в 8:29 утра по восточному времени, которое остается в силе, продлевая этот сбой, подробно описывает несколько продуктов, которые в данный момент недоступны. Нет ETA относительно того, когда эти проблемы будут решены.

«С сожалением сообщаем вам, что namecheap.com, общие серверы, реселлер, VPS, EasyWP и службы частной электронной почты испытывают временные проблемы с сетевым подключением в настоящий момент. Наши технические специалисты работают над этой проблемой и делают все возможное, чтобы сократить время простоя, "гласит предупреждение.

«Ошибка «Тайм-аут соединения» может отображаться при попытке доступа к серверу (при открытии веб-сайта, использовании службы электронной почты, FTP и т. Д.)»

На момент написания, последнее обновление предупреждения поступило с 9:27 утра по восточному времени и сообщает:

«Вся наша команда продолжает работать трудно иметь вопрос будет решен как можно скорее. К сожалению, нет ETA сейчас. Большое спасибо за ваше терпение.»

Тайм-ауты, связанные с определенным геолокацией

В некоторых частях мира пользователи по-прежнему сталкиваются с проблемами при доступе к доменам, размещенным на Namecheap.

В наших тестах BleepingComputer мог получить доступ к доменам, размещенным, включая мой собственный, на общих серверах Namecheap из США, даже через VPN. Однако домены приводили к тайм-аутам при доступе из Великобритании, Канады, Мексики и других регионов.

Выполнение диагностического теста traceroute на моем домене, например, из Великобритании, показало таймауты, причем последней точкой отказа был IP-адрес, принадлежащий NTT (192.80.17.102).

Тот же самый тест ранее показал конечную точку отказа как IP-адрес 4.68.73.226, принадлежащий Level3 (CenturyLink). Вероятно, это связано с отключением Level3, происходящим сегодня.

Это правдоподобно из-за того, что промежуточные маршрутизаторы из-за длительного простоя решили использовать IP-адреса NTT на пути к службам Namecheap, в отличие от Level3.

Несколько пользователей жалуются

Twitterverse быстро реагирует на отключение, которое началось где-то посреди ночи для тех, кто базируется в Северной Америке.

Другой пользователь Исаак Гарсия спросил компанию: «Службы @Namecheap не работают, ни мои домены, ни служба поддержки не работают, у вас есть примерное время для решения? Согласно вашему журналу состояния проблемы начались с незапланированного обслуживания»…

Хотя компания изучает проблему, и мы еще не уверены, что именно ее вызывает, кажется странным, что сразу несколько систем уважаемого хоста и регистратора выходят из строя.

Более того, упоминание «внепланового технического обслуживания» в самом первом предупреждении тоже вызовет у вас тревогу.

Это развивающаяся история, которая будет обновляться по мере поступления дополнительной информации.

Обновление: Namecheap решил некоторые проблемы. Пользователям рекомендуется регулярно проверять страницу обновлений статуса». ***(Ax Sharma. Namecheap hosting and email DOWN in prolonged outage // Bleeping Computer® (https://www.bleepingcomputer.com/news/technology/namecheap-hosting-and-email-down-in-prolonged-outage/). 30.08.2020).***

***

«Эксперты компании Positive Technologies поделились результатами анализа киберинцидентов за второй квартал 2020 года. Исследование показало, что доля атак на промышленность существенно выросла по

сравнению с предыдущим кварталом, 16% фишинговых атак были связаны с темой COVID-19, а среди общего объема данных, похищенных в атаках на организации, доля учетных данных выросла вдвое.

По данным исследования, число атак во II квартале выросло на 9% по сравнению с первым кварталом и на 59% по сравнению с аналогичным периодом 2019 года. По мнению экспертов, громкие мировые события неминуемо сопровождаются ростом числа кибератак, поскольку создают благоприятную почву для применения злоумышленниками методов социальной инженерии. Апрель и май 2020 года стали рекордными по числу успешных кибератак. Эксперты связывают это со сложной эпидемиологической и экономической ситуацией в мире, которая пришлась на эти месяцы. Так, во втором квартале 2020 года с темой COVID-19 было связано 16% атак с использованием методов социальной инженерии (против 13% в первом квартале). Более трети (36%) из них не были привязаны к конкретной отрасли, 32% атак направлены против частных лиц, 13% — против госучреждений.

Существенно выросла доля атак, направленных на промышленность. Во II квартале среди атак на юридические лица она составила 15% против 10% в I квартале. Наибольший интерес к промышленности проявляют операторы шифровальщиков и кибершпионские APT-группы. Во II квартале стало известно о первых жертвах шифровальщика Snake — автомобильном производителе Honda и гиганте ТЭК, компании Enel Group. Кроме Snake, промышленность атаковали операторы шифровальщиков Maze, Sodinokibi, NetWalker, Nefilim, DoppelPaymer. При этом начальным вектором проникновения в атаках на промышленность были фишинговые письма (83% от общего числа атак) и уязвимости на сетевом периметре (14%).

По данным экспертов, во II квартале доля учетных данных выросла с 15% до 30% от общего объема данных, украденных у организаций. По словам аналитика Positive Technologies Яны Авезовой, особо ценятся корпоративные учетные данные сотрудников. Их злоумышленники продают в дарквебе или используют для дальнейших атак, например для рассылки писем с вредоносными вложениями от имени взломанных организаций. Спросом пользуются также базы учетных данных клиентов взломанных компаний. Жертвами во II квартале преимущественно становились онлайн-сервисы, интернет-магазины и организации сферы услуг. Как правило, в ходе атак на эти компании злоумышленники эксплуатировали веб-уязвимости или подбирали пароли для доступа к сайтам. Среди других наиболее распространенных сценариев похищения данных — рассылка фишинговых писем и заражение вредоносным ПО.

«Что касается фишинговых атак с целью кражи учетных данных, надо отметить, что, как правило, злоумышленники подделывают формы аутентификации продуктов Microsoft: Office 365, Outlook, SharePoint, — отмечает Яна Авезова. — Однако во II квартале на фоне пандемии наблюдались также атаки, направленные на кражу учетных данных для подключения к системам аудио- и видеосвязи, как в случае с фишинговой кампанией, направленной на удаленных сотрудников, использующих Skype, когда злоумышленники рассылали письма с фейковыми уведомлениями от сервиса. Получатель, перейдя по ссылке из письма, попадал на поддельную форму аутентификации, где его просили ввести логин и пароль от

Skype. Подобные атаки во II квартале зафиксированы также на пользователей платформ Webex и Zoom». ***(Positive Technologies: в киберпреступном мире растет спрос на учетные данные // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/v-kiberprestupnom-mire-rastet-spros-na-uchetnye-dannye/). 26.08.2020).***

***

Сполучені Штати Америки

«…Державний департамент США заплатить до $10 млн за інформацію про іноземних хакерів, які намагатимуться втручатись у вибори в США у листопаді 2020 року. Про це заявив держсекретар США Майк Помпео під час брифінгу…

Для цього Держдепартамент США розробив спеціальну програму під назвою «Нагорода за справедливість». Цю ініціативу підтримала Служби дипломатичної безпеки США.

За даними американської розвідки, Росія вже намагалась втручатись в вибори в США на користь Дональда Трампа. Також російські спецслужби намагались втрутитись у праймеріз Демократичної партії на боці Берні Сандерса…». ***(Влада США пропонує $10 млн за інформацію про втручання хакерів в вибори // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/25214/2020-08-06-vlada-ssha-proponue-10-mln-za-informatsiyu-pro-vtruchannya-khakeriv-v-vibori/). 06.08.2020).***

***

«Пандемия, протесты в США и скандалы из-за выборов создали идеальные условия для распространения дезинформации в социальных сетях. Для борьбы с ней используются различные фактчекинг-инструменты на базе искусственного интеллекта, но эта технология все еще далека от совершенства.

Недавно Twitter пометил одно из сообщений Дональда Трампа как содержащее недостоверные данные. Из-за этого многие задались вопросом, должны ли соцсети вообще заниматься фактчекингом и как обеспечить объективность проверки. Пока прогноз ученых не слишком оптимистичен.

Сам Трамп заявил, что Twitter вмешивается в выборы 2020 года, добавляя к сообщению ярлык, предлагающий читателю «узнать больше о рассылке бюллетеней для голосования». После этого главы технологических компаний начали обсуждать идею автоматизированной технологии с открытым кодом для фактчекинга, которая бы могла решить проблему. Однако далеко не все были настроены так оптимистично.

«Боюсь показаться скучным, но чувствую, что мне слишком трудно это представить, — говорит Эндрю Дадфилд, глава отдела по автоматизированному фактчекингу в британской НКО Full Fact. – Для этой задачи нужно учесть столько

тонкостей и выполнить ее с такой точностью, на которую технологии пока не способны».

Full Fact получила грант от Google AI за общественно полезные разработки, которые дополняют, но не заменяют традиционную проверку фактов. Способность программы синтезировать большие объемы информации помогла фактчекерам приспособиться к масштабу информационной онлайн-среды. Но некоторые задания, например, истолковать проверенные факты в контексте, или учесть оговорки и лингвистические тонкости, лучше поручить человеку.

«Мы ограниченно применяем ИИ… чтобы найти пример, который можем отдать на проверку человеку и сказать: "Похоже, здесь совпадение", — говорит Дадфилд. – Я думаю, что пока нельзя настолько доверять проверку автоматической системе – сейчас это преждевременно».

Социолог Мона Слоун из Нью-Йоркского университета изучает, как в ИИ-системах проявляется неравенство. Она беспокоится, что полностью автоматизированный фактчекинг только укрепит предвзятость. В частности, Слоун указывает на сегмент афроамериканских пользователей Twitter — эта соцсеть слишком часто отмечает их разговорный язык как потенциально оскорбительный.

Поэтому, считают Слоун и Дадфилд, важно учитывать характер данных, которые обрабатывает алгоритм. «ИИ кодифицирует ту информацию, которую получает, поэтому, если в систему поступают неоднозначные данные, неоднозначным будет и результат, — говорит Дадфилд. — Но вводные данные получены от людей. Поэтому в таких случаях в конечном счете важно убедиться, что данные на входе верны, и что вы регулярно за этим следите».

Если упустить эти нюансы, могут появиться инструменты, провоцирующие неравенство, которые «явно будут направлены на усиление социальной иерархии, которая строится на расе, классе и гендере, — пишет в своей книге Race after Technology профессор Принстонского университета Руха Бенжамин. — Дискриминация по умолчанию появляется из-за того, что при разработке игнорируется социальное неравенство».

Но что происходит, когда в разработке участвует бизнес? Когда социальные платформы применяют эти технологии избирательно, в интересах своих клиентов?

Кэти Кальвер, директор центра журналистской этики в Висконсинском университете в Мэдисоне, считает, что экономические стимулы для увеличения числа пользователей и вовлеченности часто показывают, как компании относятся к социальной ответственности.

«Если сто крупнейших работодателей скажут: "Нам надоели мифы и дезинформация на вашей платформе, и мы отказываемся размещать на ней свой контент", можно быть уверенным — платформы будут над этим работать», — говорит Кальвер.

Но проблема в том, что рекламодатели часто сами и распространяют дезинформацию. Возьмем Faceboook, одного из партнеров Full Fact. Правила социальной сети не распространяются на ее крупнейших рекламодателей — политиков и политические организации. Иными словами, они не обязаны проходить фактчекинг.

Как оправдывает это Марк Цукерберг? Этикой маркетплейса идей — верой в то, что правда и общепринятые идеи выиграют в информационном соревновании. Но на этом маркетплейсе «сила распределена неравномерно», говорит Кальвер.

Внутреннее расследование Facebook обнаружило, что у радикально правых «намного больше аккаунтов и авторов», чем у радикально левых, несмотря на то, что большинство американцев придерживаются скорее левых взглядов. Вновь и вновь Facebook увеличивал присутствие платного контента — даже когда информация явно вводила в заблуждение или была направлена на аудиторию афроамериканцев.

«Этика использовалась как прикрытие, потому что она не регулируется законом, — говорит Слоун. — Она не подстраивается под более широкий политический, социальный и экономический контекст. Это умышленно неопределенный термин, который поддерживает системы власти, потому что власть решает, что этично».

Facebook знает, что его алгоритмы толкают пользователей на разные стороны баррикад и стимулируют плохие действия. Но он также знает, что борьба с этими проблемами может повлиять на пользовательскую вовлеченность — и доход от рекламы, который составляет 98% выручки компании и достиг почти $69,7 млрд в одном только 2019 году. Поэтому Facebook ничего не делал.

Борьба с дезинформацией и двусмысленностью требует больше, чем алгоритмы на базе искусственного интеллекта. Для этого нужна смелость и понимание истоков проблемы.

«Продукты и сервисы, которые предлагают решения для избавления от социальных предубеждений... в конечном итоге могут воспроизводить или даже углублять дискриминацию из-за субъективного понимания справедливости», — пишет Бенджамин.

Прежде чем использовать автоматизированный фактчекинг, стоит разобраться: с учетом чьих интересов он спроектирован и чьи интересы он подавляет? Какова мотивация социальных платформ в борьбе с фейками и дезинформацией? Пока мы не обеспечим непредвзятость в процессе разработки, ИИ не научится борьбе с фейками и дезинформацией». ***(Елена Лиханова. Автоматизированный фактчекинг: подходит ли он для соцсетей // Rusbase (https://rb.ru/story/auto-fact-checking/). 23.08.2020).***

***

«Президент США Дональд Трамп підписав указ, що обмежує роботу популярної соцмережі ТікТок на території країни. Згідно з документом, усі американські компанії, які співпрацюють з власником платформи, мають припинити транзакції через 45 днів.

ТікТок належить китайські фірмі. Трамп вважає це загрозою національній безпеці, оскільки вона нібито передає дані про користувачів китайському уряду. У самій компанії звинувачення відкидають…» ***(У США заборонили ТікТок // ООО "Национальные информационные системы" (https://podrobnosti.ua/2362181-u-ssha-zaboronili-tktok.html). 07.08.2020).***

***

«В работе основных сервисов Google, включая Gmail, Drive, Docs, Meet, Groups, Chat, Keep и Voice, произошел глобальный сбой. О проблемах в работе сервисов пользователи по всему миру начали сообщать после 7:00 утра.

Загрузка файлов в сервисы Google не выполнялась должным образом, включая загрузку вложений в электронных письмах Gmail. В некоторых случаях пользователи не могли даже просто написать новое электронное письмо или ответить на входящее.

Как сообщила компания Google, возникшие проблемы были связаны с отправкой писем через Gmail, видеотелефонной связью в Meet, созданием файлов в сервисе Google Диск, загрузкой CSV-файлов в консоли администратора, отправкой сообщений в Google Chat, добавлением новых страниц на сайтах, а также с сервисами Keep и Voice.

В то же время в пользователи Twitter пользователи массово жалуются на проблемы с загрузкой роликов в YouTube.

Что стало причиной сбоя пока неизвестно. Команда разработчиков подтвердила, что активно работают над установлением причины неполадок и их устранением». ***(По всему миру произошел сбой в работе большинства сервисов Google // SecurityLab.ru (https://www.securitylab.ru/news/511348.php). 20.08.2020).***

***

Китай

«Правительство КНР внедрило в механизм национальной системы контроля интернет-трафика, известной как «большой китайский файрвол», блокировку зашифрованных HTTPS-соединений, совершаемых с использованием протоколов TLS 1.3 и ESNI, сообщает ZDNet.

TLS (Transport Layer Security) – протокол криптозащиты данных, передаваемых в открытом канале между узлами Интернета. Он защищает трафик при просмотре сайтов в браузере, передаче электронной почты, файлов, VoIP. ESNI (Encrypted Server Name Indication) – расширение TLS, используемое в версии TLS 1.3, с целью скрыть не только трафик, но и доменное имя, к которому обратился пользователь.

Китай открывает великий файрвол – московское заявление главного в КНР по ИБ

HTTPS-трафик через более ранние версии TLS (1.1 или 1.2) по-прежнему разрешён. В этом случае можно видеть, с каким доменом пытаются связаться пользователи. Вероятно, китайское правительство готово удовлетвориться наблюдением за тем, к каким доменам обращаются пользователи на территории страны. Когда такой возможности из-за ESNI не стало, весь трафик такого рода попал под запрет.

Блокировка TLS 1.3 и ESNI введена в КНР с конца июля, отмечается в совместном отчёте трех организаций, мониторящих ситуацию с интернет-цензурой в Китае – iYouPort, University of Maryland и Great Firewall Report.

Согласно отчёту, китайское правительство блокирует весь трафик через TLS 1.3 и временно (на две-три минуты) блокирует IP-адреса, участвующие в подобной коммуникации». ***(В Китае блокирован шифрованный HTTPS-трафик, использующий TLS 1.3 и ESNI – СМИ // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5685638-V-Kitae-blokirovan-shifrovannyj-HTT.html). 10.08.2020).***

***

«В то время как США, Россия, Израиль и несколько европейских стран обладают развитым киберпотенциалом, специалисты из компании IntSights утверждают, что агрессивный подход Китая к кибероперациям сделал его, возможно, самым могущественным кибергосударством.

Китайские киберпреступные группировки продолжают осуществлять кибератаки с целью кражи интеллектуальной собственности и/или политических секретов, а китайское правительство расширяет как свои методы, так и стратегии, сообщается в отчете «Dark Side of China: The Evolution of a Global Cyber Power» («Темная сторона Китая: Эволюция глобальной киберсилы»).

Агрессивный подход страны к использованию кибероперацій для достижения политических и национальных целей отличает ее киберстратегию от более осторожных и продуманных подходов большинства других стран. Правительство США уже обозначило Китай как главную киберугрозу страны.

«За последнее десятилетие Китай становился все более откровенным в своих намерениях, и это изменение наблюдается и в кибероперациях. Специалисты отметили резкие различия в тактике, методах и поведении спонсируемых китайским государством кибергруппировок, а также военных и политических групп за последние несколько лет», — сообщили эксперты.

На брифинге для прессы в июле нынешнего года директор ФБР Кристофер Рэй (Christopher Wray) назвал кибератаки китайских хакеров, нацеленные на интеллектуальную собственность американских компаний и сбор личной информации граждан США, «одним из крупнейших трансферов богатств в истории человечества». ФБР обвинило китайских хакеров во взломе Equifax в 2017 году, в результате которого были похищены личные данные около 150 млн американцев, и отметило, что половина из 5 тыс. контрразведывательных расследований, проводимых в настоящее время в США, связана с Китаем». ***(Эксперты считают Китай самой сильной кибердержавой в мире // SecurityLab.ru (https://www.securitylab.ru/news/511551.php). 28.08.2020).***

***

Інші країни

«При посредничестве властей Израиля NSO Group заключила многомиллионные сделки с Бахрейном, Оманом, Саудовской Аравией и ОАЭ.

Правительство Израиля выступало посредником в ряде сделок по продаже шпионского программного обеспечения производства компании NSO Group

Technologies в Объединенные Арабские Эмираты и другие страны Персидского залива для содействия в слежке за диссидентами, сообщило издание Haaretz.

По данным газеты, компания заключила многомиллионные сделки с Бахрейном, Оманом, Саудовской Аравией, а также эмиратами Абу Даби и Рас-эль-Хайма (ОАЭ). Сумма одного из таких контрактов составляла $250 млн.

«Продукт, продаваемый в Европе за $10 млн, можно продать странам Персидском залива в 10 раз дороже», - отметил источник издания.

Согласно публикации, представители израильского правительства принимали участие в ряде встреч чиновников разведслужб арабских стран и топ-менеджеров NSO, некоторые из этих переговоров проводились в Израиле.

Отмечается, что NSO Group сотрудничала только с правительствами и официальными организациями, но не делала различий между демократическими и тоталитарными странами.

Продажами шпионского ПО в страны Персидского залива, по информации газеты, занимается специальный отдел компании NSO Group. Каждой стране было присвоено свое кодовое имя, например, Subaru (Саудовская Аравия), BMW (Бахрейн) или Jaguar (Иордан). Также отмечается, что израильские власти запретили NSO Group сотрудничать с союзником Ирана Катаром.

По словам сотрудников компании, несмотря на утверждения, что NSO Group тщательно регулирует использование ПО только для отслеживания преступников и подозреваемых в терроризме, на деле такие проверки не производятся.

Программное обеспечение Pegasus, разработанное компанией, позволяет следить и контролировать телефоны через приложение WhatsApp, тайно управляя его камерами и микрофонами с удаленных серверов и очищая личные данные и геолокацию. В частности, последняя версия программы Pegasus 3, позволяет взломать телефон всего за несколько часов при наличии всего лишь телефонного номера. Кроме того, разработчики могут удаленно управлять программой, отключать ее или просматривать собранные данные в режиме реального времени.

Что интересно, программа самоуничтожается в случае, если устройство, на котором она установлена, пересекает границу Израиля, Ирана, России, Китая или США». ***(Израиль продает шпионское ПО арабским странам // SecurityLab.ru (https://www.securitylab.ru/news/511420.php). 24.08.2020).***

***

Протидія зовнішній кібернетичній агресії

«Введение санкций Евросоюзом за якобы учиненные Россией и Китаем кибератаки приводит к новому политическому противостоянию и «кибер хаосу», заявил МИД.

«Можно сделать вывод, что ЕС предпочитает политику одностороннего давления и ограничений серьезному разговору, ведущему к урегулированию разногласий и наращиванию взаимного доверия. Такой подход приводит к новому политическому противостоянию и кибер хаосу, а не к порядку, о котором так

любят говорить наши партнеры ЕС», – говорится в сообщении Facebook министерства.

Ведомство напомнило, что ЕС обвиняет россиян к причастности к «кибер-инцеденту» 2018 года, за год до учреждения механизма кибер-санкций.

«Другими словами, они используют его ретроактивно. Видимо, юристы ЕС намеренно забыли, что закон не ретроактивен», – отметили в МИД…». ***(Алексей Дегтярев. Москва предупредила Евросоюз о «кибер хаосе» из-за санкций // Деловая газета «Взгляд» (https://vz.ru/news/2020/8/1/1052934.html). 01.08.2020).***

***

«Агентство по доходам Канады (CRA) приостановило онлайн-сервисы после того, как в эти выходные аккаунты подверглись третьей волне атак с использованием учетных данных, что дало злоумышленникам доступ к различным государственным услугам.

Канадские власти заявили, что почти 15 000 онлайн-аккаунтов для различных государственных служб стали жертвами трех недавних атак по подбору учетных данных. Эти учетные записи могут дать злоумышленникам доступ к информации о налогах и льготах канадцев, деньгам из фонда помощи в связи с коронавирусом и многому другому.

Атаки с заполнением учетных данных - это когда злоумышленники получают доступ к учетным записям, используя имена пользователей и пароли, которые были украдены во время предыдущих взломов. На встрече с прессой в понедельник Марк Бруйяр, исполняющий обязанности директора по информационным технологиям правительства Канады, сказал, что с начала августа различные правительственные счета пострадали от трех волн атак по подбору учетных данных, последняя из которых произошла в минувшие выходные.

Злоумышленники взломали 5 500 учетных записей Канадского налогового агентства (CRA), которые подключаются к порталу, позволяющему канадцам просматривать и управлять своей налоговой информацией и информацией о льготах в Интернете. Они также нацелились на 9041 учетную запись GCKey, предоставив доступ к порталу, используемому 30 федеральными департаментами и 12 миллионами канадцев, предоставляя доступ к онлайн-информации и государственным услугам, таким как трудоустройство, иммиграция и многое другое.

«Доступ ко всем затронутым учетным записям был отключен для обеспечения безопасности и защиты информации налогоплательщиков, и Агентство связывается со всеми затронутыми лицами и будет работать с ними, чтобы восстановить доступ к их CRA MyAccount», - говорится в сообщении правительства Канады. пресс - релиз в эти выходные.

Атаки

По данным правительства, из 9041 учетной записи GCKey, которая была атакована, треть использовалась для доступа к различным службам и в настоящее время дополнительно исследуется на предмет подозрительной активности. Эти услуги могут включать в себя услуги по трудоустройству или фонды помощи в связи с коронавирусом, предлагаемые Канадской программой экстренного

реагирования, которая предлагает до 2000 долларов для правомочных граждан. По словам Бруйяра, важно отметить, что внутренние службы самого GCKey не были скомпрометированы.

Затронутые учетные записи GCKey были аннулированы, как только угроза была обнаружена, и отделы связываются с пользователями, учетные данные которых были отозваны, чтобы предоставить инструкции о том, как получить новый GCKey.

Тем временем, сразу после атак, нацеленных на 5 500 учетных записей CRA, правительство отключило службы, связанные с «Моя учетная запись», «Моя учетная запись для бизнеса» и «Представление клиента» на веб-сайте CRA. В понедельник власти заявили, что ожидают восстановления этих услуг к среде.

В понедельник правительственные чиновники также обнаружили, что уязвимость в конфигурации программного обеспечения безопасности для учетных записей CRA позволяет злоумышленникам обойти меры безопасности. По их словам, этот недостаток, возникший из-за вопросов безопасности для учетных записей, с тех пор исправлен. Однако, когда его попросили уточнить детали, Бруйяр не назвал уязвимость системы безопасности или программное обеспечение.

Остались вопросы по мерам безопасности

Многие канадцы сообщили о подозрительной активности, связанной с их учетными записями CRA, начиная с начала августа, а некоторые из них в Twitter сообщили, что злоумышленники изменили свою информацию о прямом депозите и использовали эту информацию для подачи заявки на мошенническую помощь от коронавируса.

На встрече с прессой в понедельник официальные лица канадского правительства заявили, что они впервые уведомили Королевскую канадскую конную полицию (федеральную полицейскую службу Канады) об атаках с использованием учетных данных 11 августа. После того, как в минувшие выходные произошла третья волна атак, правительство приостановило онлайн-сервисы. .

На вопрос, почему канадцы не были уведомлены об атаках раньше, Бруйяр сказал: «Мы постоянно оцениваем нашу позицию в области безопасности… это постоянная проблема. Это не хакер, пытающийся пройти через черный ход. Они проходят через систему, как обычные пользователи… и это трудно обнаружить. У нас есть системы, позволяющие отслеживать такое поведение. Именно тогда была выявлена эта конкретная атака».

Инцидент также поставил под сомнение меры безопасности канадского правительства для онлайн-сервисов. BleepingComputer протестировал веб-сайт правительства Канады и обнаружил, что многие департаменты не применяют многофакторную аутентификацию для доступа к канадским службам, таким как CRA или GCKey.

Когда его спросили об отсутствии двухфакторной аутентификации (2FA), Бруйяр признал: «Некоторые двухфакторные аутентификации могли бы предотвратить это, особенно в тех случаях, когда вам требуется ключ. Но это сложно, не у всех есть такие вещи. Это балансирующий акт. Мы ищем способы укрепить наши системы».

Предотвращение заполнения учетных данных

По заявлению властей, все пользователи, привязанные к взломанным учетным записям, уведомляются об инциденте безопасности, и с тех пор все атаки были смягчены. Они призвали пользователей следить за тем, чтобы их пароли были актуальными. Со своей стороны, исследователи в области безопасности также призвали пользователей уделять первоочередное внимание гигиене паролей, чтобы не стать жертвой атак с заполнением учетных данных.

«Атаки с заполнением учетных данных, несомненно, популярны и могут затронуть любую организацию, независимо от ее сектора или географии, и предоставить первоначальный доступ к учетным записям жертв», - сказала Threatpost Кейси Кларк, исследователь угроз из Digital Shadows. «Поскольку атаки с заполнением учетных данных используют повторное использование паролей, пользователям настоятельно рекомендуется использовать сложные и уникальные пароли для всех своих учетных записей».

Джозеф Карсон, консультант по информационной безопасности в Thycotic, согласился с тем, что важный урок заключается в том, чтобы никогда не использовать пароли повторно, а также добавил, что любая компания, предлагающая онлайн-сервисы, также должна обеспечить наличие средств защиты, таких как 2FA.

«Компании, которые предлагают аутентификацию и вход на свой веб-сайт, также должны отказаться от использования пароля в качестве единственного средства контроля безопасности», - сказал он Threatpost. «Двухфакторная аутентификация должна быть включена для всех клиентов, поскольку это снижает риски того, что клиенты, повторно использующие пароли, станут жертвами киберпреступности или подделки учетных данных. Кроме того, рекомендуйте менеджеры паролей, чтобы помочь клиентам улучшить гигиену паролей и принимать решения при создании новых учетных записей и паролей». ***(Lindsey O'Donnell. Cyberattacks Hit Thousands of Canadian Tax, Benefit Accounts // Threatpost (https://threatpost.com/cyberattacks-canadian-tax-benefit-accounts/158400/). 17.08.2020).***

***

«Хакерские группировки, предположительно поддерживаемые правительством Китая, осуществляют кибератаки с целью проникновения в сети правительственных ведомств Тайваня и кражи конфиденциальной информации граждан в рамках непрекращающихся попыток воздействия на демократическое общество. Об этом заявил замглавы подразделения по кибербезопасности Бюро расследований Тайваня Лю Чиа-цзунь.

По словам чиновника, хакеры «уже долгое время» взламывают системы тайваньских компаний, предоставляющих информационные услуги госорганам, в попытках получить государственную информацию и персональные данные граждан.

За атаками стоят четыре группировки - Blacktech, Taidoor, MustangPanda и APT40. Благодаря тому, что хакеры тщательно скрывают следы своей деятельности, специалистам пока не удалось определить, какие данные были

украдены, за исключением одного случая, когда в руки злоумышленников попали порядка 6 тыс. правительственных электронных писем, отметил Лю.

Он также добавил, что с 2018 года Тайвань провел расследование примерно 10 дел, связанных с кибератаками со стороны китайских хакеров. По оценкам главы Департамента кибербезопасности страны Цзянь Хун-вея, китайские власти осуществляют на Тайвань порядка 30 млн кибератак в месяц». ***(Тайвань обвинил Пекин в кибератаках на госорганы // SecurityLab.ru (https://www.securitylab.ru/news/511308.php). 19.08.2020).***

***

«Специалисты в области кибербезопасности хотят внедрения более строгих мер по борьбе с растущим объемом дезинформации в Сети и поддельных доменов. Согласно новому исследованию Совета международной безопасности Neustar (NISC), почти половина (48%) ИБ-экспертов считают данные проблемы угрозой для своего предприятия, а другая половина (49%) оценивает их как очень опасную угрозу в целом.

Как сообщил ресурс Infosecurity Magazine, не довольствуясь ожиданием помощи со стороны регулирующих органов, многие эксперты в области кибербезопасности сами принимают меры против подобных угроз. Почти половина опрошенных сотрудников организаций (46%) сообщили, что у них есть планы по усилению акцента на их способности реагировать на рост дезинформации и поддельных доменов. Еще 35% заявили, что борьба с данными угрозами будет их главным приоритетом в следующие шесть месяцев, в то время как 13% лишь рассмотрят возможность принятия мер, если дезинформация и поддельные домены по-прежнему будут проблемой.

В рамках исследования были опрошены 306 специалистов из шести стран Европы, Ближнего Востока и Африки и США, занимающих руководящие должности в своих организациях, которые могут предоставить информированное мнение по наиболее актуальным вопросам кибербезопасности.

«Текущая пандемия привела к резкому росту дезинформации и регистрации поддельных доменов, киберпреступники используют такие тактики, как фишинг, мошенничество и вымогательское ПО для распространения вводящих в заблуждение новостей, фальсифицированных доказательств и неверных рекомендаций», — пояснили эксперты». ***(97% ИБ-специалистов обеспокоено ростом дезинформации в Сети // SecurityLab.ru (https://www.securitylab.ru/news/511519.php). 27.08.2020).***

***

Захист персональних даних

«Интернет-эксперт в области безопасности Боб Дьяченко в начале августа текущего года обнаружил в свободном доступе незащищённую базу данных, содержавшую порядка 235 млн профилей пользователей сервисов

Instagram, TikTok и YouTube. На сегодняшний день инцидент является одной из самых масштабных утечек данных.

Весь найденный массив содержал извлеченные из публичных профилей сведения, включая логины, полные имена пользователей, контактную информацию, изображения, статистику о числе подписчиков, данные о возрасте, поле и пр. На Instagram приходится более 192 млн утекших записей, 42 млн – на TikTok и почти 4 млн – на YouTube.

Изначально исследователи связали найденную БД с ныне несуществующей компанией Deep Social, которая в 2018 году была забанена Facebook и Instagram за извлечение данных из профилей пользователей, что запрещено политиками соцсетей. Компании даже пригрозили Deep Social судебным иском, если та не прекратит эту практику.

В ответ на запрос представители Deep Social переадресовали Дьяченко в компанию Social Data, специализирующуюся на продаже информации о популярных блогерах маркетинговым фирмам. Однако в Social Data опровергли связь с Deep Social и заявили, что не считают формирование БД противоправным действием. ***(В открытом доступе оказались 235 млн профилей Instagram, YouTube и TikTok // РосКомСвобода (https://roskomsvoboda.org/62711/). 20.08.2020).***

***

«Компания Facebook Inc. столкнулась с новыми обвинениями в незаконном сборе биометрических данных пользователей — на этот раз в рамках судебного иска, направленного против приложения Instagram. Как сообщает агентство Bloomberg, в иске утверждается, что компания «собирала, хранила и извлекала выгоду» из данных более 100 млн пользователей Instagram.

В частности, речь идет о данных, связанных с технологией распознавания лиц. По мнению истцов, Instagram использует инструмент для отметки лиц на фотографиях, который задействует технологию распознавания лица для создания «шаблонов лиц». Эти шаблоны сохраняются в базе данных Facebook. Истцы считают, что Instagram автоматически применяет данный инструмент без согласия пользователей даже в случаях, если люди, фигурирующие на снимках не зарегистрированы в соцсети.

«Этот иск необоснован, — заявила представитель компании Facebook Стефани Отуэй (Stephanie Otway), — Instagram не использует технологию распознавания лиц».

Жительница Иллинойса Келли Уэлен (Kelly Whalen) в своей жалобе утверждает, что регулярно пользуется Instagram с 2011 года, что приложение для публикации фотографий нарушает закон штата о конфиденциальности, который запрещает несанкционированный сбор биометрических данных. По закону компания может быть вынуждена заплатить 1000 долларов за нарушение — или 5000 долларов, если будет установлено, что она действовала опрометчиво или преднамеренно. Согласно иску, только в начале этого года Facebook начал информировать пользователей Instagram о том, что собирает биометрические данные.

Политика онлайн-данных Instagram в отношении распознавания лиц гласит: «Если мы внедрим технологию распознавания лиц в процессе вашего использования Instagram, мы сначала сообщим вам об этом, и вы сможете контролировать, будем ли мы использовать эту технологию для вас». ***(К Facebook подан иск за незаконный сбор биометрических данных в Instagram // РосКомСвобода (https://roskomsvoboda.org/62472/). 13.08.2020).***

***

«Twitter может выплатить Федеральной торговой комиссии США от 150 до 250 млн долл. в качестве штрафа за использование персональных данных пользователей для таргетинговой рекламы, сообщила The Wall Street Journal. ФТК подала иск, в котором говорится, что соцсеть с 2013 по 2019 год использовала для рекламы телефонные номера и адреса электронной почты, предоставленные пользователями соцсети для обеспечения безопасности. В Twitter называют свои действия непреднамеренными.

Twitter обвиняют в нарушении соглашения 2011 года о неразглашении персональных данных. Компания обязалась не вводить своих клиентов в заблуждение о том, как она защищает безопасность, неприкосновенность и конфиденциальность информации пользователей, предназначенной не для широкой аудитории. Twitter также должен был разработать специальную программу аудиторских проверок соблюдения соглашения, проводимых каждый год в течение 10 лет.

Это второй случай, связанный с безопасностью данных в Twitter за последний месяц. В июле в соцсети взломали 130 аккаунтов. Злоумышленники получили к ним доступ и отправляли от их имени твиты. Компании пришлось временно заблокировать атакованные аккаунты и запретить верифицированным пользователям публиковать новые посты. Кроме того, на время расследования инцидента Twitter заблокировал все учётные записи, которые в течение последних 30 дней пытались сменить пароль.

Впрочем, ФТК начала расследование ещё в октябре прошлого года. Пока неясно, сколько людей пострадали от действий компании». ***(Twitter грозит штраф до 250 млн долл. за использование данных пользователей // РосКомСвобода (https://roskomsvoboda.org/62188/). 04.08.2020).***

***

«Президент США Дональд Трамп подписал документы, запрещающие жителям США заключать сделки с китайскими приложениями TikTok и WeChat…

Принятие столь жестких ограничительных мер объясняется рисками для национальной безопасности страны, связанными с раскрытием личных данных американцев. В указах говорится, что приложения могут следить за пользователями и передавать информацию китайскому правительству. Оба документа вступят в силу через 45 дней, 20 сентября.

Представители TikTok уже прокомментировали решение Трампа и ещё раз напомнили о том, что не передавали и не намерены передавать информацию о пользователях Китаю:

«Мы шокированы недавним указом президента, который был издан без соблюдения процессуальных норм. В течение почти года мы стремились добросовестно взаимодействовать с правительством США, чтобы найти конструктивное решение высказанных опасений».

Уже больше месяца власти США грозят TikTok и WeChat ограничениями. В Белом доме убеждены, что данные из этих приложений идут прямо на серверы в Китае, к китайским военным и Китайской коммунистической партии.

В начале недели СМИ писали, что Трамп требовал продать TikTok американской компании, в противном случае сервис окажется под запретом на территории США. Желание приобрести компанию изъявил IT-гигант Microsoft, в скором времени он готов начать переговоры о покупке…». ***(Трамп запретил TikTok и WeChat // РосКомСвобода (https://roskomsvoboda.org/62318/). 07.08.2020).***

***

«В интернете на одном из форумов выставили на продажу личные данные около 1 млн водителей Москвы и Подмосковья… Начальная цена базы — 1,5 тыс. долл. Перечень содержит дату регистрации автомобиля, государственный регистрационный знак, марку, модель, год выпуска, ФИО владельца, его телефон и дату рождения, регион регистрации, VIN-код, серию и номер свидетельства о регистрации и ПТС.

База интересная угонщикам и мошенникам, использующих социальную инженерию. Человек может сообщить пароли, контактные данные, информацию о карте и расположении автомобиля, считая, что говорит с сотрудником ГИБДД или банка, пояснили собеседники издания. Знание VIN-номера также может дать информацию об установленной на автомобиль сигнализации, а данные владельца помогают определить место парковки…». ***(В Сеть утекли данные 1 миллиона автомобилистов московского региона // РосКомСвобода (https://roskomsvoboda.org/62113/). 03.08.2020).***

***

«Представители Университета Юты сообщили, что недавно учебное заведение было вынуждено выплатить хакерам 457 059 долларов, чтобы не допустить утечки данных о студентах.

Официальное заявление гласит, что в июле 2020 года учебному заведению удалось избежать серьезной атаки шифровальщика, в ходе которой неназванные хакеры смогли зашифровать лишь 0,02% данных, хранящихся на серверах университета. И хотя в итоге все эти данные были благополучно восстановлены из резервных копий, еще до начала шифрования злоумышленники успели похитить информацию о студентах вуза, а затем потребовали у руководства учебного заведения выкуп, в противном случае угрожая опубликовать украденное в открытом доступе.

Шантаж заставил Университет Юты пойти уступки и заплатить вымогателям. К счастью, часть запрошенной суммы покрыл специальный полис киберстрахования, а университет предоставил лишь оставшуюся часть средств. При этом подчеркивается, что для оплаты выкупа не использовались поступившая плата за обучение, гранты, пожертвования, государственные средства или деньги налогоплательщиков.

Издание ZDNet, со ссылкой на специалиста компании Emsisoft Бретта Кэллоу (Brett Callow), сообщает, что за данной атакой, судя по всему, стояла хак-группа NetWalker, хотя официальных подтверждений этому нет…». ***(Мария Нефёдова. Университет Юты выплатил вымогателям 457 000 долларов // Хакер (https://xakep.ru/2020/08/21/university-of-utah-ransom/). 21.08.2020).***

***

«Использование сторонних файлов cookie для отслеживания и таргетинга рекламы гигантами-брокерами данных Oracle и Salesforce стар предметом коллективного иска, поданного против компаний в Великобритании и Нидерландах.

В иске утверждается, что массовое наблюдение за пользователями Интернета для проведения аукционов в режиме реального времени не может быть совместимо со строгими законами ЕС в отношении согласия на обработку персональных данных.

По мнению истцов, общая сумма коллективных исков может превысить 10 миллиардов евро.

В Великобритании дело может также столкнуться с некоторыми юридическими препятствиями из-за отсутствия установленной модели для преследования коллективного ущерба в делах, касающихся прав на данные. Хотя есть признаки, что это меняется.

Некоммерческий фонд The Privacy Collective подал сегодня иск в окружной суд Амстердама, обвинив двух гигантов-брокеров данных в нарушении Общего регламента ЕС по защите данных (GDPR) при обработке и обмене информацией людей с помощью отслеживания третьей стороной файлов cookie и с использованием других рекламных технологий.

Голландское дело, является крупнейшим коллективным иском в Нидерландах, связанным с нарушением GDPR, при этом фонд истца представляет интересы всех голландских граждан, чьи персональные данные были использованы без их согласия и ведома Oracle и Salesforce.

Аналогичный иск будет подан в Высокий суд Лондона, в Англии, в котором будет сделана ссылка на GDPR и PECR Великобритании (Правила конфиденциальности электронных коммуникаций) - последние регулируют использование личных данных для маркетинговых коммуникаций.

Согласно GDPR, согласие на обработку персональных данных граждан ЕС должно быть информированным, конкретным и свободно предоставляемым. Регламент также наделяет людей правами в отношении их данных, например, возможностью получать копию их личной информации.

Это те требования, на нарушении которых построена аргументация исковых требований, а также аргументы в пользу того, что сторонние файлы cookie используются для отслеживания технологических гигантов, BlueKai и Крукс - трекеры, которые размещены на множестве популярных веб-сайтов, таких как Amazon, Booking.com, Dropbox, Reddit и Spotify и многих других - наряду с рядом иных методов отслеживания, которые применяются для массового неправомерного использования данных европейцев.

Согласно маркетинговым материалам Oracle, ее партнеры-провайдеры Data Cloud и BlueKai Marketplace имеют доступ к примерно 2 млрд глобальных профилей потребителей.

В то время как Salesforce утверждает, что ее маркетинговое облако «взаимодействует» с более чем 3 млрд браузеров и устройств в месяц.

Обе компании годами наращивали свои возможности отслеживания и таргетинга за счет приобретений; Oracle покупает BlueKai в 2014 году, а Salesforce - Krux в 2016 году.

Процесс назначения ставок в режиме реального времени (RTB), который передают файлы cookie и методы отслеживания пары, обеспечивая фоновую, высокоскоростную торговлю профилями отдельных веб-пользователей во время их просмотра для проведения аукционов динамической рекламы и показа поведенческой рекламы, ориентированной на их интересы, в последние годы неоднократно подвергался жалобам на нарушения GDPR.

В этих жалобах утверждается, что обработка информации людей RTB является нарушением правил, поскольку по своей сути небезопасно транслировать данные стольким другим организациям, в то время как GDPR, наоборот, предусматривает требование конфиденциальности по умолчанию и по умолчанию.

Судебный процесс финансируется Innsworth, спонсором судебных разбирательств, который также финансирует коллективный иск Уолтера Меррикса в отношении 46 миллионов потребителей против Mastercard в судах Лондона. И GDPR, похоже, помогает изменить направленность коллективных исков в Великобритании - поскольку он позволяет отдельным лицам подавать частные судебные иски. Структура также может поддерживать третьи стороны в подаче исков о возмещении ущерба от имени физических лиц. В то время как изменения во внутреннем законодательстве о правах потребителей, похоже, также приводят к коллективным искам.

Отдельный и все еще продолжающийся судебный процесс в Великобритании, который требует возмещения убытков от Google от имени пользователей Safari, чьи настройки конфиденциальности он исторически игнорировал, также, по всей видимости, повысило перспективы коллективных судебных исков, связанных с проблемами кибербезопасности.

Хотя суды первоначально отклонили иск в прошлом году, апелляционный суд отменил это решение, отклонив аргумент Google о том, что законодательство Великобритании и ЕС требует «доказательства причинно-следственной связи и косвенного ущерба» для подачи иска, связанного с потерей контроля над данными.

Стоит отметить, что технология таргетинга рекламы коварна в том смысле, что большинство людей не подозревают о ее влиянии или о нарушениях

конфиденциальности и прав на данные, которые она влечет за собой. В рамках этой рекламной среды Oracle и Salesforce ежедневно выполняют действия, которые нарушают европейские правила конфиденциальности, но их привлекают к ответственности впервые. Эти дела привлекут внимание к астрономической прибыли, получаемой от личной информации людей, и к рискам для отдельных лиц и общества из-за отсутствия ответственности». ***(Романов Роман. К Oracle и Salesforce предьявлены иски на сумму более 10 млрд. евро за незаконное использование файлов cookies // Internetua (https://internetua.com/K-oracle-i-salesforce-predjavleny-iski-na-summu-bolee-10-mlrd-evro-za-nezakonnoe-ispolzovanie-failov-cookies). 14.08.2020).***

***

«…Агентство Privacy Affairs опублікувало звіт Dark Web Price Index 2020. В ньому розповіли про середні ціни на зламані облікові записи соцмереж в даркнеті.

Дослідники проаналізували сотні записав у даркнеті, де хакера регулярно обмінюються вкраденими обліковими даними. В ході дослідження вдалось проіндексувати середні ціни на різні типи облікових записів.

Зламані акаунти в соцмережах кошують у Facebook ($74,5), Instagram ($55,45), Twitter ($49). Зламаний акаунт в Gmail вартує дорожче - $155,75. Дослідники пояснюють це тим, що зламана пошта дає доступ і до інших акаунтів жертви.

Згідно зі звітом, в даркнеті відносно небагато пропозицій по злому і продажу акаунтів. Можливо, це пов'язано з відсутністю попиту в поєднанні з посиленням заходів безпеки.

Продаються в даркнеті і дані про банківські картки. Доступ для банківських карт з сумами від $ 2 тис. коштує всього $65. Продавці дають гарантію успішного зняття коштів в районі 80%. За доступ до даних по акаунту платіжної системи PayPal хакера просять в середньому $198. Це найбільш популярний запит на ринку незаконних послуг.

Також можна купити 1000 підписників в таких сервісах, як Twitch, Spotify, Pinterest, SoundCloud. Ціни на них стартують від $1 до $10.

Дослідники також визначили вартість DDoS-атак. Наприклад, 24-годинна атака потужністю 10000-50000 запитів в секунду на незахищений веб-сайт в середньому коштує $60.

Звіт містить дані й про підроблені документи. Найдорожче коштують паспорти США, Канади та країн Європи - їхня середня ціна складає $1500.

Для того, щоб зберегти свої акаунти від злому, варто дотримуватись простих правил. По-перше, не відкривати фішингові листи та переходити за сумнівними посиланнями. По-друге, використовувати двофакторну аутентифікацію. По-третє, користуватися різними браузерами, а не лише Google Chrome. По-четверте, надаючи програмі дозвіл на доступ до ваших персональних даних, дізнайтеся, де саме планують використовувати ці дані…». ***(Скільки коштують зламані акаунти Facebook та Instagram в даркнеті – дослідження // MEDIASAPIENS***

(https://ms.detector.media/kiberbezpeka/post/25187/2020-08-04-skilki-koshtuyut-zlamani-akaunti-facebook-ta-instagram-v-darkneti-doslidzhennya/). 04.08.2020).

***

«У відкритому доступі опинились дані 235 млн користувачів Instagram, YouTube і TikTok опинилися. За даними неурядової групи, яка займається дослідженнями питаннями кібербезпеки, Comparitech масовий витік стався через незахищену базу даних.

В мережу потрапили дані майже 190 млн користувачів Instagram, 42 млн користувачів TikTok та майже 4 млн даних користувачів YouTube. В мережу потрапили справжні імена, адреси та аватари, кожен п'ятий запис містив або номер телефону, або адресу електронної пошти.

За даними Comparitech, відповідальною за витік даних є компанія Deep Social, яка вже припинила своє існування. З цією компанією Facebook співпрацювала до 2018 року. Після того, як Facebook відібрала у Deep Social доступ до свого API, компанія припинила своє існування. Однак дані, які вона встигла зібрати, опинились в мережі.

На думку редактора Comparitech Пола Бішоффа, ця інформація, ймовірно, буде найбільш цінною для спамерів і кіберзлочинців, які проводять фішингові кампанії…». ***(У мережу потрапили дані 235 млн користувачів Instagram, TikTok та YouTube // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/25317/2020-08-20-u-merezhu-potrapili-dani-235-mln-koristuvachiv-instagram-tiktok-ta-youtube/). 20.08.2020).***

***

«Практически во всех браузерах есть режим инкогнито, который должен сохранять в тайне историю посещения веб-страниц. Важно понимать, какие данные при этом действительно удаляются, а какие — нет.

Как устроен режим инкогнито

Считается, что при использовании приватного режима веб-браузер забывает о сеансе сразу после его завершения: посещенные страницы не сохраняются в журнале, а cookie-файлы, которые регистрируют некоторые из действий пользователя в сети, быстро стираются.

Именно этот тип файлов позволяет сохранять информацию о содержимом корзин интернет-магазинов, даже если забыть о них на несколько дней. Также с помощью cookie-файлов сайты запоминают, заходили ли вы туда раньше: например, большинство ресурсов предлагает подписаться на обновления только при первом посещении, а при последующих визитах этого не делают. Но если открыть те же страницы в режиме инкогнито, все повторится заново.

У этой анонимности есть как плюсы, так и минусы. Например, при входе в аккаунт Twitter или Gmail в режиме инкогнито придется каждый раз вводить логин и пароль, но по этой же причине можно получить доступ к множеству бесплатных статей с платных сайтов (большинство ресурсов не сразу вычисляет, что вы уже посещали платформу до этого).

В последнее время браузеры становятся все более персонализированными: веб-сайты, которые пользователь посещает чаще других, первыми появляются при вводе текста в адресной строке или окне поиска. В режиме инкогнито история просмотров и информация, которую пользователь вводил в веб-формы, не сохраняются: эти данные исчезают сразу после закрытия браузера. Поэтому сайты, которые вы посещали в режиме инкогнито, не должны отображаться в этих подсказках (впрочем, здесь есть исключения, о которых можно узнать ниже).

Режим инкогнито удобен в тех случаях, когда нужно использовать несколько учетных записей одновременно. Вам не придется каждый раз выходить из аккаунта — браузер сделает это за вас. Приватный режим также незаменим в тех случаях, когда пользователю нужно найти информацию по конфиденциальным темам — например, по поводу проблем со здоровьем — и он не хочет, чтобы эти данные сохранялись в истории просмотров или влияли на контекстную рекламу.

Данные о действиях пользователя в режиме инкогнито действительно удаляются из истории браузера и используемого устройства, стоит только закрыть соответствующие окна. Но не стоит забывать, что в современном мире отслеживание и анализ данных выходят далеко за эти рамки.

От чего не защищает приватный режим

Как только пользователь в режиме инкогнито заходит на один из популярных сайтов — Facebook, Amazon, Gmail и т.д. — его действия перестают быть анонимными как минимум для этих ресурсов. После завершения сеанса cookie-файлы и данные отслеживания удаляются, но во время посещения сайта эта информация активно используется в том числе для того, чтобы связывать его действия в различных учетных записях.

Например, если вы вошли в Facebook, соцсеть может видеть ваши действия на других сайтах и корректировать рекламу в соответствии с ними даже при включенном режиме инкогнито. Блокировка сторонних cookie-файлов в браузере (в Chrome даже есть соответствующая функция) может в некоторой степени затруднить этот процесс, но остановить его полностью не получится из-за особенностей устройства рекламных сетей и технологий отслеживания.

У Google уже были неприятности из-за этой практики. При использовании сервисов компании в режиме инкогнито поисковые запросы регистрируются и связываются с учетной записью, если она настроена соответствующим образом. Кроме того, есть вероятность, что Google продолжает следить за пользователем и тогда, когда он переходит на другие сайты.

Для того чтобы стать объектом отслеживания, необязательно входить в аккаунты — веб-сайты могут использовать IP-адрес и данные о типе устройства и браузере пользователя, чтобы установить его личность и связать это с другими данными. Некоторые браузеры борются с этим типом отслеживания, который называется «создание цифрового отпечатка», но полностью избежать его пока не удается.

Кроме того, режим инкогнито не защищает данные о посещенных страницах от работодателя и интернет-провайдера: с его помощью можно скрыть информацию о ваших действиях от конкретного браузера и других людей, использующих то же устройство — в остальном никаких гарантий нет.

Оставаться полностью невидимым в сети довольно сложно. Чтобы свести отслеживание к абсолютному минимуму, можно выбирать специальные браузеры, ориентированные на конфиденциальность, использовать сервисы типа поисковой системы DuckDuckGo, и подключаться к интернету через VPN». ***(Александра Степанова. Режим инкогнито: действительно ли он защищает данные пользователей // Rusbase (https://rb.ru/story/incognito-mode-explainer/). 12.08.2020).***

***

«Новый вид мошенничества появился в соцсети Instagram. Мошенники могут завладеть чужим аккаунтом, предложив получить подтвержденный статус для него. Об этом сообщает Telegram-канал Gurov Digital.

С подтвержденного аккаунта знаменитости, который помечен синей галочкой как Verified | Support, поступает предложение получить для учетной записи такой же статус.

После этого необходимо только ввести пароль на специальном сайте. Ввод пароля приведет к полной потере Instagram-аккаунта». ***(Екатерина Кочкина. В Instagram появился новый вид мошенничества // Rusbase (https://rb.ru/news/instagram-scam/). 16.08.2020).***

***

«В 2010 году фонд Electronic Frontier Foundation был сыт по горло проблемой навязчивого интерфейса Facebook... Компания принуждала людей отказываться от своей приватности всё сильней и сильней. Спрашивается, как назвать это принуждение? Zuckermining? Facebaiting? Zuckerpunch? Название, которое в конечном итоге прижилось — Privacy Zuckering («Цукеринг приватности»), или «вас обманом заставляют публично делиться большей информацией о себе, чем вы изначально намеревались».

За десять лет Facebook пережил достаточно скандалов и увидел, что люди обеспокоены этими манипуляциями. В прошлом году он даже заплатил штраф в размере пяти млрд долл. за «ложные заявления о способности потребителей контролировать конфиденциальность своих персональных данных». И всё же исследователи обнаружили, что Privacy Zuckering и другие теневые тактики живут и здравствуют в интернете, особенно в социальных сетях, где управление конфиденциальностью более запутанно, чем где-либо.

Ещё в 2010 году Facebook использовал трюк, когда позволил пользователям «отказаться» от сайтов партнеров платформы, собирающих их общедоступную информацию в соцсети. Все, кто отказывались, видели всплывающее окно с вопросом: «Вы уверены? Разрешение мгновенной персонализации даст вам больше возможностей при просмотре веб-страниц». До недавнего времени Facebook также предостерегал людей от отказа от распознавания лиц: «Если вы выключите распознавание лиц, мы не сможем применить эту технологию, когда незнакомец использует вашу фотографию, чтобы выдать себя за вас». Кнопка включения настройки яркая и синяя, а кнопка выключения — серая, менее цепляющая глаз.

Исследователи называют эти проектные и языковые решения «тёмными паттернами» (dark patterns), которые пытаются манипулировать вашим выбором. Instagram донимает вас «пожалуйста, включите уведомления» и не предоставляет возможности отказаться? Это тёмный паттерн. LinkedIn показывает вам часть сообщения в электронной почте, но заставляет посетить платформу, чтобы прочитать больше? Тоже он. Facebook перенаправляет на «выход из системы», когда вы пытаетесь деактивировать свой аккаунт? Снова тёмный паттерн.

Тёмные паттерны есть по всему интернету, они побуждают людей подписываться на информацию или услуги, приобретать товары. Колин Грей, исследователь взаимодействия человека и компьютера в Университете Пердью, изучает тёмные паттерны с 2015 года. Он и его команда выделили пять их основных типов:

— нытьё;
— препятствия;
— утаивание;
— вмешательство в интерфейс;
— принуждение.

Такие игры не ограничиваются социальными сетями. Они распространились по всему интернету, особенно после введения Общего регламента по защите персональных данных (General Data Protection Regulation, GDPR). С тех пор как GDPR вступил в силу в 2018 году, сайты обязаны запрашивать у людей согласие на сбор определённых типов данных. Но некоторые баннеры просто просят вас принять политику конфиденциальности — без возможности сказать «нет». «Некоторые исследования показали, что более 70% баннеров согласия в ЕС имеют какой-то тёмный паттерн, встроенный в них», — говорит Грей.

В прошлом году американские сенаторы Марк Уорнер и Деб Фишер внесли законопроект, который запретит подобные «манипулятивные пользовательские интерфейсы». Проблема в том, что становится очень трудно определить тёмный паттерн. «Любой дизайн имеет определённую степень убеждения», — говорит Виктор Йокко, автор книги «Дизайн для ума: семь психологических принципов убеждающего дизайна».

По своему определению дизайн побуждает использовать продукт каким-либо образом, что изначально не плохо. Плохо, если дизайн разрабатывается с целью обмануть.

Грей тоже столкнулся с трудностями разграничения тёмных паттернов и просто плохого дизайна. Он даже создал фреймворк определения последнего. Так, плохой дизайн лишает пользователя выбора и подталкивает его к тому решению, которое приносит пользу не ему, а компании. Дизайнеры используют такие стратегии, как искажение информации, торг и двуличность (реклама блокатора рекламы, который тоже содержит рекламу).

Грей приводит в пример приложение для смартфонов Trivia Crack, которое заставляет своих пользователей играть в другую игру каждые два-три часа. Такие спам-уведомления уже много лет используются социальными сетями для того, чтобы вызвать тот вид синдрома упущенной выгоды, который держит вас на крючке. «Мы знаем, что если мы дадим людям такие вещи, как свайп или

обновление статуса, то с большей вероятностью люди вернутся, — говорит Йокко. — Это также может привести к компульсивному поведению».

Самые мрачные варианты развития событий возникают, когда люди пытаются покинуть эти платформы совсем. Попробуйте деактивировать свой аккаунт в Instagram, и вы обнаружите, что это чрезвычайно трудно. Во-первых, вы даже не можете сделать это приложении. В ПК-версии сайта эта настройка скрыта внутри «Edit Profile» и поставляется с серией вопросов: «Почему вы отключаетесь? Слишком отвлекает? Попробуйте отключить уведомления здесь. Просто нужен перерыв? Разлогиньтесь вместо того, чтобы уйти совсем»).

«Это создает препятствия на вашем пути, чтобы вам было труднее решиться», — говорит Натали Нахай, автор книги «Паутина влияния: психология онлайн-убеждения». Много лет назад, удалив свой аккаунт в Facebook, она обнаружила похожий набор манипулятивных тактик. Соцсеть показывала фотографии некоторых её близких друзей. «Они используют язык, который, по моему мнению, является принуждающим, — рассуждает Нахай. — Из-за него тебе психологически больно уходить».

Хуже того, говорит Грей, исследования показывают, что большинство людей даже не знают, что ими манипулируют.

Но согласно одному исследованию, «когда люди были заранее подготовлены к манипуляциям, вдвое больше пользователей могли распознать тёмные паттерны». По крайней мере, есть некоторая надежда, что большая осведомлённость может вернуть пользовательский контроль хотя бы частично». ***(How Facebook and Other Sites Manipulate Your Privacy Choices // WIRED (https://www.wired.com/story/facebook-social-media-privacy-dark-patterns//). 12.08.2020).***

***

«Корпоративный облачный гигант Cloudera отключила несколько своих облачных серверов хранения данных, несмотря на то, что изначально они утверждали, что серверы были «открытыми по замыслу», после того как исследователь безопасности обнаружил внутри конфиденциальные внутренние файлы.

Крис Викери, директор по исследованиям рисков охранной компании UpGuard,в конце июля обнаружил серверы облачного хранения, известные как корзины, размещенные на Amazon Web Services. Данные в основном содержат устаревшие данные Hortonworks, полученные до слияния всех акций компании Cloudera на сумму 5,2 миллиарда долларов в январе 2019 года.

Когда они были достигнуты, пресс-секретарь Cloudera Мэдж Миллер сообщила TechCrunch.что корзины должны были быть открытыми и содержать файлы и код, открытые для клиентов, пользователей и более широкого сообщества. Однако компания заявила, что обнаружила три файла с конфиденциальной информацией, которые были удалены из корзин.

Но вскоре после этого компания изменила свою позицию и полностью прекратила работу.

Викери, который поделился своими выводами исключительно с TechCrunch, сказал, что, хотя подавляющее большинство файлов в облачных корзинах предназначалось для публичного и общественного потребления, он также обнаружил файлы, содержащие учетные данные, токены доступа к учетной записи, пароли и другие секреты для внутренней системы Jenkins Cloudera. которые компания использует для создания и тестирования своих программных проектов. По словам Викери, в корзинах также содержатся целые базы данных SQL для внутренних баз данных сборки.

Cloudera подтвердила нарушение безопасности в более позднем электронном письме в TechCrunch.

«Благодаря вопросам исследователя безопасности мы глубоко погрузились в работу и обнаружили некоторые учетные данные и дампы SQL в общедоступных корзинах, которые не должны были туда помещаться. Учетные данные были для нашего внутреннего процесса сборки Jenkins, а дампы SQL - для нашей базы данных сборки», - сказал представитель.

«С тех пор мы удалили эту информацию из общедоступных корзин и предприняли дальнейшие шаги по исправлению ситуации, изменив учетные данные и ротацию ключей. Мы также пришли к выводу, что можем закрыть доступ к нескольким неиспользуемым общедоступным сегментам ».

Компания заявила, что после удаления конфиденциальные данные не содержали никаких данных о клиентах или какой-либо другой личной информации.

В целом, нарушение безопасности могло быть еще хуже - даже если бы инцидента можно было вообще избежать.

Но Викери сказал, что этот инцидент важно раскрыть, поскольку он раскрывает неотъемлемый риск использования чрезвычайно больших контейнеров облачного хранилища. Другими словами, корзины были настолько большими и в них было столько файлов, что почти невозможно заметить, когда что-то важное по ошибке добавляется в корзину.

«Когда так много каталогов и файлов разного формата спрятаны вместе, становится слишком легко что-то ошибочно поместить среди них и остаться незамеченным, как это, похоже, здесь произошло», - пишет Викери». ***(Zack Whittaker. Cloudera pulls sensitive files from its 'open by design' cloud servers // TechCrunch (https://techcrunch.com/2020/08/24/cloudera-hortonworks-data-exposed/). 24.08.2020).***

***

«Хакеры могли захватить учетные записи пользователей в десятках мобильных приложений для фитнеса и тренажерного зала, даже если был активен механизм двухфакторной аутентификации (2FA).

Общей площадкой для всех приложений является Fizikal, израильская платформа для управления тренажерными залами и спортивными клубами, которая позволяет клиентам управлять своей подпиской и регистрацией в классе.

Несколько уязвимостей, влияющих на платформу Fizikal, могут быть объединены в цепочку для обхода проверок безопасности, перечисления

пользователей, подбора одноразового пароля (OTP) для входа в систему и получения доступа к учетной записи пользователя.

Легкая грубая сила

Сахар Авитан, консультант израильской компании по кибербезопасности Security Joes, обнаружил, что около 80 приложений используют API Fizikal для облегчения доступа к клубу и его удобствам.

На момент написания в разделе здоровья и фитнеса Google Play Store имеется около 70 приложений Fizikal, многие из которых были добавлены за последние несколько дней. Некоторые из старых приложений имеют более 5000 загрузок и вместе составляют не менее 240 000 активных установок.

Интерес Авитана к анализу платформы возник после того, как он сбросил пароль для своей учетной записи EZ Shape, одного из приложений, которые он использовал, и заметил, что получил слабый, состоящий из 4 символов.

Одна вещь, которую заметил исследователь, заключалась в том, что процедура сброса пароля давала разные результаты для телефонных номеров, присутствующих в базе данных, и несуществующих.

Это позволило ему лучше понять весь механизм, что привело к обходу проверок безопасности и возможности перечислять пользователей. Эта информация позволила ему узнать номера телефонов, которые пользователи определили для получения пароля OTP по SMS для подтверждения сброса.

Однако другой недостаток позволил подобрать номера OTP (процесс завершается примерно за одну минуту) и отправить их в Fizikal API до того, как законный пользователь получит предупреждение.

По словам Security Joes, процесс проверки OTP не был защищен механизмом защиты от автоматизации или капчей, которая блокировала бы попытки грубой силы.

Имея OTP на руках, Avitan отправил его на сервер Fizikal и получил уникальный TokenID, необходимый для генерации нового пароля. Он доставил код на сервер в заголовках HTTP вместе со свежим паролем.

Взлом учетной записи приложения для приложения, которое использует платформу управления Fizikal, не только позволило злоумышленнику заблокировать пользователя или отменить его подписку, но и предоставил доступ к личной информации:

телефонный номер
ФИО
Дата рождения
адрес электронной почты
почтовый адрес
идентификационный номер

Авитан смог автоматизировать всю процедуру с помощью проверочного кода, который использовал недостатки, обнаруженные им в Fizikal.

Идо Наор, основатель и генеральный директор Security Joes, сказал BleepingComputer, что злоумышленник мог использовать эти уязвимости, чтобы узнать расписание кого-то известного или члена правительства.

По словам исследователей, Fizikal и CERT в Израиле получили полный отчет о результатах и оперативно приняли меры для решения проблем». ***(Ionut Ilascu. Gym app management platform exposed info of thousands of users // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/gym-app-management-platform-exposed-info-of-thousands-of-users/). 18.08.2020).***

***

«Брокер данных из социальных сетей оставил без защиты базу с информацией о 238 миллионах аккаунтов. Компания занимается тем, что собирает данные из профилей в социальных сетях, находящиеся в свободном доступе, и объединяет их в базы данных. Эти базы интересны маркетологам, но также ими интересуются киберпреступники. Указанная информация не поможет взломать чей-то аккаунт, но вполне может поспособствовать повышению эффективности фишинговых кампаний.

В открытой базе данных содержалась информация из 192 миллионов профилей Instagram, 42 миллионов профилей TikTok и 4 миллионов профилей YouTube. В каждой записи содержались полностью либо частично: имя профиля, настоящее имя, изображение аккаунта, описание, возраст, пол и другие. Пятая часть профилей сопровождалась электронным адресом или номером телефона. База была закрыта спустя три часа после обнаружения ее специалистами, однако неизвестно, как долго она находилась без защиты». ***(Информация из 238 миллионов профилей оказалась без защиты // SecureNews (https://securenews.ru/information-from-238-million-profiles-was-left-unprotected/). 19.08.2020).***

***

«Пользователь Twitter опубликовал сообщение, в котором заявил, что владеет большим количеством слитой информации компании Intel. В доказательство он оставил ссылку на облачное хранилище с некоторым количеством документов. Документы действительно оказались классифицированы как секретные и попадающие под требование о неразглашении. Пользователь, разместивший заявление также сказал, что всего в его распоряжении 20 ГБ таких данных, а получил он их от анонимного хакера, взломавшего сервера компании.

Среди документов предположительно находятся дорожные карты некоторых проектов, сведения об архитектуре процессоров и инструментах разработки, схемы, техническая информация и другие важные сведения.

Сама компания говорит о том, что инцидент не является результатом взлома. По словам представителей Intel информация взята из Центра ресурсов и дизайна, где она расположена для подрядчиков, клиентов и партнеров с правом доступа к ней. По всей видимости информацию распространил инсайдер, имевший доступ». ***(20 ГБ секретных данных Intel оказались в сети // SecureNews (https://securenews.ru/20-gb-of-secret-intel-data-was-on-the-network/). 07.08.2020).***

***

«Исследовательская команда ресурса CyberNews обнаружила в Сети публично доступный сервер Amazon AWS, на котором хранилось 7 ГБ незашифрованных файлов, содержавших 350 млн уникальных электронных адресов. Владельца базы данных установить не удалось.

Незащищенный бакет содержал в общей сложности 67 CSV- файлов, из них 21 файл включал как незашифрованные, так и хешированные электронные адреса. Судя по датам загрузок, эти адреса были либо украдены, либо куплены на черном рынке в октябре 2018 года, а затем постепенно расшифрованы владельцем бакета.

По данным экспертов, сервер находился в открытом доступе по меньшей мере 18 месяцев и пока неясно, попал ли он в поле зрения злоумышленников. Поскольку исследователи не смогли идентифицировать владельца сервера, они обратились к Amazon. Компания закрыла доступ к серверу 10 июня нынешнего года». ***(В Сети найден незащищенный сервер, содержавший 350 млн электронных адресов // SecurityLab.ru (https://www.securitylab.ru/news/511102.php). 12.08.2020).***

***

«Пользователям популярного инструмента для удаленного управления ПК TeamViewer настоятельно рекомендуется обновиться до новой версии TeamViewer в связи с опасной уязвимостью в программном обеспечении, позволяющей похитить системный пароль и скомпрометировать систему. Более того, атака почти не требует взаимодействия с пользователем, все что нужно - убедить жертву посетить вредоносный сайт.

Уязвимость, получившая идентификатор CVE 2020-13699, связана с тем, как TeamViewer обрабатывает заголовки URI, что позволяет злоумышленнику заставить ПО передать запрос NTLM аутентификации на систему атакующего.

Проще говоря, преступник может использовать URI схему TeamViewer, чтобы заставить установленное на системе жертвы приложение инициировать соединение с подконтрольной атакующему сетевой папке SMB. Таким образом он может вызвать утечку имени системы и NTLMv2 хэшированную версию пароля и авторизоваться на системе жертвы.

Для успешной атаки злоумышленнику потребуется внедрить вредоносный iframe на web-сайт, а затем затем заставить жертву посетить ресурс. Далее на компьютере автоматически запустятся десктопная версия TeamViewer и удаленная папка SMB, при открытии которой система отправит запрос NTLM аутентификации. Перехватив этот запрос, злоумышленник может выполнить код или использовать для взлома хеша.

Уязвимость затрагивает следующие заголовки URI: teamviewer10, teamviewer8, teamviewerapi, tvchat1, tvcontrol1, tvfiletransfer1, tvjoinv8, tvpresent1, tvsendfile1, tvsqcustomer1, tvsqsupport1, tvvideocall1 и tvvpn1.

Разработчики TeamViewer устранили уязвимость с выпуском обновлений для версий TeamViewer с 8 по 15. В настоящее время нет сведений об атаках, эксплуатирующих данную уязвимость, но, учитывая огромную популярность ПО, их следует ожидать уже в скором времени». ***(Уязвимость в TeamViewer позволяет***

удаленно украсть системный пароль // SecurityLab.ru (https://www.securitylab.ru/news/510976.php). 11.08.2020).

***

«Основатель сервиса Have I Been Pwned (HIBP) для проверки скомпрометированных паролей, решил открыть кодовую базу проекта…

Сервис Have I Been Pwned был запущен в 2013 году как инструмент кибербезопасности, позволяющий интернет-пользователям проверить свои аккаунты на предмет утечки учетных данных. Have I been pwned представляет собой реверсивную поисковую систему. Достаточно ввести свой адрес почты или пароли, и сервис покажет, фигурировали ли эти данные в известных утечках.

По словам Ханта, за прошедшие семь лет он вложил немало ресурсов в проект и больше не в состоянии поддерживать его в одиночку. Ранее эксперт подумывал о продаже HIBP, но сделка не состоялась, и Хант решил пойти альтернативным путем - открыть исходный код Have I Been Pwned, что, по его мнению, поможет усовершенствовать сервис

«Наиважнейшей целью этого процесса являлось обеспечение более устойчивого будущего для HIBP и это стремление не изменилось; проект не может всецело зависеть от меня и все же именно в таком положении мы сейчас находимся - если я исчезну, HIBP быстро завянет и умрет», - написал Хант.

В связи с невозможностью публикации проекта на GitHub в его текущем виде исходный код HIBP будет открываться поэтапно, однако когда он станет полностью доступен, пока неизвестно». ***(Трой Хант откроет исходный код сервиса Have I Been Pwned // SecurityLab.ru (https://www.securitylab.ru/news/510958.php). 10.08.2020).***

***

«Данные более 150 млн пользователей социальных сетей Facebook, LinkedIn и Instagram оказались в свободном доступе в сети. Об этом сообщает «РИА Новости» со ссылкой на основателя сервиса разведки утечек DLBI Ашота Оганесяна.

По его словам, система DLBI 25 августа обнаружила в свободном доступе сервер Elasticsearch, в индексах которого содержались данные указанных соцсетей.

Всего в утечках оказались 81,5 млн профилей пользователей пользователей Facebook (имя, ссылка на профиль, электронная почта, телефон, страна, данные по подписчикам), 66,1 млн профилей пользователей LinkedIn (имя, ссылка на профиль, электронная почта, страна, место работы, должность) и 11,6 млн профилей Instagram (имя, ссылка на профиль, электронная почта, телефон, страна, данные по подписчикам).

«База оказалась доступна для скачивания с открытого, благодаря неправильной конфигурации, сервера. Число российских пользователей в ней точно не известно, но, по нашим оценкам, относительно невелико, так как она собиралась в интересах китайских компаний, работающих на рынках Европы и США», — отметил Оганесян.

По его словам, утечка, вероятнее всего, произошла из-за неправильной конфигурации Elasticsearch-серверов, принадлежащих китайской компании Shenzhen Benniao Social Technology (socialarks.com), которая специализируется на сборе лидов из социальных сетей.

«Эта база не представляет большой опасности, так как в ней содержатся только открытые данные пользователей социальных сетей, собранные парсером со страниц их профилей», — добавил он». ***(Анастасия Марьина. Данные более 150 млн пользователей Facebook, LinkedIn и Instagram оказались в сети — DLBI // Rusbase (https://rb.ru/news/leak-social-networks/). 28.08.2020).***

***

«Freepik, один из популярнейших сайтов в интернете (занимает 97 место в топ-100 по версии Alexa), подвергся взлому. Согласно официальному заявлению компании, неизвестные злоумышленники воспользовались SQL-инъекцией и получили доступ к БД с пользовательскими данными. В итоге хакеры смогли похитить имена пользователей и парольные хеши 8,3 млн клиентов сайтов Freepik и Flaticon. Когда именно произошла атака, не сообщается.

Представители Freepik пишут, что не ко всем учетным записям были привязаны пароли, поэтому в некоторых случаях взломщики похитили только email-адреса. Так, примерно 4,5 млн человек использовали для входа учетные записи Google, Facebook или Twitter.

Таким образом, были украдены логины и парольные хеши примерно 3,77 млн пользователей. Для паролей 3,55 млн пострадавших использовался bcrypt, а для остальных 229 000 — соленый MD5. В компании уверяют, что после взлома все парольные хеши были переведены на bcrypt.

Теперь компания занимается расследованием случившегося, вместе со специалистами из правоохранительных органов, а также уведомляет о случившемся пострадавших пользователей. Для тех людей, чьи пароли были хешированны с помощью MD5, был осуществлен принудительный сброс паролей, а те, чьи пароли были хешированы с помощью bcrypt, получили письма с информацией об инциденте и рекомендацию как можно быстрее сменить пароль». ***(Мария Нефёдова. Хакеры похитили данные 8 300 000 пользователей Freepik с помощью SQL-инъекции // Xakep (https://xakep.ru/2020/08/24/freepik/). 24.08.2020).***

***

«До 200 000 историй болезни из Office 365 и Google G Suite с жестко заданными учетными данными и другими ненадлежащими элементами управления доступом.

Ошибка разработчика вызвала утечку от 150 000 до 200 000 медицинских карт пациентов, хранящихся в приложениях для повышения производительности от Microsoft и Google, которые недавно были обнаружены на GitHub .

Голландский исследователь Джелле Урсем обнаружил девять отдельных файлов с конфиденциальной личной медицинской информацией (PHI) из таких приложений, как Office 365 и Google G Suite, из девяти отдельных организаций здравоохранения. Ему было трудно связаться с компаниями, чьи данные были

утечками, и поэтому в конечном итоге он сообщил о взломе DataBreaches.net, который вместе с ним опубликовал совместный документ «Нет взлома, когда он утекает», посвященный результатам.

Название относится к открытию того, что информация была раскрыта не в результате атаки или несанкционированного доступа в системы здравоохранения, а из-за неправильной конфигурации разработчиками средств управления доступом и жестко закодированных учетных данных при хранении информации, говорится в документе.

К числу ошибок, допущенных разработчиками, относятся: встраивание жестко заданных учетных данных для входа в код вместо того, чтобы делать их параметром конфигурации на сервере, на котором выполняется код; использование публичных репозиториев вместо частных репозиториев; отказ от использования двухфакторной или многофакторной аутентификации для учетных записей электронной почты; и / или отказ от репозиториев вместо того, чтобы удалять их, когда они больше не нужны, писали они.

Урсем, самопровозглашенный «самый хромой хакер, которого вы знаете», обнаружил утечку информации с помощью простого поиска, чтобы узнать, действительно ли кто-то «достаточно глуп, чтобы загружать данные о медицинских клиентах на GitHub», - сказал он DataBreach.net. GitHub - это онлайн-платформа для разработки программного обеспечения и контроля версий.

Ему потребовалось менее 10 минут, чтобы найти открытые данные с помощью вариаций простых поисковых фраз, таких как «пароль от medicaid FTP», чтобы найти «потенциально уязвимые жестко запрограммированные имена пользователей и пароли для систем», - пишут исследователи. По их словам, Урсем может легко получить доступ к системам здравоохранения и файлам, используя открытые учетные данные.

«Не имеет значения, относятся ли учетные данные, которые находит Урсем, к базе данных, учетной записи Office365 или Gmail или узлу безопасной передачи файлов», - говорится в документе. «Вы просто указываете нужное программное обеспечение и нажимаете «подключиться», - сказал Урсем DataBreach.net. "Это действительно так просто."

Более того, по словам исследователей, данные пациентов не только были обнаружены из-за распространенных ошибок, но и оставались незамеченными в течение нескольких месяцев из-за небрежной политики безопасности в компаниях, отвечающих за данные.

Компаниям не удалось провести простой аудит безопасности - например, безопасность своих разработчиков и соответствие политикам или предоставить контролируемую учетную запись для исследователей, чтобы они могли сообщать о проблемах безопасности, - что позволяло данным оставаться открытыми без ведома компании.

Компании также не отреагировали на попытки DataBreach.net ответственного раскрытия информации из опасения, что полученные уведомления были атаками социальной инженерии, что еще раз демонстрирует слабую политику в отношении защиты их данных, пишут исследователи.

Данные пациентов, найденные в файлах, были получены от медицинских организаций Xybion, MedPro Billing, Texas Physician House Calls, VirMedica, MaineCare, Waystar, Shields Health Care Group, AccQData и еще одной компании, которая описана в отчете, но не названа.

В отчете описывается один заблудший разработчик, которого называют «Тифозная Мэри утечек данных» из-за множества ошибок и повторения этих ошибок при использовании GitHub в отношении не только хранения и управления медицинскими данными, но и другими файлами.

«Казалось, что если бы этот разработчик мог сделать что-то не так или что-то испортить, он бы сделал это», - пишут исследователи. «И он, казалось, на удивление не осознавал, что все, что он делал, было видно другим».

Исследователи обнаружили, что GitHub даже поразил разработчика запросом DMCA на удаление электронной книги, которую он ненадлежащим образом поделился еще в 2018 году, но он продолжал раскрывать данные и платформы, с которыми работал на сайте.

«Если бы это уведомление об удалении не было тревожным сигналом, чтобы другие могли увидеть всю его работу, мы не знаем, что бы это было», - написали они.

В целом отчет еще раз демонстрирует, насколько часто данные оказываются в облаке, когда не установлены надлежащие средства защиты и контроля.

Разработчики, работающие на таких платформах, как GitHub, должны проявлять особую бдительность при работе с конфиденциальными данными клиентов, и компании также должны принимать надлежащие меры, чтобы знать, у кого есть доступ к их данным, где и на каких платформах они используются. сказали исследователи.

Исследователи предупреждают, что даже если сама компания не использует GitHub или даже не знает о его существовании, это не означает, что ее данные не публикуются на сайте. «Один из ваших поставщиков или деловых партнеров может иметь сотрудника, использующего его, как один провайдер обнаружил на собственном горьком опыте», - писали они». ***(Elizabeth Montalbano. Medical Data Leaked on GitHub Due to Developer Errors // Threatpost (https://threatpost.com/medical-data-leaked-on-github-due-to-developer-errors/158653/). 26.08.2020).***

***

Кібербезпека Інтернету речей

«Эксперты CyberNews рассказали о недавно проведенном ими эксперименте, посвященном небезопасности IoT-устройств в целом и принтеров в частности. Стоит отметить, что многие ИБ-специалисты уже осудили команду CyberNews из-за неэтичности данного теста.

Исследователи утверждают, что при помощи поисковика Shodan они выявили в интернете более 800 000 принтеров с включенными функциями сетевой печати, причем порядка 447 000 были не защищены от атак.

Для проведения эксперимента исследователи отобрали из 800 000 доступных принтеров 50 000 случайных устройств, к которым попытались получить доступ (с помощью автоматизированного скрипта) и заставить их распечатать руководство по безопасности.

В итоге специалисты отчитались о том, что скомпрометировали 27 944 принтера из 50 000 (то есть успешными оказались 56% атак), напечатав на них листовки с предупреждением о небезопасности. Исходя из этой цифры исследователи предполагают, что из 800 000 подключенных к интернету принтеров по меньшей мере 447 000 являются незащищенными.

Нужно отметить, что массовая компрометация уязвимых принтеров ради печати какой-либо агитации или весьма сомнительных пранков – вовсе не новость. К примеру, в 2016 году известный black hat Эндрю Ауэрнхаймер (Andrew Auernnheimer), также известный под ником Weev, точно так же скомпрометировал десятки тысяч принтеров и заставил их печатать листовки антисемитского содержания. Еще один похожий случай произошел в 2017 году, тогда неизвестный атакующий заставил 150 000 принтеров распечатать послания с ASCII-графикой. А в 2018 году хакер, скрывающийся под ником TheHackerGiraffe, взломал около 50 000 принтеров, распечатав на них листовки с призывами подписываться на YouTube-канал PewDiePie». ***(Мария Нефёдова. Исследователи взломали 28 000 принтеров, чтобы привлечь внимание к их небезопасности // Хакер (https://xakep.ru/2020/08/28/printers-hack/). 28.08.2020).***

***

Кіберзлочинність та кібертероризм

«Одна з найбільших американських компаній, виробник віскі Jack Daniel's, Brown-Forman постраждала від кібератаки…

Brown-Forman всесвітньо відома брендами віскі - Jack Daniel's, Woodford, Old Forester, Collingwood, Glenglassaugh, Glendronach, текіли - Herradura, El Jimador, Pepe Lopez, горілки - Finlandia і вина - Sonoma-Cutrer.

Штаб-квартира компанії знаходиться в місті Луїсвілл, штат Кентуккі.

Вказується, що в п'ятницю оператори вимагача REvil (Sodinokibi) заявили, що скомпрометували комп'ютерну систему Brown-Forman і більше місяця вивчали дані компанії.

Хакери стверджують, що викрали 1 ТБ інформації про співробітників, контракти, контакти і фінансові компанії.

Зловмисники нібито вимагають викуп, погрожуючи продажем даних.

Вказуються, що в Brown-Forman підтвердили кібератаку, але заявили, що переговорів з хакерами не ведуть…». ***(Петро Івасюк. Хакери зламали найбільшого алковиробника // Інформаційне агентство «Українські Національні***

Новини» (https://www.unn.com.ua/uk/news/1886507-khakeri-zlamali-naybilshogo-alkovirobnika). 17.08.2020).

***

«С апреля по июнь количество DDoS-атак во всем мире увеличилось втрое по сравнению с аналогичным периодом 2019 г., по данным «Лаборатории Касперского». Главными мишенями стали образовательные и государственные учреждения. При этом число атак на первый сектор сократилось во второй половине июня (вероятно из-за начала школьных и студенческих каникул).

Пики активности киберзлоумышленников пришлись на 1 апреля (в этот день зафиксировано 287 атак) и 9 апреля (298 атак). Также дважды – 13 и 16 мая – количество атак превышало рекордные значения за два прошлых квартала.

Эксперты отмечают, что такая высокая динамика противоречит общей тенденции: как правило, наибольший объем DDoS-атак фиксируют зимой, то есть в высокий сезон для бизнеса, а весной и летом, наоборот, наблюдается спад. Например, количество атак во II квартале 2019 г. снизилось на 39% по сравнению с показателями I квартала 2019 г., а в 2018 г. разница между двумя кварталами составила 34%. Этот же год стал исключением из правил: во II квартале 2020 г. среднее число атак выросло по сравнению с январем-мартом на 30%.

Ограничительные меры по борьбе с пандемией, которые во втором квартале частично или полностью сохранялись во многих странах, привели к перемещению многих процессов в онлайн: чаще, чем раньше, люди использовали цифровые ресурсы как в личных, так и в рабочих целях. В итоге, увеличилось количество возможных целей для DDoS и наблюдался беспрецедентный рост мусорного трафика. По всей видимости, третий квартал в этом плане пройдет не менее напряженно». ***(Количество DDoS-атак во втором квартале выросло втрое // Компьютерное Обозрение (https://ko.com.ua/kolichestvo_ddos-atak_vo_vtorom_kvartale_vyroslo_vtroe_134150). 18.08.2020).***

***

«Исследователи компании Check Point Software Technologies подготовили отчет о брендах, которые чаще всего использовались в фишинговых атаках во втором квартале. В подобных атаках хакеры имитируют официальный веб-сайт известного бренда, используя аналогичный домен или URL-адрес. Хакеры используют различные методы для распространения ссылок на фейковые веб-сайты, перенаправляя пользователей во время просмотра веб-страниц. Как правило, цель хакера – кража учетных данных, личной информации или платежей.

Чаще всего во второй четверти хакеры имитировали Google и Amazon, – а бренд Apple (который занял первое место в I квартале) опустился на седьмое место. Общее количество всех попыток фишинга брендов остается примерно таким же, как и в первом квартале. Ниже приведены 10 брендов, которые ранжированы по частоте использования в фишинговых атаках во втором квартале: Google (13%);

Amazon (13%); WhatsApp (9%); Facebook (9%); Microsoft (7%); Outlook (3%); Apple (2%); Netflix (2%); Huawei (2%); PayPal (2%).

Фишинг по электронной почте – второй наиболее распространенный тип мошенничеств после веб-фишинга. В первом квартале он был на третьем месте. Причиной роста может быть ослабление глобальных ограничений, связанных с Covid-19: сейчас уже многие предприятия открыты, а сотрудники вернулись на работу в офисы. Фишинговые эксплойты, составляющие почти четверть (24%) всех фишинговых атак, направлены на Microsoft, Outlook и Unicredit.

Почти 15% фишинговых атак направлены на смартфоны. В таких атаках злоумышленники чаще всего маскируются под Facebook, WhatsApp и PayPal.

В конце июня исследователи Check Point обнаружили фишинговый веб-сайт, который имитировал страницу входа в облачные сервисы Apple – iCloud. Цель этого веб-сайта – попытаться украсть учетные данные для входа в iCloud. Его домен – «account-icloud [.]com». Домен впервые был активен в конце июня и зарегистрирован под IP – 37.140.192.154, расположенным в России.

В мае исследователи Check Point обнаружили фейковый веб-сайт, который имитировал страницу входа в PayPal. Адрес сайта был paypol-login[.]com. Домен под IP в США 52.22.86.101 впервые зарегистрирован в 2018 г. и использовался в конце мая.

Как оставаться в безопасности:

Используйте оригинальные сайты. Убедитесь, что вы находитесь, используете, вводите данные только на подлинных сайтах. Не нажимайте на рекламные ссылки в электронных письмах – ищите вместо этого в Google нужного вам продавца и переходите по ссылке на странице результатов поиска;

Избегайте «специальных» предложений. Скидка 80% на новый iPhone – это подозрительное предложение и вряд ли является правдой;

Остерегайтесь похожих доменов. Следите за орфографическими ошибками в электронных письмах или на сайтах.

Фишинг в цифрах:

Предполагается, что с фишинга начинаются более 90% всех кибератак;

Почти треть (32%) фактических нарушений данных связана с фишингом (по данным Verizon);

Фишинг замечали в 78% случаев кибершпионажа, а также при установке и использовании бэкдоров для сетей (отчет Verizon – PDF, EN)». ***(Почти 15% фишинговых атак направлены на смартфоны // Компьютерное Обозрение (https://ko.com.ua/pochti_15_fishingovyh_atak_napravleny_na_smartfony_134042). 07.08.2020).***

***

«Как сообщает издание BleepingComputer, американские сайты и сервисы Canon оказались взломаны и до сих пор не работают.

Представители компании пока не подтвердили официально информацию о взломе, но сайт, отвечающий за работу Canon в США не работает до сих пор, спустя уже пять часов после первого сообщения о проблемах. В компании информацию о вымогательстве не подтверждают.

По данным BleepingComputer, в результате атаки блокирована электронная почта компании, Microsoft Teams и работа некоторых корпоративных сервисов.

Якобы за атакой на Canon стоит хакерская группировка Maze, которая требует выкуп за восстановление работы компании…». ***(Сайты и сервисы Canon в США подверглись атаке шифровальщика // Компьютерное Обозрение (https://ko.com.ua/sajty_i_servisy_canon_v_ssha_podverglis_atake_shifrovalshhika_134037). 06.08.2020).***

***

«Эксперты Akamai предупредили о новой волне DDoS-вымогательства. Хакеры шантажируют компании, угрожая DDoS-атаками, и выдают себя за такие известные хакерские коллективы, как Fancy Bear и Armada Collective.

По данным специалистов, вымогательские атаки начались около недели назад, и они нацелены на самые сферы, включая финансовый сектор и розничные продажи. Подобно DDoS-шантажистам прошлых лет, злоумышленники связываются с компаниям и предупреждают их о грядущей DDoS-атаке, которая произойдет, если компания-жертва не выплатит выкуп. В некоторых случаях злоумышленники также пишут о том, что вымогательские требования нужно держать втайне, а в противном случае угрожают начать DDoS-атаку немедленно.

«Если вы сообщите об этом СМИ и попытаетесь получить бесплатную рекламу, используя наше имя, вместо того, чтобы заплатить, атака начнется немедленно и будет длиться очень долго», — предупреждают злоумышленники, представляющиеся Armada Collective.

Группировка, называющая себя Armada Collective, требуют заплатить выкуп в размере 5 BTC (или 10 BTC по истечении отведенного срока). Хакеры предупреждают, что сумма будет увеличиваться на 5 BTC в день, пока выкуп не будет оплачен.

В свою очередь, злоумышленники, которые называют себя Fancy Bear, требуют 20 BTC в качестве выкупа (или 30 BTC по истечении отведенного срока). После этого сумма будет увеличиваться на 10 BTC каждый день.

Более того, в посланиях шантажисты утверждают, что способны устраивать DDoS-атаки мощностью до 2 Тбит/сек.

Эксперты Akamai говорят, что эти группировки, конечно, являются лишь подражателями и не имеют никакого отношения к настоящим Fancy Bear и Armada Collective. Репутацию известных хак-групп эти преступники используют лишь в качестве средства запугивания, чтобы жертвы охотнее и быстрее платили выкуп. На самом деле эти хакеры могут оказаться неспособны устроить даже слабую DDoS-атаку…». ***(Мария Нефёдова. DDoS-шантажисты выдают себя за Fancy Bear и Armada Collective // Xakep (https://xakep.ru/2020/08/19/ddos-extortion-2/). 19.08.2020).***

***

«Представители Carnival Corporation сообщили американской Комиссии по ценным бумагам и биржам, что 15 августа 2020 года компания подверглась атаке неназванного шифровальщика. Согласно поданным компанией

документам, злоумышленники получили доступ к системам неназванного дочернего бренда Carnival Corporation и зашифровали файлы на пострадавших машинах.

Кроме того сообщается, что хакеры похитили файлы из сети пострадавшей компании. В итоге считается, что злоумышленники могли получить доступ к личным данным некоторых сотрудников и клиентов.

Круизная компания уже занимается расследованием случившегося при содействии правоохранительных органов. Никаких технических подробностей об инциденте в Carnival Corporation пока не раскрывают, а также не сообщают, какой именно шифровальщик стоял за этой атакой.

При этом эксперты компании Bad Packets рассказали журналистами издания Bleeping Computer, что Carnival Corporation могла быть взломана благодаря уязвимости CVE-2019-19781, которая затрагивает ряд версий Citrix Application Delivery Controller (ADC), Citrix Gateway, а также две старые версии Citrix SD-WAN WANOP. Эту проблему обнаружили еще в конце 2019 года, и уже тогда аналитики предупреждали, что в открытом доступе можно обнаружить более 80 000 уязвимых серверов, то есть проблема угрожали десяткам тысяч компаний из 158 странах мира.

Также, по мнению специалистов, проблема могла заключаться в уязвимости CVE-2020-2021, обнаруженной в PAN-OS, операционной системе, работающей на брандмауэрах и корпоративных VPN-устройствах производства Palo Alto Networks.

В настоящее время Carnival Corporation является крупнейшей в мире мультинациональной круизной туристической компанией. Она объединяет более 20 дочерних круизных компаний, включая Carnival Cruise Lines, Princess Cruises, Holland America Line и Seabourn Cruise Line, P&O Cruises, Cunard Line, Ocean Village, AIDA Cruises, Costa Cruises и P&O Cruises Australia.

Carnival Corporation принадлежат более 600 судов, а в штате компании работают 150 000 сотрудников, ежегодно обслуживающих более 13 000 000 человек». ***(Мария Нефёдова. Крупнейшая в мире круизная компания Carnival Corporation пострадала от вымогательской атаки // Xakep (https://xakep.ru/2020/08/18/carnival-corporation-hack/). 18.08.2020).***

***

«Специалисты Group-IB сообщают, что с начала августа 2020 года три крупных благотворительных организации подверглись атакам с использованием спуфинга адреса электронной почты. Также эксперты выявили следы готовящихся кампаний против еще 7 благотворительных организаций.

В ходе атак злоумышленники отправляли поддельные письма от лица руководителей благотворительных фондов их коллегам, например, из финансового отдела, с просьбой срочно оплатить лечение кого-то из подопечных организации.

К примеру, 3 августа трое сотрудников Благотворительного фонда Константина Хабенского получили письмо, якобы написанное директором благотворительной организации, с просьбой немедленно перевести средства, собранные для одного из подопечных фонда, на указанные реквизиты.

Подозрительное сообщение насторожило команду фонда. Дело в том, что благотворительная организация никогда не осуществляет переводов на личные банковские счета и персональные кошельки, получатели переслали письмо для проверки на предмет мошенничества в Group-IB.

Анализ показал, что подлинный почтовый аккаунт директора фонда скомпрометирован не был. Злоумышленники отправили письмо с сервера хостинг-провайдера Timeweb, подделав технический заголовок под нужный адрес, чтобы ввести в заблуждение сотрудников фонда. При этом в поле «обратный адрес» (данная строка видна не во всех почтовых клиентах) вместо официального домена фонда Хабенского bfkh[.]ru использовался фальшивый домен, отличающийся последовательностью букв: bfhk[.]ru. Если бы пользователь ответил на письмо, например, для уточнения деталей перевода, его сообщение направилось бы мошенникам.

Три дня спустя экспертам специалистам CERT-GIB стало известно об аналогичной попытке вывести средства из фонда «Кислород». Рассылка в адрес сотрудников была зафиксирована 6 августа, для нее киберперступниками специально был зарегистрирован домен bfkislorod[.]ru (домен оригинального сайта bf-kislorod[.]ru). Примечательно, что перед атаками сотрудники Фонда Хабенского и фонда «Кислород», от лица которых потом рассылались фейковые письма, получили email-сообщения от одного и того же лица с абстрактными вопросами. Предположительно, мошенники сделали это для того, чтобы создать полностью идентичные профили для будущей рассылки — скопировать фото, данные о корпоративной подписи и так далее.

Изучив домен bfkislorod[.]ru с помощью системы графового анализа, эксперты обнаружили, что в период с 5 по 6 августа злоумышленники зарегистрировали еще семь доменов, копирующих имена известных благотворительных организаций, в том числе фондов «Алеша», «Подари жизнь» и «Старость в радость». По состоянию на 19 августа 2020 года попытка мошенничества была зафиксирована только в отношении фонда «Старость в радость». Остальные шесть доменов на данный момент остаются «спящими» и находятся на мониторинге у специалистов CERT-GIB.

«С начала августа Group-IB фиксирует серию таргетированных атак на благотворительные организации. Для фондов подобные атаки имеют куда более серьезные последствия, чем для других организаций, т.к. они наносят удар по их главному активу — человеческому доверию. Для нашей компании работа над этим кейсом имеет особую важность, поскольку в данном случае речь идет не о репутационных и финансовых рисках, а зачастую — о шансах людей на жизнь», — говорит Ярослав Каргалев, заместитель руководителя CERT Group-IB.

На текущий момент специалисты Group-IB занимаются блокировкой развернутой злоумышленниками инфраструктуры, расследованием инцидентов и сбором информации о предполагаемых атакующих. Благодаря оперативному детектированию мошеннической схемы и бдительности сотрудников фондов, которые регулярно сталкиваются с новыми видами фрода, ущерба удалось избежать.

Чтобы минимизировать риски подобных атак, эксперты советуют организациям внедрить правила аутентификации SPF (Sender Policy Framework) и DKIM (DomainKeys Identified Mail), а также технологию проверки этих записей — DMARC. Это существенно усложнит отправку писем от имени официального домена — такие послания будут помечаться как не прошедшие аутентификацию, попадать в спам или вовсе отклоняться». ***(Мария Нефёдова. Group-IB обнаружила серию атак на благотворительные фонды // Xakep (https://xakep.ru/2020/08/20/charity-attacks/). 20.08.2020).***

***

«В начале текущей недели ИБ-специалист и оператор сервера Tor, известный как Nusenu, опубликовал результаты своего исследования. По его данным, с января 2020 года группа неизвестных лиц устанавливает контроль над выходными узлами Tor и осуществляет атаки типа SSL stripping. В какой-то момент им принадлежала четверть всех выходных узлов (380 серверов), а сейчас они контролируют около 10%, несмотря на то, что разработчики Tor трижды принимали меры для прекращения этой активности.

Исследователь пишет, что истинный масштаб операций этой группы неизвестен, но их главной целью определенно является получение прибыли. Nusenu объясняет, что злоумышленники осуществляют атаки man-in-the-middle на пользователей Tor и манипулируют трафиком, проходящим через подконтрольные им выходные узлы. Цель таких MitM-атак — применение техники SSL stripping, то есть даунгрейд трафика пользователей с HTTPS-адресов на менее безопасные HTTP.

По мнению специалиста, таким образом группировка подменяет биткоин-адреса внутри HTTP-трафика, связанного с миксер-сервисами. Подобные сервисы помогают «запутать следы», превращая простой перевод средств с одного аккаунта на другой в сложную схему: вместо одной транзакции сервис разбивает нужный платеж на сотни или тысячи мелких переводов, которые отправляются на разные аккаунты и проходят через множество кошельков, прежде чем достигнут истинной цели. То есть, подменяя адреса на уровне HTTP-трафика, злоумышленники эффективно перехватывают средства жертв, без ведома как самих пользователей, так и криптовалютных миксер-сервисов.

Сами по себе подобные атаки нельзя назвать новыми, но исследователь отмечает невиданный масштаб этой операции. Так, опираясь на контактный email-адрес вредоносных серверов, эксперт отследил по меньшей мере 9 кластеров входных узлов, добавленных за последние семь месяцев. Вредоносная сеть достигла своего пика 22 мая текущего года, когда в нее входили 380 серверов, и группировка контролировала 23,95% всех выходных узлов Tor.

Nusenu пишет, что он не раз сообщал администраторам Tor о вредоносных выходных узлах и после последней «зачистки», произошедшей 21 июня 2020 года, возможности злоумышленников сильно сократились. Впрочем, по состоянию на 8 августа 2020 года группировка по-прежнему контролировала около 10% выходных узлов.

По мнению исследователя, злоумышленники будут продолжать эти атаки и далее, так как у инженеров Tor Project нет возможности тщательно проверить всех присоединившихся к сети участников, ведь во главу угла ставится анонимность…». ***(Мария Нефёдова. Неизвестные хакеры контролировали 24% выходных узлов Tor // Xakep (https://xakep.ru/2020/08/11/exit-nodes-problem/). 11.08.2020).***

***

«Эксперты из Рурского университета и Нью-Йоркского университета в Абу-Даби опубликовали информацию об атаке ReVoLTE: у нее уже есть собственный сайт, а на конференции Usenix исследователи представили видеопрезентацию своего доклада.

Замечу, что ранее эта же исследовательская обнаружила проблему IMP4GT, которой подвержены практически все современные устройства с поддержкой LTE, то есть смартфоны, планшеты, IoT-устройства. Баг позволяет имитировать в сети оператора другого пользователя, а значит, злоумышленник сможет оформлять платные подписки за счет других людей или публиковать что-либо (к примеру, секретные документы) под чужой личиной.

Атака ReVoLTE строится на том, что многие операторы мобильной связи используют один и тот же ключ шифрования для защиты разных голосовых вызовов 4G, проходящих через одну базовую станцию. Ученые провели ряд «полевых испытаний» своей атаки, проанализировав работу случайных базовых станций по всей Германии, и оказалось, что 80% из них используют один и тот же ключ шифрования (или ключ, который легко предсказать), что подвергает пользователей риску.

Дело в том, что по умолчанию стандарт VoLTE поддерживает зашифрованные звонки, и для каждого вызова мобильные операторы должны выбрать свой ключ шифрования (потоковый шифр). В норме ключ должен быть уникальным для каждого вызова. К сожалению, выяснилось, что зачастую голосовые вызовы шифруются одним и тем же ключом или ключом, который легко предсказать.

Данная проблема обычно проявляется на уровне базовых станций, которые повторно используют один и тот же потоковый шифр или предсказуемые алгоритмы для генерации ключей шифрования. В итоге злоумышленник может записать разговор между двумя любыми пользователями 4G, подключенными к уязвимой базовой станции, а затем расшифровать его.

Всё, что требуется хакеру для реализации атаки — позвонить одной из жертв и записать разговор, чтобы этот вызов был зашифрован тем же (или предсказуемым) ключом шифрования. Единственное ограничение состоит в том, что атакующий должен быть подключен к той же базовой станции, что и его жертва, и должен действовать быстро: вызов атакующего должен быть выполнен примерно в течение 10 секунд после завершения целевого звонка.

Это можно проделать при помощи аппаратуры, чья суммарная стоимость составит около 7000 долларов. Хотя цена может показаться высокой, исследователи отмечают, что обычно интерцепторы для сетей 3G и 4G, которые

используют правоохранительные органы и преступные группы, стоят примерно столько.

«Чем дольше злоумышленник разговаривает со своей жертвой, тем больше он сумеет расшифровать из предыдущего разговора. Например, если злоумышленник и жертва говорили пять минут, позже злоумышленник сможет расшифровать пять минут предыдущего разговора», — объясняются исследователи. По сути, хакеру нужно лишь сравнить две записи и определить ключ шифрования.

Еще в декабре 2019 года исследователи сообщили о проблемах как немецким операторам мобильной связи, так и специалистам организации GSMA. В итоге GSMA выпустила обновления для протокола 4G, защищающие от атак ReVoLTE. Увы, эксперты отмечают, что даже если немецкие операторы мобильной связи и их пользователи теперь находятся в безопасности, то другие операторы по всему миру могут быть по-прежнему уязвимы.

Эксперты создали и опубликовали на GitHub специальное приложение для Android, которое операторы мобильной связи могут использовать для тестирования своих сетей и базовых станций на предмет уязвимости перед ReVoLTE. Для работы приложения требуется рутованное устройство, которое поддерживает VoLTE и работает на чипсете Qualcomm». ***(Мария Нефёдова. Атака ReVoLTE позволяет дешифровать и слушать чужие разговоры // Хакер (https://xakep.ru/2020/08/14/revolte/). 14.08.2020).***

***

«…Компанія Garmin, яка виготовляє розумні годинники, фітнес-браслети і техніки для GPS-навігації, заплатила «багатомільйонний» викуп хакерам, які влаштували атаку на онлайн-сервіси компанії. Про це повідомили джерела видання Sky News.

Видання не пише про суму “угоди”, але за даними ресурсу BleepingComputer мова може йти про $10 млн. Саме стільки вимагали хакери за відновлення доступу до сервісів компанії.

Як повідомляє Sky News, Garmin звернулася до фахівців з кібербезпеки, щоб домовитись з хакерами. Однак ніхто зі спеціалістів не погодився співпрацювати з хакерами, побоюючись санкцій з боку американської влади. Тоді компанія вирішила заплатити викуп через фірму Arete IR, щоб не потрапити під санкції США через угоди з хакерами.

За даними Sky News, до злому може бути причетна хакерське об’єднання з Росії Evil Corp. Воно знаходиться під санкціями США. Через це Garmin не змогла заплатити хакерам безпосередньо.

23 липня 2020 роки онлайн-сервіси, сайт і системи зв'язку Garmin були недоступними. Компанія змогла частково відновити доступ до своїх сервісів лише 27 липня. Garmin підтвердила, що пережила кібератаку. Деякі співробітники повідомляли, що роботу систем порушив вірус-вимагач WastedLocker…». ***(Garmin заплатила хакерам, щоб відновити доступ до своїх сервісів – ЗМІ // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/25195/2020-08-04-***

garmin-zaplatila-khakeram-shchob-vidnoviti-dostup-do-svoikh-servisiv-zmi/). 04.08.2020).

***

«Компания Group-IB обнаружила в сети свыше 200 мошеннических ресурсов, использующих названия брендов, в частности, сервисов по доставке еды, товаров для дома, средств индивидуальной защиты…

Эксперты Group-IB фиксировали фишинговые страницы, которые визуально полностью копировали официальные сайты.

«Разница была лишь в доменном имени: вместо домена верхнего уровня RU мошенники могли использовать другие домены, например, .space, а также видоизменять официальное название ресурсов доставки, добавляя дополнительные знаки препинания или используя буквенные сочетания, которые визуально схожи (например, aI(ai) al (al))», — сообщил собеседник агентства.

Проанализировав фишинговые ресурсы, специалисты обнаружили группу из более 200 связанных сайтов, незаконно использующих имена свыше 40 брендов, все из них созданы по одному и тому же шаблону. В числе них были сервисы по доставке еды, товаров для дома, средств индивидуальной защиты, и другие.

По данным Group-IB, злоумышленники заманивают пользователей на фишинговые ресурсы через контекстную рекламу с изображением известных брендов сервисов доставки или супермаркетов.

«Оказываясь на фейковой странице сервиса, пользователь оформляет заказ, после чего попадает на страницу оплаты, на которой оплатить заказ можно только картой. Таким образом, злоумышленники похищали не только сумму заказа со счета жертвы, но и получали данные банковских карт пользователей, которые могут быть ими использованы в будущем», — отметил представитель Group-IB.

Эксперт советует пользователям использовать официальные мобильные приложения сервисов по доставке еды и супермаркетов. Если заказ необходимо сделать на сайте, необходимо проверить доменное имя и регистрационные данные веб-ресурса (например, с помощью сервиса Whois)». ***(Анастасия Марьина. В сети найдено свыше 200 мошеннических ресурсов, использующих названия брендов // Rusbase (https://rb.ru/news/brands-fraud/). 06.08.2020).***

***

«Треть университетов Соединенного Королевства, ответивших на запрос о свободе информации (FOI), признали себя жертвой атаки с использованием программ-вымогателей. Это более 25% университетов и колледжей страны.

Инциденты произошли в последнее десятилетие, большинство из них - в период с 2015 по 2017 год. Несколько учебных заведений подверглись как минимум двум атакам с шифрованием файлов за последнее десятилетие, в одной из них было зарегистрировано более 40 атак с 2013 года.

Агентство цифрового пиара и SEO TopLine Comms 29 июня направило запрос о свободе информации в 134 университеты Великобритании, спрашивая, зафиксировали ли они атаку вымогателя, когда это произошло, заплатили ли они выкуп или нет, и какова сумма, если они это сделали. платить.

Люк Буда, глава компании, сказал BleepingComputer, что он отправил запросы после того, как узнал о том, что Калифорнийский университет в Сан-Франциско заплатил 1,4 миллиона долларов за дешифратор файлов от операторов вымогателей Netwalker.

Интерес проявился к университетам Russel Group, потому что их исследования указывают на наиболее ценную интеллектуальную собственность…

Из 104 ответивших организаций только 35 признали, что они были жертвой такого инцидента за последние десять лет, показали результаты TopLine Comms, а 42 отказались выполнить запрос, ссылаясь на раздел 31.1.a Закона о свободе информации., имея в виду «предотвращение или раскрытие преступления».

Многие университеты, подтвердившие наличие атаки с использованием программ-вымогателей, сообщили, что они сталкивались с атаками несколько раз, при этом университет Шеффилд-Халлам сообщил о рекордном количестве: 42 за последние семь лет.

Город, Лондонский университет (CUL) также зарегистрировал большее количество таких инцидентов: семь с 2014 года, последние два произошли в феврале 2017 года.

Школы, сообщившие о последних атаках программ-вымогателей, - это Университет Западного Лондона, который дважды сталкивался с инцидентами с использованием программ-вымогателей в начале 2020 года, а затем Хаддерсфилд с двумя инцидентами в июне и сентябре 2018 года.

Выкуп не выплачен

С другой стороны, большинство респондентов, подтвердивших, что они стали жертвами атак программ-вымогателей, заявили, что они не платили выкуп злоумышленникам, указывая на то, что они восстановили затронутые системы из резервных копий, хотя некоторые были более сдержанными и отказались отвечать.

Однако результаты FOIA плохо отражают недавний период, поскольку почти половина всех школ, получивших запрос, отказалась предоставить какую-либо информацию, мотивируя это опасениями, что признание атаки только поощрит хакеров.

Тем не менее, они сказали, что их молчание не следует интерпретировать как признание или отрицание нападения. Оксфордский университет, например, заявил, что «успешное нападение [на них] будет тогда рассматриваться в криминальных кругах как заслуживающее внимания достижение, особенно с учетом высокого общественного авторитета Оксфорда». ***(Ionut Ilascu. Over 25% of all UK universities were attacked by ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/over-25-percent-of-all-uk-universities-were-attacked-by-ransomware/). 14.08.2020).***

***

«Компания Brown-Forman, производитель виски Jack Daniel’s, подверглась атаке киберпреступной группировки Sodinokibi, известной также под названием REvil. Для атаки использовался вирус-шифровальщик, но представители компании говорят, что им удалось предотвратить шифрование данных. Несмотря на это злоумышленники смогли украсть около 1 ТБ информации

и будут шантажировать ей компанию и принуждать к уплате выкупа. В этом почерк группы схож с почерком известной группировки Maze. Сейчас активных переговоров с преступниками компания не ведет, а специалисты мирового класса работают над расследованием и смягчением последствий». ***(Производитель Jack Daniel's подвергся кибератаке с крупной утечкой // SecureNews (https://securenews.ru/producer-jack-daniels-was-hit-by-a-cyberattack-with-a-major-leak/). 17.08.2020).***

***

«Злоумышленники взломали один почтовый аккаунт сотрудника SANS Institute и вывели существенное количество данных о работниках этого учреждения. SANS бросил весь свой арсенал на расследование.

Всего один ящик

SANS Institute, одна из крупнейших в мире организаций, занимающихся обучением специалистов по информационной безопасности, сама пострадала от кибератаки. Злоумышленники смогли осуществить утечку данных из SANS после того, как один из ее кадровых сотрудников попался на фишинговую атаку.

В сообщении, которое SANS опубликовал на своем сайте, говорится, что в результате успешной атаки злоумышленники смогли получить доступ к почтовому ящику сотрудника.

«Мы смогли обнаружить одиночное фишинговое письмо в качестве вектора атаки. В результате пострадал почтовый ящик отдельно взятого работника. Помимо него, по нашим данным, никакие другие аккаунты или системы в SANS не были скомпрометированы», — говорится в заявлении.

Злоумышленник, однако, настроил перенаправление всей корреспонденции, получаемой на атакованный ящик, на какой-то другой адрес и установил вредоносный аддон для Office 365.В SANS не уточнили, какой именно аддон имелся в виду, но, как предполагает издание Bleeping Computer, речь идет об Oauthapp, позволяющем обеспечить злоумышленнику длительный доступ к почтовому ящику жертвы.

В общей сложности на сторону утекли 513 сообщений, содержащих персональные данные связанных с SANS людей. Всего таким образом утекло 28 тыс. записей.

В сообщении SANS указывается, что на расследование инцидента брошен весь имеющийся у института арсенал киберкриминологических средств. Кроме того, представители организации обещают провести открытый онлайновый семинар, посвященный случившемуся и выводам, сделанным в результате расследования.

Ценные данные

В SANS утверждают, что ни паролей, ни платежной информации в этих записях не было. Зато были полные имена, телефонные номера, физические адреса, должности, названия компаний-работодателей и адреса электронной почты.

«Все эти данные легко можно использовать для проведения фишинговых и спиэр-фишинговых атак, — указывает Анастасия Мельникова, эксперт по информационной безопасности компании SEC Consult Services. — Подобные

данные ценятся меньше платежной информации, но для целевых атак на людей и юрлиц они оказываются крайне полезными. А то, насколько эффективными остаются фишинговые атаки, видно из данной ситуации с SANS: уж кого-кого, а сотрудника подобной организации вряд ли так просто обвести вокруг пальца. И тем не менее, атака оказалась успешной». ***(Хакеры разгромили главный учебный центр мира по борьбе с киберкриминалом // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5686290-Xakery-razgromili-glavnyj-uchebnyj.html). 13.08.2020).***

***

«Количество кибератак на компоненты ПО с открытым исходным кодом выросло на 430% в годовом выражении. Об этом сообщается в ежегодном отчете компании Sonatype "Состояние цепочки поставок программного обеспечения" (State of the Software Supply Chain).

Согласно отчету, киберпреступники нацелились на компоненты с открытым исходным кодом, осуществляя атаки на цепочки поставок. Эта тенденция вызывает опасения, поскольку популярность проектов с открытым исходным кодом неустанно растет среди DevOps-специалистов, желающих сократить срок выхода своих продуктов на рынок. Так, в 2020 году прогнозируется 1,5 триллиона запросов на загрузку компонентов во всех основных экосистемах с открытым исходным кодом.

В общей сложности специалисты Sonatype проанализировали 24 тыс. пректов с открытым исходным кодом и 15 тыс. компаний-разработчиков, а также опросили 5,6 тыс. разработчиков ПО.

С июля 2019-го по май 2020 года на компоненты с открытым исходным кодом было зафиксировано 929 атак. Чаще всего злоумышленники атаковали репозитории Node.js (npm) и Python (PyPI), поскольку вредоносный код может быть легко запущен в процессе инсталляции пакета.

Подобный вид атак возможен, поскольку в мире открытого кода труднее отличить хороших участников от плохих, а также из-за взаимосвязанного характера проектов, пояснили специалисты Sonatype. Во втором случае проекты с открытым исходным кодом могут иметь сотни или тысячи зависимостей от других проектов, содержащих известные уязвимости.

Согласно отчету, в 2019 году более 10% загрузок Java OSS по всему миру содержали по крайней мере один уязвимый компонент. В настоящее время 90% компонентов в приложениях являются проектами с открытым исходным кодом, и 11% из них содержат известные уязвимости». ***(Число кибератак на компоненты с открытым исходным кодом выросло на 430% // SecurityLab.ru (https://www.securitylab.ru/news/511148.php). 13.08.2020).***

***

«Фондовая биржа Новой Зеландии (NZX) подверглась атакам распределенного отказа в обслуживании (DDoS) в течение последних двух дней, что вынудило ее закрыть торговлю до тех пор, пока не будут решены проблемы с подключением.

NZX управляет рынками капитала, рисков и товаров Новой Зеландии, а также предоставляет рыночную информацию, включая котировки акций в реальном времени, рыночные данные и новости.

DDoS-злоумышленники дважды ломали сервисы NZX

Около 7 часов утра фондовый рынок объявил, что смог восстановить услуги после того, как вчера днем ему пришлось остановить денежные рынки после того, что он назвал объемной DDoS-атакой.

«Вчера днем NZX испытала объемную DDoS-атаку (распределенный отказ в обслуживании) из офшоров через своего поставщика сетевых услуг, которая повлияла на возможность подключения к сети NZX», - говорится в сообщении на веб-сайте фондовой биржи.

«Затронутые системы включали веб-сайты NZX и платформу объявлений о рынках. Таким образом, NZX решила прекратить торговлю на своих денежных рынках примерно по цене 15,57. [..] Атаку удалось смягчить, и теперь подключение к NZX было восстановлено».

Однако повторяющаяся с сегодняшнего дня DDoS-атака вынудила NZX снова прекратить торговлю в 11:14 после того, как пострадали веб-сайты NZX и платформа объявлений Markets.

Четыре часа спустя, в 15:00, основная площадка NZX, рынок долговых обязательств NZX и рынок акционеров Fonterra, которые должны были быть закрыты, вернулись к нормальной работе после завершения атаки и восстановления связи.

Согласно отчету NZ Herald, NZX позже заявила, что «поддерживает тесный контакт с участниками рынка и ценит поддержку и уровень понимания в периоды сбоев в торговле».

DDoS-сервисы по найму под огнем

Хотя в предупреждениях NZX не указывается источник угрозы, стоящий за атакой, или метод, использованный для запуска DDoS-атак, высока вероятность того, что они использовали услуги сайтов, предлагающих услуги DDoS-наем (также известные как стрессеры или ускорители).

В последнее время правоохранительные органы по всему миру закрывают десятки загрузчиков, используемых шутниками, злоумышленниками или хактивистами для запуска крупномасштабных DDoS-атак на онлайн-сервисы и сайты.

Например, группа по борьбе с киберпреступностью голландской полиции в течение одной недели в начале апреля в рамках совместных операций с внешними сторонами, включая хостеров или регистраторов, другие международные полицейские силы, Европол, Интерпол и ФБР, ликвидировала 15 бустеров.

Помимо уничтожения стрессоров, правоохранительные органы также выслеживают тех, кто их использует. Сотни лиц уже находятся под следствием после операции «Выключение питания».

В рамках этой операции в апреле 2018 года был отключен загрузчик WebStresser, служба, у которой на момент закрытия было зарегистрировано 151 000 пользователей. После этого компания Link11 сообщила, что количество DDoS-атак снизилось примерно на 60% по всей Европе.

Согласно отчету «Лаборатории Касперского», финансовое воздействие инцидента DDoS на малый бизнес может составить до 120 000 долларов, в то время как более крупным организациям может потребоваться в среднем 2 миллиона долларов на восстановление сервисов после каждой атаки». ***(Sergiu Gatlan. New Zealand stock exchange halted trading after DDoS attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-zealand-stock-exchange-halted-trading-after-ddos-attacks/). 26.08.2020).***

***

«Торговая площадка в темной паутине Empire недавно внезапно ушла из-под сильной кампании DDoS-атак и попыток вымогательства.

Согласно последним сообщениям, администраторы сайтов Empire изо всех сил пытались удержать операцию на плаву, и недавний удар кибератак не оставил им другого выбора, кроме как положить конец незаконному рынку с мрачной возможностью его возвращения.

Где следующая остановка?

Когда многие клиенты и продавцы остались в неведении (без каламбура) о местонахождении Empire, а их деньги застряли на депонировании, каков будет их следующий план действий?

Достаточно сказать, что внезапное исчезновение Empire подорвало доверие пользователей даркнета к так называемым системам условного депонирования, используемым на этих торговых площадках.

Израильская компания по мониторингу киберугроз, KELA, предоставила BleepingComputer информацию по этому поводу вместе со скриншотами.

Компания проанализировала форумы, на которых часто бывают серферы даркнета, и поделилась своими идеями.

"Проанализировав несколько сообщений на форумах, таких как Dread и TheHub, где участники даркнета свободно общаются, мы заметили, что, похоже, существует консенсус в отношении того факта, что большинство пользователей, вероятно, начнут переносить свои действия и сообщения на следующие три популярных подпольные сайты: Versus, White House Market и Icarus, а также приложение для обмена сообщениями Wickr», - заявляет Виктория Кивилевич, аналитик по анализу угроз в KELA…

В другом сообщении на форуме, предоставленном KELA, один из «бывших продавцов Empire», Arbeitsamt заявил, что они потеряли 5000 евро из-за внезапного выхода с рынка.

«Я практически лишился своего жизненного существования. Мой основной источник дохода. Я был настолько предан своему делу, поскольку у Empire был такой большой трафик, что это просто работало», - сказал продавец, объявив о планах потенциально присоединиться к Monopoly.

Хотя есть упоминания о Monopoly и Torrez, аналитик полагает, что этот выбор будет второстепенным, поскольку упомянутые выше рынки будут иметь приоритет.

«Кроме того, мы заметили, что некоторые из них также упоминали о переходе в «Монополию» или «Торрес», однако, это не были главные из

обсуждаемых вопросов. Ниже мы включили несколько скриншотов, показывающих болтовню между членами Empire о том, куда идти дальше», - продолжил Кивилевич.

Представляем бесплатные рынки

Судя по болтовне на форумах в дарквебе, похоже, что некоторые незаконные торговые площадки, такие как Icarus, хотят отказаться от платы, чтобы привлечь покровителей Empire.

Однако не гарантируется, что эти альтернативные торговые площадки защищены от угроз вымогательства и DDoS-атак, как те, которые привели к краху Empire.

«Рынок Icarus, по-видимому, размахивает [sic] гонорарами поставщиков, чтобы продавцы пришли после закрытия империи, я уверен, что он выдержит большую часть падения. Единственное, что на самом популярном рынке - это все ddos-атаки, которые обязательно последую, не думайте, что я буду куда-то спешить в течение 1-й недели или 2-х, если возможно», - заявил один пользователь.

Еще одно сообщение на форуме пришло от продавца, который утверждает, что обеспечивает «отслеживаемый лучший кокаин в Европе с доставкой из Германии».

Сообщение заверило потенциальных клиентов, что продавец не имел намерений кого-либо обманывать или исчезать с деньгами, и что они сами сильно пострадали от «аферы с выходом» Empire.

Но что еще более важно, поставщик делится подробностями своего возрождения на Wickr и White House Market.

Жулики с этикой?

В довольно ироничном сообщении на форуме, опубликованном KELA, счастливый клиент, получивший продукт, предлагал заплатить «250 долларов из этих 16 тысяч долларов», за которые, по их мнению, они несут ответственность, учитывая, что условное депонирование, ранее поддерживаемое Empire, исчезло.

«Хотел бы я сделать [sic] полностью подходящим для вас. Продукт действительно приземлился и выглядит хорошо. Я обязательно найду вас в ближайшее время на WH», - сказал пользователь, поделившись своим планом посетить Белый дом (WH) Рынок следующий.

Empire Market был одним из крупнейших и самых популярных незаконных мест в даркнете, торгующих незаконными наркотиками, химикатами, поддельными товарами, ювелирными изделиями и номерами кредитных карт, предлагая при этом способы оплаты, включая биткойны (BTC), Litecoin (LTC) и Monero (XMR).

Хотя многочисленные DDoS-атаки и вымогательства, возможно, поставили Empire на колени, существуют альтернативные рынки даркнета, которые открывают безопасные убежища для процветания киберпреступников.

Конечно, это не значит, что эти альтернативные нелегальные рынки не могут в один прекрасный день исчезнуть, как Империя.

Более того, с их растущей популярностью эти незаконные рынки даркнета обязательно попадут под пристальное внимание правоохранительных органов, таких как ФБР, учитывая масштабы их незаконной деятельности». ***(Ax Sharma. With Empire gone, patrons eye other illegal darkweb markets // Bleeping Computer®***

(https://www.bleepingcomputer.com/news/security/with-empire-gone-patrons-eye-other-illegal-darkweb-markets/). 26.08.2020).

***

«Исследователи предупреждают, что фишинг-мошенничество нацелено на пользователей Instagram через прямые сообщения в приложении.

Киберпреступники, говорящие на турецком языке, отправляют пользователям Instagram, казалось бы, законные сообщения от социальной сети с целью украсть их учетные данные Instagram и электронной почты.

Исследователи заявили, что кампания была нацелена на сотни знаменитостей, владельцев стартапов и других лиц с большим количеством подписчиков в Instagram. По их словам, эта конкретная атака впервые появилась на радарах исследователей после того, как ее мишенью стал полицейский, у которого более 16000 подписчиков в Instagram.

В то время как предыдущие фишинговые сообщения с использованием Instagram в качестве приманки были отправлены по электронной почте, злоумышленники в этой кампании отправляют фишинговые сообщения на самой платформе Instagram. Они притворяются Справочным центром Instagram и утверждают, что против владельца аккаунта была подана жалоба о нарушении авторских прав, и что теперь их аккаунт может быть удален.

«В сообщении также содержится ссылка, которая маскируется под форму для отправки апелляции, но на самом деле является фишинговой ссылкой», - заявили исследователи из Trend Micro в пятничном анализе. «Открытие ссылки ведет на страницу, где пользователя попросят указать свое имя пользователя. На момент написания в форме не было проверки данных, а это означает, что любой ввод - даже несуществующий аккаунт или его отсутствие - будет принят».

После того, как жертва нажимает кнопку «Далее» на целевой странице фишинга, появляется другой экран с запросом имени, пароля, адреса электронной почты и пароля электронной почты.

Если жертва вводит свои учетные данные и нажимает кнопку «Продолжить», страница перенаправляется на законную страницу входа в Instagram.

«Если пользователь уже был авторизован на сайте социальной сети до нажатия указанной кнопки, форма затем перенаправляется на его домашнюю страницу», - говорят исследователи. «Это создает иллюзию, что форма, которую они заполнили, официально связана с Instagram».

Получив учетные данные Instagram, злоумышленники входят в учетную запись, отключают номер мобильного телефона жертвы, связанный с учетной записью, и меняют адрес электронной почты, связанный с учетной записью. И, поскольку у них также есть учетные данные электронной почты, злоумышленники также могут захватить учетную запись электронной почты.

Злоумышленники ранее нацеливали пользователей Instagram на различные фишинговые кампании и мошенничества. Например, ранее в кампании 2019 года использовались электронные письма с просьбой подтвердить учетную запись пользователя, чтобы он мог получить подтвержденный значок.

Однако при нажатии кнопки «Подтвердить учетную запись» открывается фишинговая страница, на которой собираются адрес электронной почты, учетные данные и дата рождения пользователя. По словам исследователей, после их сбора злоумышленники получают всю информацию, необходимую для изменения информации для восстановления украденной учетной записи.

Как сообщил Threatpost Йиндрих Карасек, исследователь угроз в Trend Micro, многие атаки были успешными. По словам Карасека, последствия взлома зависят от обстоятельств.

«Некоторые жертвы могут быть достаточно известными, чтобы их шантажировали информацией, найденной в Google», - сказал Карасек Threatpost. «Большинство жертв также используют один и тот же пароль для всех социальных сетей, поэтому их личность в сети украдена, использована и оскорблена».

Исследователи посоветовали пользователям Instagram быть осторожными с кажущимися законными сайтами, которые запрашивают учетные данные для другого сайта.

Кроме того, пользователи должны «проверять содержание сообщения на наличие грамматических конструкций и орфографических ошибок» и «никогда не открывать ссылки и не загружать вложения из подозрительных источников. Наведите указатель мыши на URL-адрес, чтобы проверить, не отображается ли адрес, отличный от ожидаемого веб-сайта», - сказали исследователи.

Threatpost обратился в Instagram за дополнительными комментариями». ***(Lindsey O'Donnell. Instagram 'Help Center' Phishing Scam Pilfers Credentials // Threatpost (https://threatpost.com/instagram-help-center-phishing-scam-pilfers-credentials/158777/). 28.08.2020).***

***

«В даркнете опубликован список компаний и организаций, которые были атакованы операторами вымогательского программного обеспечения. База данных содержит список из 280 жертв 12 различных киберпреступных группировок.

В списке, например, указан один из крупнейших в США производителей алкогольных напитков Brown-Forman Corporation, которому принадлежат такие бренды как Jack Daniel's и Finlandia. Операторы вымогательского ПО REvil, также известного как Sodinokibi, на прошлой неделе заявили о взломе компьютерных систем компании. Как сообщили преступники, им удалось похитить около 1 ТБ конфиденциальных данных из сети компании, включая информацию о сотрудниках, контрактах, финансовых документах и внутренней корреспонденции.

Также в списке фигурирует американский производитель систем на кристале (SoC) MaxLinear, который в июне нынешнего года стал жертвой кибератаки со стороны операторов вымогательского ПО Maze. Злоумышленники зашифровали данные некоторых компьютерных систем компании и вскоре опубликовали 10,3 ГБ бухгалтерской и финансовой информации из более чем 1 ТБ похищенных данных.

В последнее время все больше и больше операторов вымогательского ПО разрабатывают сайты, где они публикуют похищенные конфиденциальные данные жертв, отказавшихся платить выкуп. Теперь к их рядам присоединился

относительно новый вид вымогательского ПО, известный как Conti. Однако в отчетах специалистов из Arete, Bleeping Computer и Carbon Black утверждается, что Conti «управляется той же группировкой, которая в прошлом проводила атаки с помощью вымогателя Ryuk».

На сайте утечек Conti уже перечислены 26 компаний, которые стали жертвами атак группы и отказались платить выкуп». ***(В даркнете опубликован список компаний, пострадавших от вымогательского ПО // SecurityLab.ru (https://www.securitylab.ru/news/511513.php). 27.08.2020).***

***

«38 компаний разных профилей в последние месяцы столкнулись с несанкционированным доступом к их серверам, приведшим к утечке данных, включая пароли сотрудников, необходимые для удаленной работы…

…хакеры в августе выставили на продажу информацию о VPN 900 мировых компаний. При этом 38 компаний пострадали от русскоязычных хакеров, которые получили доступ к VPN, через который могли добраться до основных систем компаний.

Среди этих компаний Hitachi Chemical Company, Ltd, Sumitomo Forestry, Zensho Co., Ltd., Onkyo, фармацевтическая компания Zenyaku Kogyo Co., Ltd., из сферы энергетики IWATANI CORPORATION, производитель оборудования DAIHEN Corporation.

Ранее Глава министерства по кибербезопасности Японии Еситака Сакурада в ходе дебатов в нижней палате парламента признался, что не умеет пользоваться персональным компьютером. В ответ на вопросы депутатов от оппозиции министр заявил, что не имеет потребности в устройствах, а если нужно использовать компьютер, этим занимаются его секретари и сотрудники». ***(Хакеры выставили на продажу информацию о VPN 900 мировых компаний // SecurityLab.ru (https://www.securitylab.ru/news/511472.php). 26.08.2020).***

***

Діяльність хакерів та хакерські угруповування

«Кампанию кибершпионажа против сотрудников государственных и военных организаций по всему миру выявила «Лаборатория Касперского». По оценкам специалистов, за последний год группа Transparent Tribe, использующая для проведения кампаний кибершпионажа троянец удаленного доступа Crimson, атаковала более тысячи целей в 27 странах. В основном жертвы располагались в Афганистане, Пакистане, Индии, Иране и Германии.

Атаки начинались с распространения вредоносных документов Microsoft Office в фишинговых письмах. Чаще всего Transparent Tribe использует зловред .NET RAT, или Crimson. Это троянец удаленного доступа, который состоит из различных компонентов и позволяет атакующим производить на зараженных устройствах многочисленные действия: манипулировать файлами на дисках,

создавать скриншоты, подслушивать и подглядывать через встроенные в устройстве микрофоны и камеры, а также красть файлы со съемных носителей.

Группа Transparent Tribe также известна как PROJECTM и MYTHIC LEOPARD. Она проводит масштабные кампании кибершпионажа с 2013 г., а «Лаборатория Касперского» следит за ее деятельностью с 2016 г. Несмотря на то, что тактика и техники группы остаются неизменными в течение многих лет, атакующие постоянно совершенствуют свой основной инструмент: эксперты находят новые, ранее неизвестные компоненты троянца Crimson». ***(Кибергруппа Transparent Tribe шпионит за гос и военными организациями по всему миру // Компьютерное Обозрение (https://ko.com.ua/kibergruppa_transparent_tribe_shpionit_za_gos_i_voennymi_organizaciyami_po_vsemu_miru_134217). 21.08.2020).***

***

«Компания Group-IB представила аналитический отчет о ранее неизвестной хакерской группе RedCurl, специализирующейся на корпоративном шпионаже. Менее чем за три года она атаковала десятки целей по всему миру. Группа, предположительно, состоящая из русскоговорящих хакеров, проводит тщательно спланированные атаки на частные компании различных отраслей, используя уникальный инструментарий. Цель атакующих – документы, представляющие коммерческую тайну и содержащие персональные данные сотрудников. Корпоративный шпионаж в целях конкурентной борьбы – редкое явление на хакерской сцене, однако частота атак говорит о том, что вероятнее всего оно получит дальнейшее распространение.

Группа RedCurl, обнаруженная экспертами Group-IB, активна как минимум с 2018 г. За это время она совершила по меньшей мере 26 целевых атак исключительно на коммерческие организации. Среди них – строительные, финансовые, консалтинговые компании, ритейлеры, банки, страховые, юридические и туристические организации. RedCurl не имеет четкой географической привязки к какому-либо региону: ее жертвы располагались в России, Украине, Великобритании, Германии, Канаде и Норвегии.

Группа действовала максимально скрытно, чтобы минимизировать риск обнаружения в сети жертвы. Во всех кампаниях главной целью RedCurl была кража конфиденциальных корпоративных документов – контрактов, финансовой документации, личных дел сотрудников, документов по судебным делам, по строительству объектов и др. Все это может свидетельствовать о заказном характере атак RedCurl с целью недобросовестной конкуренции.

Примечательно, что одной из вероятных жертв группы стал сотрудник компании, занимающейся информационной безопасностью и предоставляющей клиентам защиту от таких атак. Всего Group-IB удалось идентифицировать 14 организаций, ставших жертвами шпионажа со стороны RedCurl. Некоторые были атакованы несколько раз.

Самая ранняя известная атака RedCurl была зафиксирована в мае 2018 г. Как и во всех будущих кампаниях группы, первичным вектором было тщательно проработанное фишинговое письмо. Группа детально изучает инфраструктуру

целевой организации; каждое письмо составляется не просто под организацию-жертву, а под конкретную команду внутри нее. Чаще всего атакующие направляли свои письма от имени HR-департамента. Как правило, атака шла на нескольких сотрудников одного отдела, чтобы снизить их бдительность, например, все получали одинаковую рассылку по ежегодному премированию. Фишинговое письмо составляется максимально качественно – в нем фигурируют подпись, логотип, поддельное доменное имя компании. Специалисты отмечают, что подход RedCurl напоминает социотехнические атаки специалистов по пентесту.

Для доставки полезной нагрузки RedCurl используют архивы, ссылки на которые размещаются в теле письма и ведут на легитимные облачные хранилища. Ссылки замаскированы так, что пользователь не подозревает, что открывая вложение с документом о премировании якобы с официального сайта, он инициирует развертывание трояна, контролируемого атакующими через облако, в локальной сети. Троян-загрузчик RedCurl.Dropper – пропуск злоумышленников в целевую систему, который установит и запустит остальные модули ВПО. Как и весь собственный инструментарий группы, дроппер был написан на языке PowerShell.

Главная цель RedCurl – кража документации из инфраструктуры жертвы и корпоративной переписки. Оказавшись в сети, злоумышленники сканируют список папок и офисных документов, доступных с зараженной машины. Информация о них отправляется на облако, и оператор RedCurl решает, какие папки и файлы выгрузить. Параллельно все найденные на сетевых дисках файлы с расширениями .JPG, .PDF, .DOC, .DOCX, .XLS, .XLSX подменялись на ярлыки в виде модифицированных LNK-файлов. При открытии такого файла другим пользователем происходит запуск RedCurl.Dropper. Таким образом, RedCurl заражают большее количество машин внутри организации-жертвы и продвигаются по системе.

Также злоумышленники стремятся получить учетные данные от электронной почты. Для этого используется инструмент LaZagne, который извлекает пароли из памяти и из файлов, сохраненных в веб-браузере жертвы. Если необходимые данные получить не удается, RedCurl задействуют сценарий Windows PowerShell, который показывает жертве всплывающее фишинговое окно MicrosoftOutlook. Как только доступ к электронной почте жертвы получен, RedCurl проводят анализ и выгрузку всех интересующих их документов на облачные хранилища.

В ходе реагирований на инциденты, связанные с группой RedCurl, специалисты Group-IB выяснили, что после получения первоначального доступа атакующие находятся в сети жертвы от двух до шести месяцев. Троян RedCurl.Dropper, как и остальные инструменты группы, не подключается к командному серверу злоумышленников напрямую. Вместо этого все взаимодействие между инфраструктурой жертвы и атакующими происходит через легитимные облачные хранилища, такие как Cloudme, koofr.net, pcloud.com и другие. Все команды отдаются в виде PowerShell скриптов. Это позволяет RedCurl оставаться невидимыми для традиционных средств защиты длительное время». ***(Группа RedCurl промышляет корпоративным шпионажем по всему миру // Компьютерное Обозрение***

(https://ko.com.ua/gruppa_redcurl_promyshlyaet_korporativnym_shpionazhem_po_vsemu_miru_134149). 17.08.2020).

***

«Фирма McAfee сообщила в понедельник, что операторы ransomware NetWalker — одна из наиболее опасных групп киберпреступников — с марта этого года получили более 25 млн долл., шантажируя свои жертвы.

Хотя точной статистики доходов преступной индустрии нет и не может быть, очевидно, что 25-миллионная прибыль вводит NetWalker в одну лигу с наиболее успешными бандами ransomware современности, такими как Dharma, REvil (Sodinokibi) и лидирующая с большим отрывом Ryuk.

Приведенная McAfee цифра была получена в результате отслеживания платежей, сделанных жертвами шантажа на известные адреса биткойн, связанные с преступниками. Эксперты не исключают, что их сведения не дают полной картины, и что реальный доход от нелегальных операций Netwalker может быть ещё больше.

Штамм ransomware под названием Mailto впервые появился в августе прошлого года, и впоследствии был переименован в NetWalker. Фактически, NetWalker это портал RaaS (Ransomware-as-a-Service), где прошедшие процесс отбора хакеры строят собственные версии этого ransomware.

Именно эти преступные группы второго звена, собственно и занимаются распространением вымогательских программ. В последнее время, при отборе таких аффилированных групп NetWalker предпочтение отдаётся тем, кто специализируется на целевых атаках крупных корпоративных сетей путём хирургически точных вторжений в серверы RDP, сетевое оборудование, брандмауэры, серверы VPN и т.п. Кроме того, автор NetWalker, скрывающийся за псевдонимом Bugatti, заинтересован в сотрудничестве только с русскоговорящими клиентами.

За последние месяцы активность NetWalker значительно возросла. На данный момент, самая высокопрофильная его жертва это Мичиганский университет — его сеть была взломана в конце мая.

По мнению экспертов McAfee, NetWalker представляет опасность для компаний по всему миру, а не только в США и Западной Европе — его основных «охотничьих угодьях».

Одной из отличительных особенностей сервиса RaaS, обеспечившей ему популярность в преступной среде, является «сайт утечек». Если переговоры с жертвой завершились безрезультатно, похищенные у неё конфиденциальные данные выкладываются на этом сайте в режиме отложенной публикации с таймером.

Таким образом вымогатели создают дополнительное давление на скомпрометированные компании, многие из которых опасаются не только уничтожения своих данных, но и утечки интеллектуальной собственности, а также имиджевого ущерба от появления в прессе известий об их взломе». ***(Группа кибер-вымогателей NetWalker за полгода получила 25 млн долл. // Компьютерное Обозрение (https://ko.com.ua/gruppa_kiber-vymogatelej_netwalker_za_polgoda_poluchila_25_mln_doll_134004). 04.08.2020).***

***

«Издание The Register сообщает, что на сайте группировки, стоящей за созданием шифровальщика Maze, появились данные, якобы похищенные у южнокорейской компании SK Hynix, одного из крупнейших в мире поставщиков оперативной и флеш-памяти.

Группировка выложила в открытый доступ ZIP-архив размером 570 Мб, в котором, как утверждают злоумышленники, содержится лишь 5% похищенных у компании данных. То есть операторы Maze заявили, что не просто успешно атаковали SK hynix, но и похитили у компании около 11 Гб информации, прежде чем зашифровать файлы на зараженных машинах.

Журналисты The Register пишут, что в опубликованном архиве, судя по всему, содержатся конфиденциальные соглашения о поставке NAND-памяти Apple, а также различные корпоративные и личные файлы, в «возрасте» нескольких лет.

Представители SK Hynix пока никак не прокомментировали ситуацию, но издание отмечает, что операторы Maze обычно не бросают слов на ветер, и если группировка заявляет о взломе какой-то компании, как правило, это правда. Кроме того, среди жертв Maze уже числится немало крупных компаний». ***(Мария Нефёдова. Операторы вымогателя Maze утверждают, что взломали компанию SK hynix // Xakep (https://xakep.ru/2020/08/20/maze-sk-hynix/). 20.08.2020).***

***

«Низкоквалифицированные хакеры, вероятно, из Ирана, присоединились к бизнесу вымогателей, нацеленному на компании в России, Индии, Китае и Японии. Они преследуют легкие цели, используя в своей деятельности общедоступные инструменты.

Новая группа развертывает программу-вымогатель Dharma. Судя по артефактам судебно-медицинской экспертизы, это не изощренная, финансово мотивированная банда, которая плохо знакома с киберпреступностью.

Хакеры-любители на работе

Подрывник не жадный. Их спрос составляет от 1 до 5 биткойнов (в настоящее время от 11700 до 59000 долларов США), что находится в более низком диапазоне требований выкупа по сравнению с другими операциями вымогателей.

Они находят жертв путем сканирования диапазонов IP-адресов в Интернете на предмет открытых подключений к удаленному рабочему столу (RDP); их предпочтительным инструментом на этом этапе является Masscan, сканер портов с открытым исходным кодом.

Затем они запускают перебор с помощью утилиты NLBrute, которая пробует список паролей RDP в попытке найти комбинацию, которая работает. Попав внутрь, они иногда пытаются повысить привилегии, используя старую уязвимость (CVE-2017-0213) в Windows 7–10.

Исследователи из компании по кибербезопасности Group-IB узнали об этой новой группе в июне во время операции по реагированию на инциденты в компании в России. Основываясь на артефактах судебной экспертизы, они

определили, что злоумышленник был «хакерами-новичками, говорящими по-персидски».

Этот вывод подтверждается подсказками, полученными на следующих этапах атаки, которым, похоже, не хватает уверенности со стороны актера, который знает, что делать один раз после взлома сети…

«Например, чтобы отключить встроенное антивирусное ПО, злоумышленники использовали Defender Control и Your Uninstaller», - поясняют исследователи.

Дополнительным доказательством того, что эта операция является работой скриптового детектива из Ирана, являются поисковые запросы на персидском языке для поиска других инструментов, необходимых для атаки, а также каналы Telegram на персидском языке, предоставляющие их…

Число жертв, скомпрометированных этим злоумышленником, остается неизвестным, как и путь, который привел злоумышленника к операции Dharma ransomware-as-a-service (RaaS).

Однако, учитывая, что операторы Dharma предоставляют инструментарий, который позволяет любому легко стать киберпреступником, неудивительно, что неопытные люди развертывают это вредоносное ПО для шифрования файлов.

Олег Скулкин, старший аналитик DFIR в Group-IB, говорит, что утечка исходного кода программы-вымогателя Dharma в марте также объясняет более широкое использование этого штамма вредоносного ПО.

Что удивительно, так это использование этого вредоносного ПО для получения финансовой выгоды иранской группой угроз. Исторически киберактивность, происходящая из этого региона, была связана с поддерживаемыми государством операциями шпионажа и саботажа.

«Удивительно, что Дхарма попала в руки детей с иранским шрифтом, которые использовали ее для финансовой выгоды, поскольку Иран традиционно был страной спонсируемых государством злоумышленников, занимающихся шпионажем и саботажем» - Олег Скулкин». ***(Ionut Ilascu. Iranian hackers attack exposed RDP servers to deploy Dharma ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/iranian-hackers-attack-exposed-rdp-servers-to-deploy-dharma-ransomware/). 24.08.2020).***

***

«Специалисты центра мониторинга и реагирования на киберугрозы Solar JSOC выявили новую киберпреступную группировку. Она использует сложную схему атаки и уникальное вредоносное ПО, не известное ранее. Новая группировка получила название TinyScouts – по сочетанию наименования главных функций в коде. На данный момент эксперты фиксируют атаки на банки и энергетические компании.

На первом этапе атаки киберпреступники рассылают сотрудникам организаций фишинговые письма, в которых получателя предупреждают о начале второй волны пандемии коронавируса и для получения дополнительной информации предлагают пройти по ссылке. Встречаются также варианты фишинговых писем, имеющий четкий таргетинг: сообщение напрямую относится к

деятельности организации и выглядит вполне убедительно, однако также содержит вредоносную ссылку.

Кликнув по ней, жертва запускает загрузку основного компонента вредоносного ПО, которая происходит в несколько итераций. На этом этапе злоумышленники действуют максимально медленно и осторожно, поскольку каждый шаг в отдельности не привлекает внимания службы безопасности и систем защиты информации. Загрузка происходит через анонимную сеть TOR, что делает неэффективной такую популярную меру противодействия, как запрет на соединение с конкретными IP-адресами, которые принадлежат серверам злоумышленников.

На следующем этапе атаки вредоносное ПО собирает информацию о зараженном компьютере и передает ее злоумышленникам. Если данный узел инфраструктуры не представляет для них существенного интереса, то на него загружается дополнительный модуль – «вымогатель», шифрующий всю информацию на устройстве и требующий выкуп за расшифрование. В ходе атаки используется и легитимное ПО, в частности, принадлежащее компании Nirsoft. Перед тем, как данные на компьютере будут зашифрованы, оно собирает пароли пользователя из браузеров и почтовых клиентов, не оставляя заметных следов активности, поскольку не требует установки и не формирует записей в реестре ОС.

Если же зараженный компьютер интересен злоумышленникам и может служить их дальнейшим целям, скачивается дополнительное дополнительное ПО, защищенное несколькими слоями обфускации и шифрования, которое обеспечивает членам кибергруппировки удаленный доступ и полный контроль над зараженной рабочей станцией. Примечательно, что оно написано на PowerShell – это один из крайне редких случаев, когда этот язык не просто используется злоумышленниками в ходе атаки, а является инструментом для создания полноценного вредоносного ПО такого класса. Этот сценарий атаки предоставляет киберпреступникам широкий спектр вариантов монетизации: вывод финансовых средств, хищение конфиденциальных данных, шпионаж и т.д.

«TinyScouts используют такое вредоносное ПО и такие методы его доставки, упоминание о которых мы не нашли в открытых источниках, а значит можно сделать предположение о том, что это работа новой группировки. Этот факт вкупе с количеством уловок, направленных на то, чтобы остаться незамеченными, и индивидуальность сценария атаки для каждой конкретной жертвы говорит о том, что это не просто еще одна команда, организующая нецелевые массовые атаки. По нашим оценкам, технические навыки TinyScouts совершенно точно не ниже, чем у группировки, стоящей, например, за атаками Silence, а в технических аспектах доставки ПО на машину жертвы TinyScouts даже превосходят их, хотя и уступают APT-группировкам и правительственным кибервойскам», – отметил Игорь Залевский, руководитель отдела расследования инцидентов, Solar JSOC.

То, что решение о сценарии атаки принимается злоумышленником после получения информации о том, какой организации принадлежит конкретная зараженная машина, косвенно свидетельствует о планируемых масштабах активности TinyScouts – как минимум, о технической готовности к ряду одновременных атак на крупные организации». ***(Выявлена новая хакерская***

группировка // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5686387-Specialisty-Solar-JSOC-vyyavili-nov.html). 14.08.2020).

***

«Специалисты «Лаборатории Касперского» раскрыли подробности недавних атак китайской киберпреступной группировки CactusPete, в ходе которых хакеры использовали обновленную версию бэкдора Bisonal.

CactusPete, также известная под названиями Karma Panda и Tonto Team, активна с 2013 года. Как правило, ее целью являются военные и дипломатические организации, а также объекты инфраструктуры в Азии и Восточной Европе. Хотя кампании группировки не отличаются высокой техничностью исполнения, они довольно успешны, отметили исследователи.

В ходе новых атак, направленных на военные и финансовые организации в восточной Европе, CactusPete использовала новый вариант бэкдора Bisonal. Специалистам пока не удалось выяснить, как именно злоумышленники инфицировали системы в недавней кампании. В предыдущих атаках CactusPete использовала целевой фишинг с целью эксплуатации неисправленных уязвимостей и проникновения в системы.

Оказавшись на системе, вредонос отправляет на командный сервер злоумышленников различную информацию о сети жертвы, включая имя хоста, IP- и MAC- адрес, версию ОС, время заражения, данные об использовании прокси или виртуальной среды. Функционал бэкдора включает возможность удаленного запуска шелла, незаметного запуска программ, извлечения списка процессов, завершения процессов, загрузки/выгрузки/удаления файлов, извлечения списка драйверов и файлов из определенной папки.

Помимо Bisonal, арсенал группировки включает кастомные версии инструмента Mimikatz и кейлоггеров для кражи учетных данных и повышения привилегий, а также бэкдор DoubleT. Кроме того, специалисты заметили использование вредоноса ShadowPad, что может говорить о наличии внешней поддержки. ShadowPad применялась в атаках на организации в оборонной, энергетической, правительственной, горнодобывающей и телекоммуникационной сферах». ***(Китайская APT CactusPete атакует финансовые и военные организации в Восточной Европе // SecurityLab.ru (https://www.securitylab.ru/news/511204.php). 14.08.2020).***

***

«Согласно совместному сообщению, опубликованному сегодня несколькими правительственными агентствами США, северокорейские хакеры, которых отслеживают как BeagleBoyz, использовали вредоносные инструменты удаленного доступа в рамках продолжающихся атак для кражи миллионов у международных банков.

В совместном выпуске говорится, что с февраля 2020 года хакерская группа BeagleBoyz из Северной Кореи снова начала грабить банки с помощью удаленного доступа в Интернет для финансирования северокорейского режима.

BeatleBoys в настоящее время нацелены на банки в более чем 30 странах в рамках продолжающейся схемы ограбления банков, пытаясь украсть 2 миллиарда долларов, как написало в Твиттере Киберкомандование США .

Информация, представленная сегодня правительством США, является результатом информации, собранной и исследованной аналитиками Агентства по кибербезопасности и безопасности инфраструктуры (CISA), Министерства финансов (Казначейство), Федерального бюро расследований (ФБР) и US Cyber Командование (USCYBERCOM).

«С февраля 2020 года Северная Корея возобновила нацеливание на банки в нескольких странах с целью инициирования мошеннических международных денежных переводов и обналичивания наличных в банкоматах. Недавнее возрождение последовало за перерывом в обращении с банками с конца 2019 года», - говорится в сообщении.

Согласно сообщению, в ходе одной атаки схемы обналичивания банкоматов BeagleBoyz позволили им снимать наличные в банкоматах, эксплуатируемых банками из десятков стран, включая США.

BeagleBoyz также нацеливается на международные банки-жертвы в схемах SWIFT-мошенничества с использованием систем ничего не подозревающих банков, например, кража 81 миллиона долларов у Банка Бангладеш в течение 2016 года.

К счастью, Федеральный резервный банк Нью-Йорка смог остановить оставшуюся часть попытки перевода 1 миллиарда долларов после выявления аномалий в инструкциях по переводу, полученных от Банка Бангладеш.

BeagleBoyz из Северной Кореи несет ответственность за сложные кампании по обналичиванию денег через банкоматы с поддержкой киберпространства, публично обозначенные как «FASTCash» в октябре 2018 года. С 2016 года BeagleBoyz применяют схему FASTCash, нацеленную на инфраструктуру системы розничных платежей банков (т. обработка сообщений Международной организации по стандартизации [ISO] 8583, которые являются стандартом обмена сообщениями о финансовых транзакциях).

BeagleBoyz входят в состав Генерального разведывательного бюро правительства Северной Кореи и действуют по крайней мере с 2014 года, крадя сотни миллионов из банков для финансирования режима страны.

Деятельность BeagleBoyz пересекается с другими группами, отслеживаемыми фирмами по кибербезопасности, включая APT38 (FireEye), Bluenoroff (Kaspersky), Lazarus Group (ESTSecurity) и Stardust Chollima (CrowdStrike).

Также известно, что они стоят за обналичиванием банкоматов FASTCash, о которых сообщалось в октябре 2018 года, злоупотреблением взломанными конечными точками системы SWIFT с 2015 года, а также кражами со стороны криптовалютных фирм.

После первоначального предупреждения CISA о кампаниях FASTCash в Северной Корее, BeagleBoyz переместился на региональные межбанковские платежные системы с вредоносным ПО FASTCash помимо отдельных банков, демонстрируя четкую цель изучения других «восходящих возможностей в платежной экосистеме».

«BeagleBoyz использует различные инструменты и методы для получения доступа к сети финансового учреждения, изучения топологии для обнаружения ключевых систем и монетизации их доступа. Технический анализ ниже представляет собой совокупность нескольких известных инцидентов, а не детали одного операции ", - сказали в агентстве.

Было замечено, что северокорейцы использовали широкий спектр методов для получения доступа к системам своих жертв, включая целевой фишинг и водопой, а также социальную инженерию в тематических фишинговых атаках с использованием служебных приложений, начиная с 2018 до начала 2020 года.

Они, возможно, также наняли услуги криминальных хакерских групп, таких как TA505, для первоначального доступа к целевым финансовым учреждениям, запустив в некоторых случаях последнюю атаку на системы банков-жертв через несколько месяцев.

«Помимо ограбления традиционных финансовых учреждений, BeagleBoyz нацелена на криптовалютные биржи для кражи больших объемов криптовалюты, иногда оцениваемой в сотни миллионов долларов за инцидент», - говорится в сообщении.

«Криптовалюта предлагает BeagleBoyz необратимый метод кражи, который можно конвертировать в бумажную валюту, потому что постоянный характер переводов криптовалюты не позволяет использовать механизмы возврата».

Помимо совместной технической готовности, США Cyber Command также выпустил три анализа вредоносных программного обеспечения Отчетов (MARS) на Правительство Северной Кореи в АТМ обналичить схему с информацией о ECCENTRICBANDWAGON, VIVACIOUSGIFT и FastCash для Windows, вредоносных программ.

Казначейство США санкционировало три КНДР спонсируемый хакерских групп (Lazarus, Bluenoroff и Андариэль) в сентябре 2019 года.

Дополнительная информация о СКРЫТЫХ действиях КОБРЫ в виде предыдущих предупреждений доступна через Национальную систему киберпространства США». ***(Sergiu Gatlan. US govt warns of North Korean hackers targeting banks worldwide // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/us-govt-warns-of-north-korean-hackers-targeting-banks-worldwide/). 26.08.2020).***

***

«Продвинутая группа наемных хакеров взломала компьютеры архитектурной фирмы, которая участвует в проектах роскошной недвижимости стоимостью в миллиарды долларов США.

Группа осуществляет шпионские операции, вектор атаки - вредоносный плагин для программного обеспечения Autodesk 3ds Max для создания профессиональной трехмерной компьютерной графики.

Выбрать цели

Согласно расследованию Bitdefender, неназванная жертва - важная компания, работающая с застройщиками элитной недвижимости в США, Великобритании,

Австралии и Омане, которые нанимают услуги ведущих архитекторов и дизайнеров интерьера.

Для этой операции злоумышленник полагался на инфраструктуру управления и контроля (C2) в Южной Корее, которая регистрировала трафик от образцов вредоносных программ в нескольких странах (США, Южная Корея, Япония, Южная Африка), предлагая также избранных жертв в этих регионах.

Доказательства, обнаруженные исследователями безопасности, указывают на группу, которая предоставляет сложные хакерские услуги различным клиентам, ищущим внутренние финансовые детали и переговоры о дорогостоящих контрактах…

Осторожная операция

В этом случае вектор атаки представлял собой уязвимость, затрагивающую несколько версий Autodesk 3ds Max, которая допускает выполнение кода в системе Windows.

Ранее в этом месяце Autodesk предупредил, что существует уязвимость для скриптовой утилиты MAXScript в виде вредоносного плагина под названием «PhysXPluginMfx». При загрузке в 3ds Max плагин может заразить другие файлы MAX, таким образом распространяясь на других пользователей в сети.

В отличие от групп киберпреступников, которые стремятся получить немедленную финансовую выгоду, этот злоумышленник использует вредоносное ПО, которое собирает сведения о взломанном хосте (имя компьютера, имя пользователя) и крадет конфиденциальную информацию.

Помимо использования инструментов, которые делают снимки экрана и извлекают пароли и данные истории из Google Chrome, у актера также есть вредоносное ПО, которое крадет файлы с определенными расширениями.

Исследователи Bitdefender оценивают, что злоумышленник компилирует этот компонент для кражи файлов для каждой жертвы, чтобы включить список файлов, которые они хотят украсть.

Сохранение небольшой площади

Чтобы оставаться незамеченными на скомпрометированной машине, злоумышленник прибегнул к интересной уловке, которая заставляла вредоносный двоичный файл бездействовать, если запущены диспетчер задач или монитор производительности.

В зависимости от того, какая площадь окна была видна для этих двух приложений, был установлен флаг, предписывающий вредоносной программе переходить в спящий режим, тем самым уменьшая использование ЦП и помещая ее ниже в списке энергоемких процессов.

В то же время сжатие файлов применялось только к некоторым файлам. Данные, которые в случае архивации привлекли бы ненужное внимание, будут пропущены из этой операции.

В сегодняшнем отчете Bitdefender говорится, что данные телеметрии показывают, что аналогичные образцы вредоносных программ контактировали с тем же C2 в Южной Корее менее месяца назад.

Хотя это может помочь связать точки с другими операциями, это ни в коем случае не начало временной шкалы активности группы». ***(Ionut Ilascu. Hackers for***

hire attack architecture firm via 3ds Max exploit // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-for-hire-attack-architecture-firm-via-3ds-max-exploit/). 26.08.2020).

***

Вірусне та інше шкідливе програмне забезпечення

«Агентство национальной безопасности (АНБ) США и Федеральное бюро расследований (ФБР) опубликовали отчет, в котором обвинили Россию в создании и запуске нового вируса под названием Drovorub. За разработку вируса было ответственно военное подразделение Главного разведывательного управления (ГРУ), запуск вируса — часть его операций по кибершпионажу, говорится в заявлении ведомств.

По данным США, Drovorub поражает систему Linux. «Drovorub представляет угрозу для пользователей систем национальной безопасности, Министерства обороны и базы оборонной промышленности, использующих системы Linux», — говорится в отчете.

В документе даже называется конкретное подразделение — «26165 85-го Основного центра специальных служб Главного управления Генштаба России, которое в частном секторе называют Fancy Bear, Strontium или APT 28»…

«Дроворуб» обладает широким набором возможностей, которые позволяют злоумышленнику выполнять множество различных функций, таких как кража файлов и удаленное управление компьютером жертвы, отмечает технический директор компании McAfee Стив Гробман.

В McAfee также назвали вирус «швейцарским армейским ножом для взлома Linux». Помимо прочего Drovorub использует передовые руткит-технологии, которые затрудняют его обнаружение. Это позволяет внедрять вирус сразу во множество разных типов цели и открывает возможность для атак в любое время.

Полный технических подробностей 45-страничный отчет АНБ и ФБР продолжает серию разоблачений российских хакеров в преддверии президентских выборов в США. В отчете не уточняется, какие типы организаций подверглись атакам с использованием системы «Дроворуб».

Чтобы предотвратить возможные последствия атаки Drovorub, в ФБР и АНБ посоветовали компаниям и госорганизациям в США обновить Linux-системы до версии ядра 3.7 или новее. В более новых версиях есть функция принудительной подписи ядра, которая не позволит Drovorub устанавливать руткиты». ***(Спецслужбы США уличили российскую разведку в релизе хак-инструмента Drovorub // РосКомСвобода (https://roskomsvoboda.org/62507/). 14.08.2020).***

***

«Эксперты компьютерной безопасности обнаружили, по всей видимости, первый вредоносный криптомайнер с функцией кражи с заражённых серверов учётных данных AWS. Эта новая опасная специализация выявлена в программном обеспечении, используемом киберпреступной группой TeamTNT.

Согласно исследованию, недавно опубликованному Trend Micro, данная группа активна как минимум с апреля. TeamTNT сканирует Интернет в поисках систем Docker, в которых из-за неправильной настройки управляющий API-интерфейс оставлен доступным из Интернета без пароля.

Затем группа развёртывает внутри уязвимых инсталляций Docker серверы, которые запускают вредоносные программы для DDoS-атак и ПО для крипто-майнинга.

В новом отчете, от 17 августа, британская фирма Cado Security сообщила, что TeamTNT недавно распространила свои атаки на Kubernetes. Но самое главное новшество, которое выходит за рамки типичной для таких группировок функциональности, — это функция, которая сканирует инфицированные серверы в поисках любых учётных данных Amazon Web Services (AWS).

Найденные файлы ~/.aws/credentials и ~/.aws/config копируются и загружаются на командный (C&C) сервер TeamTNT. Оба они не зашифрованы и содержат записанные открытым текстом идентификационные данные и сведения о конфигурации для базовых аккаунта и инфраструктуры AWS.

По мнению исследователей из Cado преступники пока (по состоянию дел на 17 августа) не использовали похищенную таким образом информацию. Тем не менее, она позволяет TeamTNT серьёзно повысить доходы путём установки криптомайнеров на более мощные кластеры AWS EC2, либо торгуя украденными данными на чёрном рынке». ***(Ботнет TeamTNT крадёт учётные данные AWS // Компьютерное Обозрение (https://ko.com.ua/botnet_teamtnt_kradyot_uchyotnye_dannye_aws_134179). 18.08.2020).***

***

«Компания Eset выявила фишинговую кампанию с использованием бренда Netflix. Киберпреступники рассылают пользователям письма с уведомлением о задолженности и требованием изменить платежные данные для продления подписки.

В письме содержится ссылка, ведущая на страницу с формой для ввода платежных данных.

Таким образом, пользователи передают мошенникам свои имя и фамилию, номер карты, срок действия и даже CVV. После ввода данных жертва перенаправляется на официальный сайт Netflix и даже не подозревает, что ее приватная информация оказалась у преступников…». ***(Злоумышленники используют популярность Netflix для организации фишинговых атак // Компьютерное Обозрение (https://ko.com.ua/zloumyshlenniki_ispolzuyut_populyarnost_netflix_dlya_organizacii_fishingovyh_atak_134191). 19.08.2020).***

***

«По сравнению с предыдущим месяцем, в июле на Android-устройствах было обнаружено на 6,7% меньше угроз. Число вредоносных программ

сократилось на 6,75%, нежелательных – на 4,6%, потенциально опасных – на 8,42%, а рекламных – на 9,83%.

В течение месяца вирусные аналитики «Доктор Веб» выявили в каталоге Google Play несколько новых вредоносных программ. Одной из них был банковский троян Android.Banker.3259, скрывавшийся в приложении для работы с SMS. Другие оказались троянами семейства Android.HiddenAds, которые показывали надоедливые рекламные баннеры. Кроме того, был обнаружен очередной представитель семейства Android.Joker, подписывавший пользователей на премиум-сервисы и выполнявший произвольный код.

Самые распространенные вредоносные программы июля, согласно статистике антивирусных продуктов Dr.Web для Android:

Android.HiddenAds.530.origin – троян, предназначенный для показа навязчивой рекламы. Распространяется под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают его в системный каталог;

Android.Click.348.origin – вредоносное приложение, которое самостоятельно загружает веб-сайты, нажимает на рекламные баннеры и переходит по ссылкам. Может распространяться под видом безобидных программ, не вызывая подозрений у пользователей;

Android.RemoteCode.6122, Android.RemoteCode.256.origin – вредоносные программы, которые загружают и выполняют произвольный код. В зависимости от модификации эти трояны могут загружать различные веб-сайты, переходить по ссылкам, нажимать на рекламные баннеры, подписывать пользователей на платные услуги и выполнять другие действия;

Android.DownLoader.906.origin – троян, загружающий другие вредоносные программы и ненужное ПО. Может скрываться во внешне безобидных приложениях, которые распространяются через каталог Google Play или вредоносные сайты.

Наиболее распространенные нежелательные программы июля:

Program.FreeAndroidSpy.1.origin, Program.Mrecorder.1.origin, Program.MSpy.14.origin – приложения, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа. Они могут контролировать местоположение устройств, собирать данные об SMS-переписке, беседах в социальных сетях, копировать документы, фотографии и видео, выполнять прослушивание телефонных звонков и окружения и т.п.;

Program.FakeAntiVirus.2.origin – детектирование рекламных программ, которые имитируют работу антивирусного ПО. Такие программы могут сообщать о несуществующих угрозах и вводить пользователей в заблуждение, требуя оплатить покупку полной версии;

Program.CreditSpy.2 – детектирование программ, предназначенных для присвоения кредитного рейтинга на основании персональных данных пользователей. Такие приложения загружают на удаленный сервер SMS-сообщения, информацию о контактах из телефонной книги, историю вызовов, а также другие сведения.

Самые распространенные потенциально опасные программы:

Tool.SilentInstaller.6.origin, Tool.SilentInstaller.11.origin, Tool.SilentInstaller.13.origin, Tool.SilentInstaller.14.origin – потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему;

Tool.Packer.1.origin – специализированная утилита-упаковщик, предназначенная для защиты Android-приложений от модификации и обратного инжиниринга. Она не является вредоносной, но может быть использована для защиты как безобидных, так и троянских программ.

Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах. В зависимости от семейства и модификации они могут демонстрировать рекламу в полноэкранном режиме, блокируя окна других приложений, выводить различные уведомления, создавать ярлыки и загружать веб-сайты. Adware.Adpush.36.origin, Adware.Adpush.6547, Adware.Myteam.2.origin, Adware.Mobby.5.origin, Adware.Toofan.1.origin.

Среди угроз, выявленных в Google Play в июле, были новые представители семейства Android.HiddenAds. Злоумышленники распространяли их под видом приложений для редактирования фотографий.

Как и другие трояны этого семейства, после запуска они скрывали свои значки из списка программ в меню главного экрана, чтобы пользователям было сложнее их удалить. После этого они начинали показывать баннеры поверх окон других приложений и интерфейса операционной системы.

Другой троян, которого обнаружили вирусные аналитики «Доктор Веб», получил имя Android.Joker.279. Он скрывался в приложении для работы с SMS и после запуска подписывал жертв на дорогостоящие мобильные сервисы, а также мог выполнять произвольный код.

Также специалисты выявили банковского трояна Android.Banker.3259. Вирусописатели создали его на основе SMS-мессенджера с открытым исходным кодом.

При запуске банкер соединяется с управляющим сервером и ожидает от него дальнейших команд. В зависимости от полученного ответа троян либо продолжает работать как безобидное приложение, либо пытается украсть у жертвы ее персональные данные, показывая фишинговое окно. Кроме того, Android.Banker.3259 сохраняет все входящие и исходящие SMS в облачную базу данных Firebase. В дальнейшем злоумышленники могут использовать информацию, полученную из этих сообщений, для организации новых атак». ***(Число вредоносных программ для Android в июле сократилось на 7% // Компьютерное Обозрение (https://ko.com.ua/chislo_vredonosnyh_programm_dlya_android_v_iyule_sokratilos_na_7_134097). 12.08.2020).***

***

«В июле анализ данных статистики компании «Доктор Веб» показал снижение общего числа обнаруженных угроз на 6.41% по сравнению с июнем.

При этом количество уникальных угроз увеличилось на 8.58%. Рекламные программы, загрузчики и установщики вредоносного ПО продолжают лидировать по общему количеству обнаруженных угроз. В почтовом трафике на первых позициях находится многомодульный банковский троян Trojan.SpyBot.699. Кроме того, пользователям по-прежнему угрожают программы, использующие уязвимости документов Microsoft Office, а также различные модификации вредоносных HTML-документов, распространяемых в виде вложений и перенаправляющих пользователей на фишинговые сайты.

В июле статистика вновь зафиксировала снижение числа обращений пользователей за расшифровкой файлов – на 16.34% по сравнению с июнем. Самым распространенным энкодером остается Trojan.Encoder.26996, на долю которого пришлось 23.51% всех инцидентов.

Угрозы июля 2020 г., по данным сервиса статистики «Доктор Веб»:

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;

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.BPlug.3845 – вредоносное расширение для браузера, предназначенное для осуществления веб-инжектов в просматриваемые пользователями интернет-страницы и блокировки сторонней рекламы.

Рейтинг вредоносных программ в почтовом трафике.

Trojan.SpyBot.699 – многомодульный банковский троян. Позволяет киберпреступникам загружать и запускать на зараженном устройстве различные приложения и исполнять произвольный код;

Exploit.CVE-2012-0158 – измененный документ Microsoft Office Word, использующий уязвимость CVE-2012-0158 для выполнения вредоносного кода;

W97M.DownLoader.2938 – семейство троянов-загрузчиков, использующих в работе уязвимости документов Microsoft Office. Предназначены для загрузки на атакуемый компьютер других вредоносных программ;

HTML.Redirector.32, HTML.Redirector.38 – вредоносные HTML-документы, как правило маскирующиеся под безобидные вложения к информационным письмам. При открытии перенаправляют пользователей на фишинговые сайты или загружают полезную нагрузку на заражаемые устройства.

По сравнению с июнем в июле в антивирусную лабораторию «Доктор Веб» поступило на 16.34% меньше запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков. При этом наиболее активными были:

Trojan.Encoder.26996 – 23.51%, Trojan.Encoder.567 – 7.93%, Trojan.Encoder.29750 – 7.37%, Trojan.Encoder.11464 – 2.55%, Trojan.Encoder.30356 – 2.55%.

В течение июля в базу нерекомендуемых и вредоносных сайтов было добавлено 198467 интернет-адресов, что на 61.78% больше, чем в июне.

В июле общее количество угроз, обнаруженных на Android-устройствах пользователей, снизилось на 6.7%. Часть новых вредоносных программ, выявленных за прошедший месяц, вновь распространялась через каталог Google Play. Среди них оказались рекламные трояны, получившие имена Android.HiddenAds.2190 и Android.HiddenAds.2193. Они показывали пользователям надоедливые баннеры и мешали работе с устройствами. Другими угрозами стали многофункциональный троян Android.Joker.279, а также банкер Android.Banker.3259. Обе программы маскировались под приложения для работы с SMS». ***(В июле зафиксировано некоторое снижение активности шифровальщиков // Компьютерное Обозрение (https://ko.com.ua/v_iyule_zafiksirovano_nekotoroe_snizhenie_aktivnosti_shifrovalshhikov_134096). 11.08.2020).***

***

«В почти трети кибератак (30%) в 2019 г. были задействованы легитимные инструменты удаленного управления и администрирования, по данным «Лаборатории Касперского». Это позволяет злоумышленникам долго скрывать следы своей деятельности. Так, в среднем атака, проводимая с целью кибершпионажа и кражи конфиденциальных данных, длилась 122 дня.

Самый распространенный инструмент – PowerShell (применялся в каждой четвертой атаке). Этот мощный инструмент администрирования может быть использован с разными целями: от сбора данных до управления вредоносным ПО. В 22% атак использовалась утилита PsExec, предназначенная для запуска программ на удаленных компьютерах. Замыкает топ-3 инструмент SoftPerfect Network Scanner, предназначенный для сканирования сетей. Он использовался в 14% атак.

Применение злоумышленниками легитимных инструментов усложняет процесс обнаружения их деятельности, ведь с помощью подобного ПО могут выполняться и рядовые задачи, и несанкционированные действия. Однако иногда характер активности определяется достаточно быстро, например, в случае атак программ-вымогателей, когда для шифрования используются легальные утилиты, но ущерб виден невооруженным взглядом.

Полностью отказаться от подобных программ невозможно по многим причинам, однако, если применять необходимые политики безопасности и системы мониторинга, то подозрительную активность в сети и сложные атаки можно обнаруживать на ранних стадиях. Чтобы своевременно детектировать атаки с использование легитимных инструментов и реагировать на них, помимо прочих мер, организациям следует запланировать внедрение EDR-решения с MDR-сервисом.

Также чтобы минимизировать вероятность использования легитимных инструментов для совершения кибератак, специалисты рекомендуют: ограничить доступ к инструментам удаленного управления с внешних IP-адресов и убедиться в

том, что доступ к интерфейсам удаленного контроля может быть осуществлен с ограниченного количества конечных устройств; ввести строгую политику паролей для всех ИТ-систем и мультифакторную аутентификацию; предоставлять учетные записи с высокими привилегиями только тем пользователям, которым они действительно нужны для выполнения рабочих задач». ***(Легитимные инструменты удаленного управления задействованы в трети кибератак // Компьютерное Обозрение (https://ko.com.ua/legitimnye_instrumenty_udalennogo_upravleniya_zadejstvovany_v_treti_kiberatak_134069). 10.08.2020).***

***

«Издание Bleeping Computer сообщает, что неделю назад компания Konica Minolta пострадала от атаки шифровальщика RansomEXX. Атака затронула многие службы холдинга.

Первые признаки сбоя были замечены клиентами компании еще 30 июля 2020 года. Тогда люди стали обнаруживать, что сайт поддержки продуктов Konica Minolta недоступен и отображает сообщение о временной недоступности. В итоге сайт компании не работал почти неделю, однако в компании не давали прямого ответа на вопрос, что послужило причиной сбоя.

Хуже того, некоторые модели принтеров Konica Minolta отображали ошибку Service Notification Failed, из-за которой специалисты компании были вынуждены обновить свое сообщение и добавить к нему ссылку на документацию.

Хотя компания до сих пор никак не прокомментировала ситуацию, журналисты Bleeping Computer заявляют, что их собственный источник предоставил в распоряжение издания записку с требованием выкупа, доказывающую, что Konica Minolta стала жертвой атаки шифровальщика. Файл называется !!KONICA_MINOLTA_README!!.txt и скриншот этого послания можно увидеть ниже». ***(Мария Нефёдова. Компания Konica Minolta пострадала от атаки шифровальщика // Xakep (https://xakep.ru/2020/08/17/konica-minolta/). 17.08.2020).***

***

«Новая операция вымогателей под названием DarkSide начала атаковать организации в начале этого месяца с помощью специализированных атак, которые уже принесли им выплаты в миллионы долларов.

Начиная примерно с 10 августа 2020 года, новая программа-вымогатель начала проводить целевые атаки на многочисленные компании.

В «пресс-релизе», выпущенном злоумышленниками, они утверждают, что являются бывшими аффилированными лицами, заработавшими миллионы долларов на других операциях с программами-вымогателями.

Не найдя «продукта», который отвечал бы их потребностям, они решили начать собственное производство…

DarkSide заявляет, что они нацелены только на компании, которые могут заплатить указанный выкуп, поскольку они не «хотят убивать ваш бизнес».

Злоумышленники также заявили, что они не нацелены на следующие типы организаций.

Медицина (больницы, хосписы).

Образование (школы, университеты).

Некоммерческие организации.

Государственный сектор.

Еще слишком рано говорить, будут ли они уважать это заявление.

От жертв, замеченных BleepingComputer, DarkSide требует выкупа от 200000 до 2000000 долларов. Эти числа, вероятно, могут быть больше или меньше в зависимости от жертвы.

По крайней мере, одна из жертв, замеченных BleepingComputer, похоже, заплатила выкуп в миллион долларов.

DarkSide крадет данные перед шифрованием жертв

Как и другие атаки программ-вымогателей, управляемых человеком, когда операторы DarkSide взламывают сеть, они распространяются по сети в поперечном направлении, пока не получат доступ к учетной записи администратора и контроллеру домена Windows.

В то время как они распространяются горизонтально, злоумышленники собирают незашифрованные данные с серверов жертвы и загружают их на свои собственные устройства.

Эти украденные данные затем отправляются на сайт утечки данных под их контролем и используются как часть попытки вымогательства.

Когда данные публикуются на сайте утечки, злоумышленники будут указывать название компании, дату, когда они были взломаны, сколько данных было украдено, скриншоты данных и типы украденных данных.

DarkSide заявляет, что если жертва не заплатит, она опубликует все данные на своем веб-сайте как минимум в течение шести месяцев.

Эта стратегия вымогательства предназначена для того, чтобы запугать жертву и заставить ее заплатить выкуп, даже если она сможет восстановить данные из резервных копий.

Если жертва заплатит выкуп, DarkSide заявляет, что она удалит украденные данные со своего сайта утечки.

Данные жертвы, заплатившей выкуп, уже удалены с сайта.

Индивидуальные атаки программ-вымогателей

При выполнении атак DarkSide создаст индивидуальный исполняемый файл программы-вымогателя для конкретной компании, которую они атакуют.

При запуске программа-вымогатель выполнит команду PowerShell, которая удаляет теневые копии томов в системе, чтобы их нельзя было использовать для восстановления файлов.

По словам Виталия Кремеза из Advanced Intel, затем он завершает работу различных баз данных, офисных приложений и почтовых клиентов, чтобы подготовить машину к шифрованию.

При шифровании компьютера DarkSide избегает завершения определенных процессов …

В частности, избегание TeamViewer редко встречается с программами-вымогателями и может указывать на то, что злоумышленники используют его для удаленного доступа к компьютерам.

Майкл Гиллеспи, проанализировавший процесс шифрования, сказал BleepingComputer, что программа-вымогатель использует ключ SALSA20 для шифрования файлов. Затем этот ключ шифруется с помощью открытого ключа RSA-1024, включенного в исполняемый файл.

У каждой жертвы также будет собственное расширение, созданное с использованием настраиваемой контрольной суммы MAC-адреса жертвы.

Каждый исполняемый файл настроен для включения персонализированной записки о выкупе «Добро пожаловать в Тьму», которая будет включать в себя количество украденных данных, тип данных и ссылку на их данные на сайте утечки данных.

В настоящее время программа-вымогатель выглядит надежно, и нет возможности восстановить файлы бесплатно.

Возможное подключение к REvil

При анализе DarkSide было обнаружено некоторое сходство с программой-вымогателем REvil.

Наиболее очевидным сходством является записка о выкупе, в которой используется почти тот же шаблон, что и в записке о выкупе REvil ниже.

В ходе поведенческого анализа DarkSide, проведенного BleepingComputer, мы заметили, что он будет выполнять закодированный сценарий PowerShell при первом запуске.

После деобфускации мы видим, что эта команда PowerShell используется для удаления теневых копий томов на компьютере перед их шифрованием.

Использование PowerShell для выполнения указанной выше команды - это тот же метод, что и REvil.

Наконец, команда MalwareHunterTeam обнаружила, что DarkSide намеренно избегает заражения жертв в странах СНГ. Код для этого аналогичен тому, что используется в REvil, а также в GandCrab.

Хотя эти связи незначительны, за ними следует следить». ***(Lawrence Abrams. DarkSide: New targeted ransomware demands million dollar ransoms // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/). 21.08.2020).***

***

«Правительственные агентства США сегодня опубликовали отчет об анализе вредоносного ПО, в котором раскрывается информация о вредоносном ПО, являющемся трояном удаленного доступа (RAT), используемым северокорейскими хакерами в атаках на государственных подрядчиков.

Вредоносное ПО было идентифицировано Агентством кибербезопасности и безопасности инфраструктуры (CISA) и Федеральным бюро расследований (ФБР) и известно как BLINDINGCAN.

Эти два агентства приписали трояна спонсируемой правительством Северной Кореи хакерской группе, известной как HIDDEN COBRA (также известной как Lazarus Group и APT38).

Вредоносное ПО, способное стереть свои следы

Согласно анализу агентств, RAT имеет «встроенные функции для удаленных операций, которые предоставляют различные возможности в системе жертвы».

«CISA получила четыре документа Microsoft Word Open Extensible Markup Language (XML) (.docx), две библиотеки динамической компоновки (DLL)», - говорится в предупреждении.

"Файлы .docx пытаются подключиться к внешним доменам для загрузки. Были представлены 32-разрядная и 64-разрядная библиотеки DLL, которые устанавливают 32-разрядную и 64-разрядную библиотеки DLL с именем 'iconcache.db' соответственно. DLL ' iconcache.db 'распаковывает и запускает вариант Hidden Cobra RAT. "

Основываясь на результатах анализа вредоносных программ CISA и ФБР, вредоносное ПО BLINDINGCAN также может удалить себя из скомпрометированных систем и очистить свои следы, чтобы избежать обнаружения среди других возможностей:

• Получение информации обо всех установленных дисках, включая тип диска и количество свободного места на диске

• Создание, запуск и завершение нового процесса и его основного потока

• Поиск, чтение, запись, перемещение и выполнение файлов

• Получение и изменить временные метки файла или каталога

• изменить текущий каталог для процесса или файла

• удалить вредоносное ПО и артефакты, связанные с вредоносным ПО, из зараженной системы

Отчет об анализе вредоносных программ AR20-232A был выпущен, чтобы предоставить организациям подробную информацию о вредоносных программах, полученную с помощью ручного обратного проектирования.

Он также призван помочь защитникам сети обнаруживать и ограничивать подверженность злонамеренной кибер-активности HIDDEN COBRA, поскольку правительство США ссылается на злонамеренную деятельность правительства Северной Кореи.

Северокорейское вредоносное ПО и вредоносная активность

В мае были обнаружены еще три северокорейских варианта вредоносного ПО, в том числе инструмент удаленного доступа, известный как COPPERHEDGE, который использовался в атаках на обмены криптовалютами, и два трояна, известные как TAINTEDSCRIBE и PEBBLEDASH.

В середине февраля правительство США выпустило шесть других рекомендаций по безопасности с информацией о северокорейских вредоносных программах, раскрывающих:

• BISTROMATH (полнофункциональная RAT),

• SLICKSHOES (программа-дроппер вредоносного ПО, упакованная Themida),

• CROWDEDFLOUNDER (троянский загрузчик удаленного доступа),

• HOTCROISSANT (имплант-маяк с возможностями бэкдора),

• ARTFULPIE (вредоносное ПО, которое загружает и запускает DLL из жестко запрограммированный URL-адрес),

• BUFFETLINE (сигнальный имплант с черными функциями).

Год назад, в 2019 году, CISA и ФБР также опубликовали информацию о другом вредоносном ПО, получившем название ELECTRICFISH, которое используется для кражи данных, а также о трояне HOPLIGHT, используемом для маскировки вредоносного трафика.

В апреле 2020 года правительство США предложило вознаграждение в размере до 5 миллионов долларов за информацию о киберактивности хакеров из КНДР, включая прошлые или текущие операции, которая приводит к пресечению незаконной деятельности, связанной с КНДР, или к идентификации или местонахождению северокорейцев. актеры.

Северокорейские хакерские группы стояли за ограблениями криптовалюты, которые привели к убыткам в 571 миллион долларов в 2017 и 2018 годах.

Минфин США подписал санкции против трех хакерских групп, спонсируемых КНДР (Lazarus, Bluenoroff и Andariel) в сентябре 2019 года.

Более подробная информация о СКРЫТЫХ действиях КОБРЫ в виде ранее выпущенных предупреждений доступна через Национальную систему кибернетической осведомленности США». ***(Sergiu Gatlan. US govt exposes new North Korean BLINDINGCAN backdoor malware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/us-govt-exposes-new-north-korean-blindingcan-backdoor-malware/). 19.08.2020).***

***

«Уникальный, продвинутый ботнет P2P-червей отбрасывает бэкдоры и криптомайнеры и распространяется по всему миру.

Одноранговый (P2) ботнет под названием FritzFrog появился на сцене, и исследователи заявили, что он активно взламывает серверы SSH с января.

Серверы SSH - это части программного обеспечения, которое можно найти в маршрутизаторах и устройствах IoT, среди других машин, и они используют протокол защищенной оболочки для приема соединений с удаленных компьютеров. Серверы SSH широко распространены как в корпоративных, так и в потребительских средах.

Согласно анализу Guardicore Labs, FritzFrog распространяется как червь, взламывая учетные данные в таких организациях, как правительственные учреждения, учебные заведения, медицинские центры, банки и телекоммуникационные компании. По словам исследователя Guardicore Офира Харпаза, FritzFrog до сих пор пытался взломать десятки миллионов машин и успешно взломал более 500 серверов. Среди жертв - известные университеты США и Европы, а также железнодорожная компания; а самые зараженные страны - Китай, Южная Корея и США.

«FritzFrog запускает вредоносную программу-червь, которая написана на Golang, является модульной, многопоточной и бесфайловой, не оставляя следов на диске зараженной машины», - пояснил Харпаз в своем сообщении в среду. После

взлома сервера «вредоносное ПО создает бэкдор в виде открытого ключа SSH, позволяя злоумышленникам получать постоянный доступ к машинам жертвы».

Он также может сбрасывать дополнительные полезные данные, такие как майнеры криптовалют.

Купание в уникальном пруду

FritzFrog - это ботнет P2P, а это означает, что он обладает большей отказоустойчивостью, чем другие типы ботнетов, поскольку управление децентрализовано и распределяется между всеми узлами; поэтому не существует единой точки отказа и командно-управляющего сервера (C2).

«FritzFrog полностью запатентован; его реализация P2P была написана с нуля, и мы узнали, что злоумышленники являются высокопрофессиональными разработчиками программного обеспечения », - сказал Харпаз. Она добавила: «Протокол P2P является полностью проприетарным и не полагается на известные протоколы P2P, такие как µTP».

Что касается других технических деталей, Guardicore проанализировал ботнет, добавив в него свои собственные узлы, что дало исследователям возможность участвовать в текущем P2P-трафике и видеть, как он был построен.

Они обнаружили, что почти все в FritzFrog уникально по сравнению с прошлыми ботнетами P2P: Harpaz отметила, что он не использует IRC, как IRCflu; он работает в памяти, в отличие от другого ботнета, занимающегося криптодобычей, DDG; и работает на Unix-машинах, в отличие от других, таких как ботнет InterPlanetary Storm.

Кроме того, его бесфайловая полезная нагрузка необычна. Харпаз писал, что файлы передаются по сети как для заражения новых машин, так и для запуска новых вредоносных программ на скомпрометированных - и что это выполняется полностью в памяти с помощью блобов.

«Когда узел A желает получить файл от своего партнера, узла B, он может запросить узел B, какие BLOB-объекты ему принадлежат, с помощью команды getblobstats», - сказал исследователь. «Затем узел A может получить конкретный BLOB-объект по его хэшу, либо с помощью команды P2P getbin, либо через HTTP с URL-адресом http: //: 1234 /. Когда на узле A есть все необходимые капли, он собирает файл с помощью специального модуля с именем Assemble и запускает его».

Как только вредоносная программа устанавливается на цель этим методом, она начинает прослушивать порт 1234, ожидая начальных команд, которые синхронизируют жертву с базой данных сетевых узлов и целей перебора. Когда эта первоначальная синхронизация завершена, FritzFrog проявляет творческий подход к обнаружению уклонений, когда дело доходит до дальнейшего взаимодействия извне ботнета: «Вместо того, чтобы отправлять команды напрямую через порт 1234, злоумышленник подключается к жертве через SSH и запускает клиент netcat. на машине потерпевшего», - говорится в анализе. «С этого момента любая команда, отправляемая через SSH, будет использоваться в качестве входных данных netcat и, таким образом, передаваться вредоносной программе».

Между тем, ботнет постоянно пополняется базами данных о целях и взломанных машинах, когда он распространяется через Интернет.

«Узлы в сети FritzFrog поддерживают тесный контакт друг с другом», - отметил Харпаз. «Они постоянно пингуют друг друга, чтобы проверить подключение, обмениваться одноранговыми узлами и целями, а также поддерживать синхронизацию друг друга. Узлы участвуют в умном процессе голосования, который, по-видимому, влияет на распределение целей грубой силы по сети. Guardicore Labs заметила, что цели распределены равномерно, так что никакие два узла в сети не пытаются «взломать» одну и ту же целевую машину».

Кроме того, он был построен с обширным словарем взломанных имен и паролей для целей перебора, что сделало его очень агрессивным («Для сравнения, DDG, недавно обнаруженный P2P-ботнет, использовал только имя пользователя root», - сказал Харпаз).

Вредоносная программа также порождает несколько потоков для одновременного выполнения различных задач. Например, IP-адрес в целевой очереди будет передан в модуль взломщика, который, в свою очередь, просканирует машину, подключенную к IP-адресу, и попытается подобрать его; машина, которая была успешно взломана, ставится в очередь на заражение вредоносным ПО модулем DeployMgmt; и машина, которая была успешно заражена, будет добавлена в P2P-сеть модулем Owned.

В случае перезагрузки скомпрометированной системы вредоносная программа оставляет за собой бэкдор, учетные данные которого сохраняются узлами сети.

«Вредоносная программа добавляет открытый ключ SSH-RSA в файл authorized_keys», - говорится в исследовании. «Этот простой бэкдор позволяет злоумышленникам, владеющим секретным секретным ключом, выполнять аутентификацию без пароля в случае изменения исходного пароля».

Вредоносная программа также отслеживает состояние файловой системы на зараженных машинах, периодически проверяя доступную оперативную память, время безотказной работы, логины SSH и статистику использования процессора. Другие узлы берут эту информацию и используют ее, чтобы определить, запускать криптомайнер или нет.

Если она решает запустить майнер, вредоносная программа запускает отдельный процесс под названием «libexec» для майнинга криптовалюты Monero с дополнительным продуктом XMRig. Хотя до сих пор ботнет использовался именно для этого вторичного заражения, его архитектура означает, что он также может установить любой другой тип вредоносного ПО на зараженные узлы, если его авторы решат это сделать.

В целом, по словам Харпаз, FritzFrog очень продвинутый, но есть простой способ предотвратить компромисс: «Слабые пароли являются непосредственным фактором атак FritzFrog», - сказала она. «Мы рекомендуем выбирать надежные пароли и использовать аутентификацию с открытым ключом, что намного безопаснее».

По ее словам, администраторы также должны удалить открытый ключ FritzFrog из файла authorized_keys, чтобы предотвратить доступ злоумышленников к машине. И «маршрутизаторы и устройства IoT часто открывают доступ к SSH и поэтому уязвимы для FritzFrog; рассмотрите возможность изменения их порта SSH

или полного отключения доступа к ним по SSH, если служба не используется». ***(Tara Seals. FritzFrog Botnet Attacks Millions of SSH Servers // Threatpost (https://threatpost.com/fritzfrog-botnet-millions-ssh-servers/158489/). 19.08.2020).***

***

«Недавно обнаруженная активная кампания под названием «Duri» использует контрабанду HTML для доставки вредоносного ПО.

Была замечена активная кампания, использующая контрабанду HTML для доставки вредоносных программ, эффективно обходя различные решения сетевой безопасности, включая песочницы, устаревшие прокси-серверы и брандмауэры.

Кришнан Субраманиан, исследователь безопасности Menlo Security, сообщил Threatpost, что раскрытая во вторник кампания, получившая название «Duri», продолжается с июля .

Это работает так: злоумышленники отправляют жертвам вредоносную ссылку. Как только они нажимают на эту ссылку, используется метод JavaScript blob для переправки вредоносных файлов через браузер на конечную точку пользователя (т. Е. Контрабанда HTML). Большие двоичные объекты, которые означают «большие двоичные объекты» и отвечают за хранение данных, реализуются веб-браузерами.

Поскольку контрабанда HTML не обязательно является новой техникой - она использовалась злоумышленниками некоторое время, - сказал Субраманиан, - эта кампания показывает, что злоумышленники продолжают полагаться на старые методы атаки, которые работают. Узнайте больше об этой последней атаке и о том, как предприятия могут защитить себя от атак, связанных с контрабандой HTML, в подкасте Threatpost на этой неделе». ***(Lindsey O'Donnell. Researchers Warn of Active Malware Campaign Using HTML Smuggling // Threatpost (https://threatpost.com/active-malware-campaign-html-smuggling/158439/). 18.08.2020).***

***

«Программа-вымогатель Avaddon - это последняя киберпреступная операция по запуску сайта утечки данных, который будет использоваться для публикации украденных данных жертв, которые не платят выкуп.

С тех пор, как операторы лабиринта начали публичную утечку файлов, украденных в результате атак программ-вымогателей, вскоре последовали их примеру и начали создавать сайты утечки данных для публикации украденных файлов.

Эти сайты предназначены для того, чтобы запугать жертв и заставить их заплатить программу-вымогатель под угрозой того, что их файлы станут достоянием общественности. Если эти данные будут опубликованы, они могут раскрыть финансовую информацию, личную информацию сотрудников и данные клиентов, что приведет к утечке данных.

Компания Kela, занимающаяся разведкой кибербезопасности, сообщила BleepingComputer, что операторы программ- вымогателей Avaddon объявили на

русскоязычном хакерском форуме в эти выходные, что они открыли новый сайт утечки данных.

На данный момент на их сайте есть только одна запись, где происходит утечка 3,5 МБ документов, украденных у строительной компании.

Использование сайтов утечки данных - это тактика, которая никуда не исчезнет, и корпоративные жертвы должны признать, что все атаки программ-вымогателей теперь являются утечками данных.

Злоумышленники надеются, что дополнительные расходы, связанные с утечкой данных и потенциальным ущербом репутации, могут подтолкнуть больше жертв к уплате выкупа.

В связи с тем, что атаки программ-вымогателей переросли в утечки данных, компании должны сообщать о них своим сотрудникам и клиентам, чтобы они знали о потенциальных рисках и действовали соответственно для защиты». ***(Lawrence Abrams. Avaddon ransomware launches data leak site to extort victims // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/avaddon-ransomware-launches-data-leak-site-to-extort-victims/). 10.08.2020).***

***

«Троян Qbot снова ворует электронные письма с цепочкой ответов, которые можно использовать для маскировки зараженных вредоносными программами писем как части предыдущих разговоров в будущих вредоносных спам-кампаниях.

Qbot (также известный как QakBot) - это вредоносное ПО для банковских операций и кражи информации, которое уже более десяти лет активно заражает жертв .

После установки Qbot попытается украсть сохраненные пароли, файлы cookie, кредитные карты, электронную почту и учетные данные онлайн-банкинга своих жертв.

Также известно, что этот троян загружает и устанавливает на зараженные компьютеры другое вредоносное ПО, в том числе полезные нагрузки ProLock Ransomware.

С июля 2020 года Qbot является предпочтительным вредоносным ПО для печально известного ботнета Emotet, и в нем наблюдается всплеск новых заражений.

Qbot крадет электронные письма жертвы для будущих кампаний по борьбе со спамом

В 2019 году мы сообщили, что QBot начал красть цепочки писем жертв, используя их в рамках контекстно-зависимой фишинговой кампании в конце марта 2019 года.

Согласно новому отчету Check Point, QBot продолжает использовать тактику, ранее использовавшуюся банковским трояном Gozi ISFB, трояном для кражи информации URSNIF и трояном Emotet [1, 2, 3]: кража полных цепочек электронной почты для использование в цепочке ответов или атаках с использованием «перехваченной цепочки писем».

Фишинговая атака с цепочкой ответов - это когда злоумышленники используют украденную цепочку писем, а затем отвечают на нее своим собственным сообщением и прикрепленным вредоносным документом.

После заражения жертв одним из вредоносных действий, выполняемых Qbot, является кража электронных писем из клиента Outlook пользователя.

Эти украденные электронные письма затем загружаются на серверы злоумышленников Qbot для использования в будущих спам-кампаниях, нацеленных на других потенциальных жертв.

Этот тип атаки делает фишинговую кампанию более правдоподобной, особенно когда она используется против тех, кто находится в исходной цепочке.

Check Point обнаружила, что эти атаки по цепочке ответов содержат вложения ZIP с вложенными вредоносными сценариями VBS. При выполнении эти сценарии VBS загрузят вредоносное ПО Qbot в систему и заразят пользователя.

«Во время отслеживания кампании по распространению вредоносного спама мы видели сотни различных URL-адресов для вредоносного удаления ZIP-файлов, хотя большинство из них были взломанными сайтами WordPress», - поясняют исследователи Check Point.

Использование украденной электронной почты жертвы против других получателей создает постоянный цикл новых жертв, используемых против других для распространения вредоносного ПО.

После добавления этого модуля кражи цепочек писем исследователи Check Point обнаружили целевые перехваченные цепочки писем, которые используются в текущих кампаниях по темам, связанным с напоминаниями об уплате налогов, пандемией Covid-19 и предложениями о работе.

Вредоносное ПО, используемое в целевых кампаниях

Авторы Qbot также добавляли необычные возможности в тот или иной момент, а также умный способ сборки вредоносного ПО из двух зашифрованных половин, чтобы избежать обнаружения при доставке в систему цели.

Вредоносная программа также известна тем, что заражает другие устройства в той же сети, используя эксплойты сетевых ресурсов, а также очень агрессивные атаки методом перебора, нацеленные на учетные записи администратора Active Directory.

Несмотря на то, что он был активен более десяти лет, этот банковский троян в основном использовался в целенаправленных атаках на корпоративные объекты, которые могли обеспечить более высокий возврат инвестиций.

В качестве доказательства этого, атаки Qbot с течением времени были довольно редкими: исследователи обнаружили одну в октябре 2014 года, одну в апреле 2016 года, а также еще одну в середине мая 2017 года. Qbot вернулся в прошлом году, будучи сброшенным в качестве полезной нагрузки первого или второго уровня бандой Emotet». ***(Lawrence Abrams. Qbot steals your email threads again to infect other victims // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/qbot-steals-your-email-threads-again-to-infect-other-victims/). 27.08.2020).***

***

«Специалисты исследовательской группы Graphika рассказали о том, как им удалось обнаружить в Twitter ботнет, состоявший примерно из 3000 ботов, которые распространяли прокитайский политический спам и повторяли официальные сообщения, распространяемые через государственные аккаунты.

Обнаружить ботнет удалось благодаря весьма экзотической причуде его создателей: подавляющее большинство бот-акаунтов использовало цитаты из «Дракулы» Брэма Стокера для первых двух твитов, а также в качестве описания профиля. Именно поэтому ботнет и получил такое название.

Ботнет Dracula во многом схож с другими Twitter-ботнетами, которые являются частью Spamouflage — это кодовое имя исследователи присвоили китайским правительственным операциям по усилению влияния в социальных сетях. Подобные кампании аналитики Graphika уже обнаруживали в сентябре 2019 года, в апреле 2020 года, а также в августе 2020 года. От других ботнетов Dracula отличает лишь то, что он сумел накопить только 3000 учетных записей, и самые старые из них датируются июлем 2020 года.

Исследователи объясняют, что бот-аккаунты не были опасны сами по себе. По всей видимости, они были автоматизированы и в основном либо цитировали «Дракулу», либо отвечали на твиты друг друга. При этом главной задачей этих учетных записей было «усиление» конкретных твитов и заранее определенных трендов, которые могли использоваться для продвижения государственной пропаганды Китая.

В настоящее время деятельность ботнета уже была прервана: Dracula прекратил работу 20 августа 2020 года, после того как вмешались разработчики Twitter. Большинство учетных записей ботнета было забанено, а некоторые аккаунты получили статус «ограниченных», что не позволяет им публиковать новый контент. При этом неясно, были эти аккаунты заблокированы неким защитным алгоритмом Twitter, или же сотрудники социальной сети сами обнаружили ботнет и прекратили его работу вручную». ***(Мария Нефёдова. В Twitter обезвредили пропагандистский ботнет Dracula // Xakep (https://xakep.ru/2020/08/27/dracula/). 27.08.2020).***

***

«Вредоносные вложения продолжают оставаться основным вектором угрозы в мире киберпреступников, даже несмотря на то, что общественная осведомленность растет, а технологические компании усиливают свою защиту.

Хотя векторы угроз, связанных с вложениями, являются одним из старейших приемов распространения вредоносных программ в книгах, пользователи электронной почты по-прежнему нажимают на вредоносные вложения, которые попадают в их почтовый ящик, будь то предполагаемое «предложение о работе» или мнимый «критический счет».

Исследователи говорят, что причина, по которой злоумышленники до сих пор полагаются на эту давнюю тактику, заключается в том, что атака все еще работает. Даже несмотря на широкую осведомленность общественности о вредоносных

файловых вложениях, злоумышленники расширяют свою игру с помощью новых уловок, позволяющих избежать обнаружения, обхода защиты электронной почты и т. Вектор атаки по-прежнему достаточно широко распространен, и технические гиганты заново изобретают новые способы, чтобы попытаться подавить его, а Microsoft только на этой неделе представила функцию для Office 365, которая направлена на защиту пользователей от вредоносных вложений, отправленных, например, по электронной почте.

«Вложения электронной почты, такие как файлы PDF или Office, являются простым средством доставки вредоносного контента конечным пользователям, - сказал Threatpost Мохит Тивари, соучредитель и генеральный директор Symmetry Systems. «Для предприятий риск состоит в том, что злоумышленники могут использовать эти вложения, чтобы установить опору на внешних границах предприятия, а затем ждать и прокладывать себе путь к жемчужинам короны в своих хранилищах данных».

Новая тактика

Отчет Verizon Data Breach Investigations Report (DBIR) за 2020 год показал, что вложения электронной почты являются основным вектором вредоносных программ, которые приводят к утечкам данных, при этом почти 20% атак вредоносных программ развертываются через вложения электронной почты. Электронные ссылки являются основным вектором атак с использованием этого метода 40%.

Хотя зараженные вредоносным ПО вложения, такие как файлы ZIP, PDF и MS office (включая вложения файлов DOC и XLSM), являются более часто используемыми вложениями, исследователи предупреждают, что злоумышленники начинают обращать внимание на новые вложения, такие как файлы образов дисков (ISO или IMG). файлы, которые хранят содержимое и структуру всего диска, например DVD или Blue-Ray) - как способ все более широкого распространения вредоносных программ.

Использование различных «приманок», используемых с помощью социальной инженерии для убеждения цели открыть привязанность, также развивается. Исследователи отметили резкий всплеск спам-кампаний на налоговую тематику в марте 2019 года, в которых использовались файлы DOC и XLSM (таблица с поддержкой макросов, созданная Microsoft Excel), например, для доставки модульного банковского трояна Trickbot. В этом году ситуация только ухудшилась из-за текущей пандемии, поскольку кибератаки стремятся рассылать вредоносные вложения под видом информации о Covid, работать из домашних ресурсов и другой важной информации.

Вредоносные вложения больше не отправляются только по электронной почте. Государственный оператор угроз Lazarus Group недавно нацелился на администраторов криптовалютной фирмы, например, с помощью вредоносных документов, отправленных через сообщения LinkedIn .

Обновленная защита

Даже в то время как злоумышленники активизируют свои атаки на основе электронной почты, поставщики услуг электронной почты и компании, занимающиеся производственными приложениями, также предпринимают шаги

для устранения этого распространенного вектора угроз. В 2019 году Microsoft запретила почти 40 новых типов расширений файлов на своей почтовой платформе Outlook в надежде, что этот шаг помешает пользователям загружать вложения электронной почты с различными расширениями файлов (включая те, которые связаны с Python, PowerShell, цифровыми сертификатами, Java и другими). . Google придерживается аналогичной политики в отношении своей почтовой службы Gmail и блокирует определенные типы файлов, включая их сжатую форму (например, файлы .gz или .bz2) или файлы, находящиеся в архивах (например, файлы .zip или .tgz).

Тем временем Microsoft на этой неделе выпускает долгожданную функцию Office 365, Application Guard для Office, которая изолирует файлы приложений для повышения производительности Office 365 (включая Word, Powerpoint и Excel), которые могут быть вредоносными. Инструмент нацелен на общий вектор атаки - целевые фишинговые кампании и другие веб-атаки, - которые будут использовать документы Word или другие вложения на основе Office в качестве средства распространения вредоносных программ. В настоящее время функция доступна в общедоступной предварительной версии. Это состояние, при котором продукт или услуга Microsoft не завершены, но доступны для предварительной версии, чтобы клиенты могли получить ранний доступ и оставить отзыв.

«Файлы из Интернета и других потенциально небезопасных мест могут содержать вирусы, черви или другие виды вредоносных программ, которые могут нанести вред компьютеру и данным ваших пользователей», - говорится в сообщении Microsoft на этой неделе. «Чтобы защитить ваших пользователей, Office открывает файлы из потенциально небезопасных мест в Application Guard, безопасном контейнере, изолированном от устройства с помощью аппаратной виртуализации».

Application Guard специально защищает от файлов, которые загружаются из доменов, которые не являются частью локальной интрасети или домена «Надежные сайты» на устройстве пользователя, файлов, которые были получены в виде вложений электронной почты от отправителей за пределами организации пользователя, файлов, которые были полученные из других типов интернет-сообщений или служб общего доступа или файлов, открытых из OneDrive или SharePoint вне организации пользователя.

«Подобные функции будут постоянно развиваться для борьбы с постоянно меняющимся полем битвы в области кибербезопасности», - сказал Threatpost Джастин Кезер, управляющий консультант nVisium. Однако, по словам Кезера, «проблема в том, что провайдеры электронной почты будут продолжать бороться, потому что безопасность электронной почты - это согласие, а не политика отказа».

«Компании должны будут правильно настроить свою Active Directory и широко внедрить эту новую функцию, однако печальная реальность такова, что большинство компаний не внедряют эти функции из-за предполагаемого влияния на бизнес», - сказал Кезер.

Эта загадка указывает на одну из самых больших проблем в защите от атак вредоносных вложений: конечных пользователей и самих корпоративных организаций.

Исследователи из Proofpoint исследовали приоритеты предприятий в защите от трех типов фишинговых приманок - ссылок, вложений и запросов на ввод данных. Хотя в 2019 году тесты на прикрепление не входили в список приоритетов организаций, они оказались наиболее эффективными для обмана пользователей. В смоделированных тестах на фишинг, развернутых организациями для тестирования своих сотрудников, большинство фишинговых тестов с наибольшим количеством отказов (65 процентов) основывались на прикреплении файлов.

Это показывает, что обучение пользователей и готовность предприятий уделять приоритетное внимание защите от векторов угроз, основанных на прикрепленных файлах, являются важными элементами защиты от подобных атак, считают исследователи.

«Общие связи и темы в этих списках - все подкрепляют наши советы по более частому тестированию уязвимостей вложений и добавлению большей персонализации в имитированные фишинговые кампании. По словам Proofpoint, даже если вы будете реже сталкиваться с атаками на основе вложений, они будут проблемой для вашей организации, если почти все пользователи попадутся на них». ***(Lindsey O'Donnell. Malicious Attachments Remain a Cybercriminal Threat Vector Favorite // Threatpost (https://threatpost.com/malicious-attachments-remain-a-cybercriminal-threat-vector-favorite/158631/). 27.08.2020).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Три людини були звинувачені в п’ятницю через їх ймовірну причетність до масового злому акаунтів Twitter на початку липня, після чого акаунти таких відомих користувачів, як Джо Байден, Барак Обама та Ілон Маск були використані для просування афери з криптовалютою…

Серед обвинувачених були Мейсон Шеппард, 19-річний британець, який користувався в мережі прізвиськом “Чехвон”, Нім Фазелі, 22-річний житель Орландо, штат Флорида, який користувався прізвищем “Ролекс”, а також неповнолітній, згідно із заявою прокурора США Девід Андерсон.

Неповнолітнім виявився 17-річний Грем Іван Кларк, який був заарештований в п’ятницю вранці в Тампі після розслідування, проведеного федеральними та державними слідчими, сказав в п’ятницю в заяві прокурор штату. У заяві стверджувалося, що Кларк був “натхненником”.

Прокурор сказав, що його офіс займається звинуваченням, тому що закон Флориди дозволяє більш гнучко, ніж федеральний закон, звинувачувати неповнолітніх як дорослих людей у подібних справах.

“У кримінальному хакерському співтоваристві існує хибне переконання, що такі атаки, як хакерство в Твіттері, може бути здійснено анонімно і без наслідків”, — сказав Андерсон у своїй заяві. “Сьогоднішнє оголошення про пред’явлення

звинувачень демонструє, що задоволення від мерзенного хакерства в безпечному середовищі заради забави або прибутку буде короткочасним".

ФБР повідомило, що двоє людей, звинувачених у зломі акаунтів, були взяті під варту.

"Сьогоднішні арешти є лише першим кроком для правоохоронних органів", — сказав помічник спеціального агента ФБР в Сан-Франциско за звинуваченням Санджай Вірмані. "Наше розслідування продовжить виявляти всіх, хто міг бути причетний до цих злочинів"…». ***(Ілля Нежигай. CNN: до хакерської атаки на Twitter причетний неповнолітній, його затримали // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1883707-cnn-do-khakerskoyi-ataki-na-twitter-prichetniy-nepovnolitniy-yogo-zatrimali). 01.08.2020).***

***

«Бывшему начальнику службы безопасности Uber Джону Салливану было предъявлено обвинение в попытке скрыть от федеральных следователей взлом, в результате которого добычей злоумышленников стали адреса электронной почты и номера телефонов 57 миллионов водителей и пассажиров сервиса интернет-такси.

Согласно пресс-релизу Минюста США, Салливан не сообщил об инциденте представителям Федеральной торговой комиссии США, расследовавшим взлом Uber в 2014 году.

Вместо этого Салливан предпочел заплатить организаторам атаки $100 тыс. в биткоинах. Выплата осуществлялась через программу вознаграждений за найденные уязвимости Uber. Кроме того, бывший топ-менеджер пытался убедить хакеров подписать соглашение о неразглашении.

Салливан работал в компании с 2015-го по 2017-й годы, он был уволен после того, как руководству стало известно, каким образом глава отдела безопасности справился с ситуацией.

Помимо обвинения в препятствии правосудию, прокуратура обвинила Салливана в сокрытии факта мошенничества. В общей сложности по предъявленным пунктам обвинения бывшему безопаснику Uber грозит до восьми лет лишения свободы». ***(Экс-главу отдела безопасности Uber в США обвинили в сокрытии факта утечки данных 57 млн водителей и клиентов // РосКомСвобода (https://roskomsvoboda.org/62726/). 21.08.2020).***

***

«Издание ZDNet, со ссылкой на болгарских правоохранителей, сообщает о задержании хакера Instakilla (настоящее имя не разглашается). Подозреваемого обвиняют во взломе, вымогательстве и продаже похищенной у компаний информации в интернете. В ходе обысков в Пловдиве у хакера были изъяты несколько компьютеров, смартфонов, флеш-накопителей, а также неназванное количество криптовалюты.

Instakilla активен примерно с 2017 года, хотя широкую известность он получил лишь в прошлом году. Так, летом 2019 года именно Instakilla слил в сеть

информацию, похищенную у Национального налогового управления Болгарии, хотя он и не принимал непосредственно участия в самом взломе.

Осенью того же года хакер скомпрометировал официальные форумы Comodo, а затем взял на себя ответственность за взлом ряда итальянских и голландских форумов для секс-работников (в этих странах проституция является законной).

В текущем году Instakilla связывали с крупным взломом форумов Stalker Online, откуда он похитил более 1,2 миллиона пользовательских записей, которые затем выставил на продажу на хакерском форуме. На этом же форуме у злоумышленника было что-то вроде собственного «магазина», где он продавал похищенные у компаний данные (включая две неназванные болгарские организации, местного хостинг-провайдера и сервис электронной почты). Причем в итоге Instakilla забанили на этом форуме за мошенничество.

Как несложно понять по перечисленным выше инцидентам, в основном Instakilla предпочитал взламывать уязвимые форумы vBulletin, откуда он похищал базы данных. Также у преступника был собственный сайт, где он предлагал свои хакерские услуги всем желающим.

В настоящее время известно, что Instakilla был задержан властями на 72 часа». ***(Мария Нефёдова. Полиция Болгарии арестовала хакера Instakilla // Хакер (https://xakep.ru/2020/08/07/instakilla/). 07.08.2020).***

***

«Основатель SpaceX и Tesla, американский предприниматель Илон Маск подтвердил, что его завод по производству электромобилей хотела атаковать группа российских хакеров.

Недавно ФБР задержала россиянина Егора Крючкова, который нашёл русскоговорящего сотрудника Gigafactory в Неваде, предложив ему 1 млн долларов наличными или биткоинами за внедрение в компьютерную сеть Tesla. Крючков хотел, чтобы тот установил вредоносное программное обеспечение на свой рабочий компьютер. Таким образом россиянин планировал получить доступ к системе компании и потребовать у нее выкуп за то, чтобы не обнародовать информацию.

После того, как с Крючковым связались сотрудники ФБР, он переехал из города Рино, штат Невада, в Лос-Анджелес, где попросил своего знакомого купить ему билет на самолет из страны, рассказали в Минюсте. 22 августа Крючкова задержали.

Некоторое время название компании не разглашалось, но вскоре сама Tesla сообщила о факте, что их работник отказался от столь внушительной суммы и, сотрудничая с ФБР, предотвратил кибератаку на производителя электромобилей.

Сотрудник, личность которого пока не разглашается, имел доступ к компьютерным сетям компании. Исходя из того, как действовал россиянин, компания и американские правоохранители предполагают, что за ним стоит команда, которая «хорошо провела своё расследование».

Работник Tesla после этой встречи проинформировал о планах руководство компании и его дальнейшее общение с российским хакером проходило под

контролем ФБР. Как сообщается в публикации, к которой приложены документы ФБР, в результате была получена, в частности, информация, что именно Крючков и его подельники стоят за атакой на сети американской компании CWT Travel, которая в итоге выплатила злоумышленниками за похищенную информацию 4,5 млн долларов. После опубликования новости в Twitter, Илон Маск в реплае написал:

«Очень признателен. Это была серьёзная атака».

Таким образом он подтвердил историю, описанную на сайте мультимедийной компании Teslarati, специализирующейся на освещении Tesla, Space X и других инновационных проектах Маска. В опубликованной на сайте Teslarati статье содержатся подробности данного «триллера», как охарактеризовали этот инцидент авторы статьи». ***(Илон Маск подтвердил факт готовившейся российскими хакерами кибератаки на завод Tesla // РосКомСвобода (https://roskomsvoboda.org/63058/). 28.08.2020).***

***

Технічні аспекти кібербезпеки

«Эксперты компании Armis представят на конференции Black Hat USA разработанную ими атаку EtherOops, которая эксплуатирует проблемы кабелей Ethernet и может использоваться для обхода сетевой защиты, а также для атак на устройства внутри закрытых корпоративных сетей.

По сути, атака EtherOops полагается на неисправные кабели Ethernet, расположенные на пути от злоумышленника к его жертве. Специалисты уверены, что из-за особых условий, требуемых для реализации атаки, EtherOops вряд ли станет массовой проблемой, угрожающей компаниям по всему миру. Тем не менее, атака все же осуществима на практике, а значит, может использоваться в определенных сценариях, и совсем сбрасывать ее со счетов тоже нельзя.

EtherOops представляет собой вариацию атаки типа packet-in-packet. В такой разновидности атак пакеты вложены друг в друга, и внешняя оболочка — это безвредный пакет, тогда как внутреннее содержимое — это вредоносный код или команда. Внешний пакет позволяет скрыть полезную нагрузку от средств сетевой защиты, тогда как внутренний пакет предназначается для атак на устройства внутри сети.

Исследователи Armis рассказывают, что благодаря EtherOops атаку типа packet-in-packet можно поднять на новый уровень. Дело в том, что неисправные кабели (которые имеют проблемы в работе из-за некорректной разводки, или из-за созданных злонамеренно помех) страдают от переворотов битов, что постепенно разрушает внешнюю оболочку и оставляет лишь внутренний пейлоад.

Таким образом, атака EtherOops может использоваться для проникновения в сети компаний из интернета; проникновения во внутренние сети из сегмента DMZ; бокового перемещения между различными сегментами внутренних сетей.

Специалисты Armis признают, что атака EtherOops сложна в реализации и требует ряда особых условий. Так, неисправные кабели должны присутствовать на

ключевых позициях внутри целевой сети. В большинстве сценариев злоумышленнику, скорее всего, потребуется заманить пользователя на вредоносный сайт, чтобы получить прямое соединение с жертвой внутри корпоративной сети для доставки полезных нагрузок. Кроме того, перевороты битов, это не слишком частое явление, а значит, придется бомбардировать целевую сеть множеством пакетов в надежде на удачный переворот битов, и процент успешных атак будет крайне мал.

«Сложно? Да, но не невозможно», — резюмируют эксперты.

Самый простой способ защиты от EtherOops — использование экранированных кабелей Ethernet или защитных решений, способных обнаруживать атаки типа packet-in-packet.

Исследователи уже создали для проблемы EtherOops специальный сайт, а также опубликовали 44-страничный отчет, описывающий все технически аспекты атаки…» ***(Мария Нефёдова. Атака EtherOops использует проблемы кабелей Ethernet // Xakep (https://xakep.ru/2020/08/06/etheroops/). 06.08.2020).***

***

«Науковці Чиказького університету розробили додаток Fawkes, який допомагає обманути системи розпізнавання облич Clearview AI. Завдяки новому інструменту вченим вдалось обманути системи розпізнавання облич Amazon, Microsoft, Facebook та китайського технічного гіганта Megvii, який розробляє системи розпізнавання облич, повідомляє New York Times.

Розробники назвали додаток Fawkes на честь знаменитої маски Гая Фокса. Він на рівні пікселів майже не помітно змінює зображення так, що його не розпізнають системи розпізнавання облич. Науковці продемонстрували це, пропустивши через систему фотографії Гвінет Пелтроу, Джессіки Сімпсон і Патріка Демпсі.

«Наша мета - змусити Clearview піти», - сказав професор комп'ютерних наук в університеті Чикаго Бен Чжао.

Додаток на веб-сайті розробників вже завантажили 50 тисяч користувачів. Хоча не обійшлось без курйозів. Журналістка видання New York Times Кашмір Хілл пропустила через програму фотографії членів своєї родини. 3-річній доньці журналістки програма намалювала бороду, а чоловікові змінила колір очей.

Розробники програми це пояснили тим, що Fawkes зіставляє зображення з зображеннями людей протилежної статі, які є в базі програми. Тому у жінок можуть з’являтись вуса і борода, а у чоловіків - довгі вії. Однак у майбутньому науковці планують удосконалити додаток, щоб він не змінював стать…». ***(Вчені створили додаток для захисту фотографій від систем розпізнавання облич // MEDIASAPIENS (https://ms.detector.media/it-kompanii/post/25232/2020-08-10-vcheni-stvorili-dodatok-dlya-zakhistu-fotografii-vid-sistem-rozpiznavannya-oblich/). 10.08.2020).***

***

«Хотя цифровая подпись должна защищать PDF от любых изменений, существуют возможности обойти защиту. Средства просмотра PDF-документов

интерпретируют некоторые изменения как малозначительные и безопасные, притом, что злоумышленники могут подменить содержание отдельных частей или даже всего документа. Как это сделать, продемонстрировали эксперты Рурского университета в Бохуме.

Несущественные изменения

Исследователи при Рурском университете в Бохуме (Германия) описали новый тип атак под общим названием Shadow attacks, позволяющих подменять содержимое защищенных PDF-файлов без нарушения целостности их цифровой подписи.

Суть атаки состоит в том, что злоумышленник может создать PDF с двумя разными типами содержимого. Один тип — ожидаемые данные со стороны тех, кто будет производить подписание PDF-документа. Второй — скрытые данные, отображаемые после того, как PDF-файл получает цифровую подпись. В результате подписант и получатель PDF могут видеть разную информацию, хотя средства просмотра не наблюдают никаких нарушений.«Если же средство просмотра не принимает изменения в структурных объектах PDF (Page, Pages, Contents), возможен второй вариант атаки, при котором оказывается прямое воздействие на перекрывающий объект посредством манипуляции таблицы Xref — каталога, в котором перечислены объекты внутри основного раздела и их местонахождение.

«Самый простой способ — создать инкрементное обновление, которое изменяет лишь содержание таблицы Xref; перекрывающему объекту присваивается значение free, — пишут исследователи. — Во многих случаях, однако, просмотрщики (включая официальный пакет Adobe) будут рассматривать это изменение как рискованное, поэтому выводится предупреждение. Поэтому мы применяем другой подход: при инкрементном обновлении мы используем тот же объект с тем же идентификатором, но меняем его тип. Например, вместо перекрывающего изображения (Image) обозначается тип XML/Metadata. Кроме того, мы изменяем таблицу Xref с указателем на объект метаданных, но сохраняем идентификатор перекрывающего объекта. При открытии модифицированного документа перекрывающий объект скрывается, поскольку метаданные не могут отображаться. При этом добавление метаданных к подписанному PDF-документу через инкрементное обновление считается безвредным, так что подпись не нарушается».

Аналогичным образом реализуемы и две другие атаки, одна из которых позволяет подменять данные, а другая — и подменять, и прятать их. В обоих случаях изменения в PDF можно произвести таким образом, чтобы средства просмотра считали их безвредными, хотя в действительности выводимые получателю данные могут радикально отличаться от тех, которые видел подписант.

Например, подмена шрифтов считается безвредной, но позволяет подменять некоторые символы. Кроме того, есть возможность модифицировать интерактивные формы в PDF так, что при получении подписи выводится одно значение, а при открытии потенциальной жертвой в том же документе отображаются другие данные.

И скажем, что так и было

Для этого злоумышленник может использовать функцию текстовых полей в PDF, позволяющих перекрывать основное содержание поля дополнительным — которое исчезает, как только выделен текст основного поля.

«Реальное значение формы содержится в ключе объекте /V, — отмечают исследователи. — Контент перекрывающего элемента определяется объектом /BBox. Этот объект похож на всплывающие подсказки в HTML-формах; например, пользователю выводится некое имя, указывающее на то, что в данное поле необходимо ввести свой логин. Однако, в отличие от HTML, в PDF нет визуальной разницы между подсказкой и реальным значением»,

Еще один вариант атаки предполагает, что в модифицированном, «теневом» документе задается некий шрифт плюс внедряется его описание. Шрифт используется для отображения определенной части контента. После подписания документа злоумышленники добавляют новое описание шрифта — поверх старого. А поскольку задание нового шрифта не считается источником угрозы, подобные манипуляции игнорируются средствами просмотра.

Наиболее опасной является третья атака (Hide-and-Replace — скрыть и подменить), которая позволяет заменить фактически весь контент в PDF-документе.

Точнее, речь идет о PDF с двойным содержанием — одно выводится подписанту, другое — получателю, при этом разное содержание хранится в объектах с одним и тем же идентификатором, так что посредством небольшого изменения таблицы Xref и раздела Trailer, с которого программы просмотра начинают обработку PDF-документа, можно добиться того, что воспринимаемое содержание документа радикально изменится при сохранении целостности цифровой подписи.

Однако, как отметили исследователи, неиспользуемые (невидимые подписанту) объекты могут быть удалены в процессе назначения цифровой подписи; вдобавок антивирусы могут среагировать на неиспользуемые объекты и вывести предупреждение. В этом случае атака не получится.

«Сама возможность подменять содержимое в документе с цифровой подписью — это, казалось бы, нонсенс, однако, как видим, существуют способы обходить защиту, — отмечает Алексей Водясов, эксперт по информационной безопасности компании SEC Consult Services. — Возможности атакующих ограничены, но подмена даже одного какого-то показателя в важном документе может иметь катастрофические последствия, так что возможность даже “незначительных” изменений в подписанном документе необходимо исключить». ***(Найден способ подменять содержимое в PDF-документе с цифровой подписью // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5685747-Najden-sposob-podmenyat-soderzhimoe.html). 11.08.2020).***

***

«Ученые из Швейцарской высшей технической школы Цюриха разработали атаку, которая позволяет не водить PIN-код во время совершения бесконтактных платежей по картам Visa Credit, Visa Electron и VPay. Данная атака позволяет злоумышленнику, который владеет данными украденной

бесконтактной карты Visa, использовать карту для оплаты дорогостоящих товаров, чья цена намного превышает лимит бесконтактных транзакций. И PIN-код при этом не понадобится.

Доклад, описывающий эту технику атак, уже опубликован в открытом доступе, а полноценную презентацию своих изысканий специалисты намерены устроить на симпозиуме IEEE, который пройдет в мае 2021 года.

Ученые рассказывают, что придуманную ими атаку очень трудно обнаружить, ведь злоумышленник будет похож на обычного клиента, который расплачивается на покупку с помощью смартфона. На самом же деле атакующий будет расплачиваться украденной бесконтактной картой Visa, которая спрятана где-то на него теле.

Для этой атаки не нужно сложное оборудование, понадобятся лишь два смартфона на Android, специальное приложение, созданное исследовательской группой, а также сама бесконтактная карта. При этом приложение, установленное на обоих смартфонах, будет работать в качестве эмулятора PoS-терминала и эмулятора самой карты.

В итоге атака выглядит следующим образом: смартфон, который имитирует PoS-устройство, помещают рядом с украденной картой, а смартфон, работающий в качестве эмулятора карты, используют для оплаты товаров. Идея заключается в том, что эмулятор PoS просит карту произвести платеж и модифицирует детали транзакции, а затем передает измененные данные через Wi-Fi на второй смартфон, который в итоге совершает крупный платеж без необходимости ввода PIN-кода (ведь злоумышленник изменил данные транзакции таким образом, чтобы ввод PIN-кода не требовался). Демонстрацию атаки можно увидеть ниже.

«Наше приложение не требует root-прав или каких-либо хитроумных хаков Android. Мы успешно протестировали его на обычных устройствах Pixel и Huawei», — пишут исследователи.

Если говорить о технической стороне вопроса, такая атака возможна из-за конструктивных недостатков стандарта EMV и бесконтактного протокола Visa. Эти баги позволяют злоумышленнику модифицировать данные бесконтактной транзакции, включая те поля, которые отвечают за детали транзакции и необходимость верификации владельца карты.

По сути, злоумышленник сообщает терминалу, что проверка PIN-кода не требуется, а владелец карты уже прошел верификацию на потребительском устройстве (например, на смартфоне). Причем эти модификации осуществляют на том смартфоне, где работает эмулятор PoS, и совершаются перед отправкой на второй смартфон. То есть на настоящее PoS-устройство передается уже измененная информация, и оно не может определить, были ли модифицированы детали транзакции.

Для обнаружения этих проблем исследователи использовали модифицированную версию инструмента под названием Tamarin, который ранее уже применялся для обнаружения сложных уязвимостей в криптографическом протоколе TLS 1.3 (PDF), а также в механизме аутентификации 5G (PDF).

С помощью этого же инструмента эксперты выявили еще одну потенциальную проблему, которая затрагивает не только Visa, но и Mastercard.

Данную брешь исследователи не тестировали «в полевых условиях» по этическим соображениям. Вот как эксперты описывают вторую проблему:

«Также наш символический анализ выявил, что в ходе оффлайновой бесконтактной транзакции с помощью карты Visa или старой карты Mastercard, карта не аутентифицируется с терминалом посредством ApplicationCryptogram (AC) — созданного картой криптографического доказательства транзакции, которое терминал не может верифицировать (может только эмитент карты). Это позволяет злоумышленникам обманом вынудить терминал принять недостоверную оффлайновую транзакцию. Позже, когда эквайер добавит данные транзакции к клиринговой записи, банк-эмитент обнаружит неверную криптограмму, но к тому времени преступник уже давно скроется вместе с товаром». ***(Мария Нефёдова. Атака позволяет обойтись без ввода PIN-кода при бесконтактных платежах Visa // Xakep (https://xakep.ru/2020/08/28/no-pin-required/). 28.08.2020).***

***

«Пользователи популярных интернет-сервисов заявили о проблемах с доступом. Об этом свидетельствуют данные портала Downdetector.

Так, среди пострадавших сервисов оказались Google, Amazon Web Service, а также Discord, Cloudflare и другие.

На проблемы в регистрации в Google жаловались 44% пользователей, а еще 55% испытывали трудности с поиском.

Проблемы начались примерно в 12-45 по московскому времени. Наибольшее количество неполадок в работе зафиксировано в России, Сингапуре, Германии, Франции, Великобритании, Турции и Индии.

Кроме того, среди пользователей Discord 91% жалоб касается проблем с подключением к серверу. По данным портала Techcrunch, неполадки в работе сервисов связаны с проблемами работы службы Cloudflare.

В результате сбоя также пострадала сборная Индии по шахматам в финале онлайн олимпиады на портале chess.com, использующем ресурсы Cloudflare. В решающих матчах трое игроков сборной Индии отключились от игры в разгар партий и двоим из них были засчитаны технические поражения. Президент ФИДЕ Аркадий Дворкович решил объявить победителями Олимпиады обе сборные России и Индии, хотя перед отключением Россия вела в счете и была предварительно объявлена победителем». ***(Произошел сбой работы интернет сервисов по всему миру // SecurityLab.ru (https://www.securitylab.ru/news/511577.php).30.08.2020).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Владельцам сайтов WordPress, которые используют плагин Newsletter, рекомендуется обновить свои установки, чтобы заблокировать атаки, которые

могут использовать исправленную уязвимость, позволяющую хакерам внедрять бэкдоры, создавать мошеннических администраторов и потенциально захватить их веб-сайты.

Уязвимость была обнаружена в плагине Newsletter WordPress, который предоставляет инструменты, необходимые для создания адаптивных информационных бюллетеней и маркетинговых кампаний по электронной почте в блогах WordPress с использованием визуального композитора.

Информационный бюллетень был загружен более 12 миллионов раз с тех пор, как он был добавлен в официальный репозиторий плагинов WordPress и теперь установлен более чем на 300 000 сайтов.

Исправлено в течение двух дней

В отчете, опубликованном сегодня командой Wordfence Threat Intelligence, аналитик угроз Рам Галл говорит, что он обнаружил два дополнительных недостатка безопасности при анализе предыдущего исправления, опубликованного разработчиками плагина 13 июля.

Wordfence обнаружил отраженный недостаток межсайтового скриптинга (XSS) и уязвимость PHP Object Injection, которые были полностью исправлены командой разработчиков Newsletter 17 июля с выпуском версии 6.8.3, через два дня после первоначального отчета, отправленного 15 июля.

В то время как эти два недостатка оцениваются как проблемы средней и высокой степени серьезности, которые могут позволить злоумышленникам добавлять мошеннических администраторов и внедрять бэкдоры после успешного использования отраженной проблемы XSS на сайтах, на которых запущены уязвимые версии плагина Newsletter.

Кроме того, уязвимость внедрения объекта PHP "может быть использована для внедрения объекта PHP, который может быть обработан кодом из другого плагина или темы и использован для выполнения произвольного кода, загрузки файлов или любых других тактик, которые могут привести к захвату сайта, "по словам Галла.

По меньшей мере 150 000 сайтов все еще подвержены атакам

Несмотря на то, что информационный бюллетень 6.8.3, версия плагина, которая поставляется с исправлением для двух уязвимостей, была выпущена 17 июля, с тех пор плагин был загружен только 151449 раз, согласно историческим данным о загрузках, включая обновления и новые установки.

Это означает, что по крайней мере 150 000 сайтов WordPress с активными установками информационных бюллетеней все еще потенциально подвержены потенциальным атакам, если хакеры начнут использовать эти ошибки в рамках будущих кампаний.

Пользователям рассылки настоятельно рекомендуется как можно скорее обновить плагин до версии 6.8.3, чтобы заблокировать атаки, предназначенные для добавления мошеннических администраторов или внедрения бэкдоров на свои сайты, учитывая, что злоумышленники часто используют в своих атаках уже исправленные уязвимости плагина WordPress.

Например, два месяца назад Wordfence сообщил о кампании, нацеленной на сотни тысяч сайтов WordPress в течение 24 часов, с попыткой собрать учетные

данные базы данных путем кражи файлов конфигурации после успешного использования известных недостатков XSS, влияющих на плагины и темы WordPress.

«В период с 29 по 31 мая 2020 года брандмауэр Wordfence заблокировал более 130 миллионов атак, направленных на сбор учетных данных баз данных с 1,3 миллиона сайтов путем загрузки их файлов конфигурации», - сказал тогда Галл.

На прошлой неделе уязвимость максимальной степени серьезности, обнаруженная в плагине wpDiscuz, установленном на более чем 70 000 сайтов WordPress, позволила хакерам захватить учетные записи хостинга с помощью атак удаленного выполнения кода». ***(Sergiu Gatlan. Newsletter plugin bugs let hackers inject backdoors on 300K sites // Bleeping Computer (https://www.bleepingcomputer.com/news/security/newsletter-plugin-bugs-let-hackers-inject-backdoors-on-300k-sites/). 03.08.2020).***

***

«Google исправил критическую ошибку, влияющую на Gmail и G Suite, которая позволяла злоумышленникам отправлять поддельные вредоносные электронные письма, как любой другой пользователь Google или корпоративный клиент.

По словам исследователя в области безопасности Эллисон Хусейн, которая обнаружила проблему безопасности, вызванную отсутствием проверки при настройке почтовых маршрутов, "строгая политика DMARC / SPF как Gmail, так и любого клиента G Suite может быть нарушена путем использования правил маршрутизации почты G Suite для ретрансляции и подтверждения подлинности мошеннических Сообщения."

Злоупотребление собственным сервером Google для придания аутентичности

Эта проблема была вызвана «отсутствием проверки при настройке почтовых маршрутов», как подробно описала исследователь безопасности Эллисон Хусейн, которая обнаружила ошибку и сообщила о ней в Google 3 апреля 2020 года.

Чтобы использовать этот недостаток для отправки аутентифицированных поддельных электронных писем, которые могут пройти как SPF, так и DMARC, злоумышленникам придется злоупотребить проблемой неработающего получателя в правилах проверки почты Google и использовать шлюз входящей электронной почты для повторной отправки сообщения из бэкэнда Google, чтобы последующие почтовые серверы могли автоматически доверять ему.

"Это выгодно для злоумышленника, если жертва, которую он намеревается выдать себя за другое лицо, также использует Gmail или G Suite, поскольку это означает, что сообщение, отправленное серверной частью Google, будет проходить как SPF, так и DMARC, поскольку их домен по своей природе использования G Suite будет настроен на разрешить серверу Google отправлять почту из своего домена ", - пояснил Хусейн.

«Кроме того, поскольку сообщение исходит от серверной части Google, также вероятно, что сообщение будет иметь более низкий рейтинг спама, и поэтому его следует фильтровать реже»…

Как показано на графике раскрытия информации, опубликованном Хусейном, Google принял проблему 16 апреля, но классифицировал ее как ошибку с приоритетом 2 и серьезностью 2, впоследствии пометив ее как дублирующуюся.

Когда исследователь уведомил компанию о том, что ошибка будет раскрыта 17 августа, Google сказал, что исправление разрабатывается с ориентировочным сроком развертывания 17 сентября.

Хотя Google обычно дает поставщикам 90 дней для устранения любых ошибок, обнаруженных исследователями и сообщенных до раскрытия информации, проблема, о которой сообщил Хусейн, не была устранена в течение 137 дней.

Однако после того, как исследователь обнародовал результаты 19 августа (через два дня после крайнего срока раскрытия информации), Google развернул «меры по снижению рисков, основанные на модификации обратного пути и механизмах предотвращения злоупотреблений» в течение семи часов после публикации сообщения в блоге Хусейна.

«[Через] семь часов после публикации этого сообщения проблема была устранена», - сказал Хусейн в обновлении сообщения в блоге, в котором раскрывается ошибка спуфинга электронной почты, затрагивающая как Gmail, так и G Suite». ***(Sergiu Gatlan. Google fixes Gmail bug allowing attackers to send spoofed emails // Bleeping Computer (https://www.bleepingcomputer.com/news/security/google-fixes-gmail-bug-allowing-attackers-to-send-spoofed-emails/). 20.08.2020).***

***

«X-Force Red, команда «белых хакеров» корпорации IBM, обнародовала детали серьёзной уязвимости в коммуникационных чипах производства Thales, открывающей для атак миллионы устройств Интернета Вещей (IoT). Она может использоваться для обхода проверок безопасности, которые предохраняют файлы и операционный код от неавторизованного доступа.

В сентябре эта уязвимость была обнаружена в модулях Cinterion EHS8, используемых, чтобы создавать защищённые каналы коммуникаций для промышленного IoT-оборудования. Поставленная в известность об этом открытии компания Thales впоследствии подтвердила, что данная проблема затрагивает и другие модули, относящиеся к тому же семейству, что и EHS8: BGS5, EHS5/6/8, PDS5/6/8, ELS61, ELS81 и PLS62.

Злонамеренное использование данной уязвимости может привести к краже интеллектуальной собственности, идентификационной информации, ключей шифрования. Преступники также смогут манипулировать показаниями датчиков (например, систем медицинского мониторинга) и даже отключать умные счётчики коммунальных сетей в масштабах целого города.

«Когда мы говорим о промышленных и критических инфраструктурных средах, таких как нефте- и газопроводы, такой тип уязвимости может привести к серьезным инцидентам для безопасности и окружающей среды, а также к дорогостоящим простоям», — отметил Фил Нерай (Phil Neray), вице-президент принадлежащей Microsoft компании CyberX, занимающейся безопасностью IoT.

Патч, закрывающий эту уязвимость, был подготовлен для клиентов уже в феврале, однако, учитывая огромные масштабы распространения чипов Cinterion, многие устройства все-ещё остаются неисправленными и уязвимыми для атак». ***(Миллионы IoT-устройств остались незащищенными из-за ошибки в чипах Cinterion // Компьютерное Обозрение (https://ko.com.ua/milliony_iot-ustrojstv_ostalis_nezashhishhennymi_iz-za_oshibki_v_chipah_cinterion_134218). 21.08.2020).***

***

«Эксперты Positive Technologies обнаружили уязвимость в системе управления корпоративными мобильными устройствами Citrix XenMobile. При переходе по специально сформированному адресу злоумышленник мог читать произвольные файлы, находящиеся за пределами корневой директории веб-сервера, в том числе файлы конфигурации и ключи шифрования конфиденциальных данных. Для эксплуатации уязвимости не требуется авторизация.

Уязвимость с идентификатором CVE-2020-8209 была выявлена в компоненте Citrix XenMobile Server. Она относится к классу Path Traversal (выход за пределы каталога) и связана с недостаточной проверкой входных данных.

Эксплуатация данной уязвимости позволяет получить информацию, которая может быть полезна для преодоления периметра, так как в конфигурационном файле зачастую хранится доменная учетная запись для подключения к LDAP. Удаленный злоумышленник может использовать полученные данные для аутентификации на других внешних ресурсах компании: в корпоративной почте, VPN, веб-приложениях. Кроме того, прочитав конфигурационный файл, атакующий может получить доступ к важным данным, например к паролю от базы данных (по умолчанию – от локальной PostgreSQL, в некоторых случаях – от удаленной SQL Server). Однако, учитывая, что база данных находится внутри корпоративного периметра и снаружи к ней не подключиться, этот вектор может быть использован разве что в сложных атаках, например при помощи сообщника внутри компании.

Уязвимости подвержены Citrix XenMobile с версии 10.8 по 10.12. Компания Citrix выпустила новую версию продукта, в которой данная ошибка исправлена, и рекомендует установить ее как можно скорее». ***(Уязвимость в Citrix XenMobile позволяет получить доступ к файлам конфигурации // Компьютерное Обозрение (https://ko.com.ua/uyazvimost_v_citrix_xenmobile_pozvolyaet_poluchit_dostup_k_fajlam_konfiguracii_134137). 17.08.2020).***

***

«Компания Eset сообщает о выявлении уязвимости KrØØk в Wi-Fi чипах еще нескольких производителей. Ранее она была зафиксирована в изделиях Broadcom и Cypress.

Используя KrØØk, злоумышленники могут перехватывать и расшифровывать конфиденциальные данные жертв. Это возможно за счет того, что данные беспроводной сети шифруются с помощью парного сеансового ключа WPA2,

состоящего из нулей, вместо надлежащего сеансового ключа. Для перехвата данных киберпреступникам не нужно знать даже пароль от Wi-Fi, а достаточно находиться в пределах сигнала Wi-Fi.

После обнаружения уязвимости специалисты Eset сообщили о ней поставщикам и опубликовали результаты исследования. Благодаря публикации материала многие производители узнали о проблеме, а некоторые из них даже обнаружили недостаток в своих продуктах и применили соответствующие исправления.

Специалисты Eset продолжили исследования и выявили подобные уязвимости в Wi-Fi чипах еще нескольких поставщиков, среди которых – Qualcomm. Обнаруженная уязвимость также приводила к нежелательному раскрытию информации путем передачи незашифрованных данных вместо зашифрованных фреймов, как и в ситуации с KrØØk. Однако в этом случае вместо шифрования с помощью нулевого сеансового ключа данные вообще не шифровались. В частности, специалисты Eset обнаружили уязвимость в D-Link DCH-G020 Smart Home Hub и беспроводном роутере Turris Omnia. При этом любые другие устройства, которые используют чипсеты Qualcomm без примененных исправлений, также будут уязвимы.

Стоит отметить, что в июле производитель Qualcomm выпустил исправления для соответствующего драйвера, который используется в продуктах с официальной поддержкой. Не все устройства с чипами Qualcomm используют этот драйвер, однако в некоторых случаях применяются драйверы Linux с открытым кодом, например, драйвер «ath9k».

Также уязвимость, связанная с отсутствием шифрования, была обнаружена в Wi-Fi чипах от MediaTek, в частности в роутерах ASUS RT-AC52U и наборе для разработки Microsoft Azure Sphere. Последний использует микроконтроллер MT3620 MediaTek и применяется в ряде IoT-приложений.

По информации MediaTek, исправления были выпущены в течение марта и апреля. Тогда как исправление для MT3620 было включено в версию операционной системы 20.0 Azure Sphere, выпущенную в июле.

Поскольку прошло более пяти месяцев с момента обнаружения уязвимости, а недостаток еще может оставаться неисправленным, компания Eset решила выпустить скрипт для проверки устройств на наличие KrØØk, в который вошло также тестирование новых версий уязвимости, описанных выше. Этот скрипт может быть использован исследователями или производителями для проверки отсутствия уязвимости и эффективного применения исправления.

В то же время пользователям рекомендуется применить необходимые обновления для точек доступа и Wi-Fi-роутеров, а также всех устройств с поддержкой Wi-Fi, так как наличие KrØØk предоставляет киберпреступникам дополнительные возможности для дальнейших атак». ***(Уязвимость KrØØk обнаружена также в Wi-Fi-чипах Qualcomm и MediaTek // Компьютерное Обозрение (https://ko.com.ua/uyazvimost_kr_k_obnaruzhena_takzhe_v_wi-fi-chipah_qualcomm_i_mediatek_134086). 11.08.2020).***

***

«На этой неделе инженеры компании Citrix выпустили ряд патчей для Citrix Endpoint Management, а точнее системы управления корпоративными мобильными устройствами XenMobile Server. Эти проблемы дают злоумышленнику возможность получить административные привилегии в уязвимых системах.

Серьезность обнаруженных проблем, которые получили идентификаторы CVE CVE-2020-8208, CVE-2020-8209, CVE-2020-8210, CVE-2020-8211 и CVE-2020-8212, различается в зависимости от используемой версии XenMobile. Так, уязвимости будут критическими для XenMobile версий от 10.12 до RP2, от 10.11 до RP4, от 10.10 до RP6 и всех версий до 10.9 RP5. В свою очередь, для XenMobile версий от 10.12 до RP3, от 10.11 до RP6, от 10.10 до RP6 и до 10.9 RP5 угроза будет низкой или средней.

Специалисты компании пишут, что все версии 10.9.x должны быть немедленно обновлены (желательно до новейшей 10.12 RP3), та как некоторые проблемы можно использовать удаленно и без аутентификации. На данный момент более 70% потенциально уязвимых клиентов, которые были предварительно уведомлены о проблемах, уже установили доступные исправления.

«Мы рекомендуем осуществить обновления немедленно. Хотя на данный момент известных эксплоитов [для этих проблем] нет, мы ожидаем, что злоумышленники очень скоро приступят к их использованию», — предупреждают в компании.

Хотя эксперты Citrix не раскрывают деталей найденных проблем, уязвимость CVE-2020-8209 обнаружил специалист Positive Technologies Андрей Медов. Он рассказал, что она относится к классу Path Traversal (выход за пределы каталога) и связана с недостаточной проверкой входных данных.

«Эксплуатация данной уязвимости позволяет получить информацию, которая может быть полезна при преодолении периметра, так как в конфигурационном файле зачастую хранится доменная учетная запись для подключения к LDAP, — рассказывает эксперт. — Удаленный злоумышленник может использовать полученные данные для аутентификации на других внешних ресурсах компании: в корпоративной почте, VPN, веб-приложениях. Кроме того, прочитав конфигурационный файл, атакующий может получить доступ к важным данным, например к паролю от базы данных (по умолчанию — от локальной PostgreSQL, в некоторых случаях — от удаленной SQL Server). Однако, учитывая, что база данных находится внутри корпоративного периметра и снаружи к ней не подключиться, этот вектор может быть использован разве что в сложных атаках, например при помощи сообщника внутри компании». ***(Мария Нефёдова. Citrix ожидает атак на свежие проблемы в XenMobile // Xakep (https://xakep.ru/2020/08/12/xenmobile-flaws/). 12.08.2020).***

***

«В июне текущего года исследователи из компании Check Point обнаружили ряд опасных уязвимостей, которые открывали для атак виртуального помощника Amazon Alexa и его пользователей.

Проблемы представляли собой CORS и XSS баги, а также проблемы в конфигурации, и они затрагивали некоторые поддомены Amazon. Эксплуатируя эти баги, злоумышленники могли получить доступ к личным данным (имена пользователей, телефонные номера, домашние адреса, голосовая история) и выполнять различные действия от имени жертв (к примеру, удалять и устанавливать навыки для Alexa).

«Для успешной эксплуатации [проблем] требовался всего один щелчок по ссылке, специально созданной злоумышленником», — пишут исследователи.

Для успешной атаки злоумышленнику действительно необходимо было создать вредоносную ссылку, которая направляла бы пользователя на amazon.com, и отправить ее жертве (каким-то образом вынудив пользователя кликнуть по ней). Исследователи предложили использовать для этих целей уязвимую track.amazon.com, — эта страница не связана с Alexa, а используется для отслеживания посылок с Amazon, и ранее на нее можно было внедрить вредоносный код.

После злоумышленник отправлял Ajax-запрос с полученными файлами cookie пользователя на amazon.com/app/secure/your-skills-page, что позволяло получить список навыков, установленных для этой учетной записи Alexa.

Ответ на такой запрос содержал и токен CSRF, который атакующий мог использовать для удаления одного навыка из списка. Затем злоумышленник мог таким же образом установить на устройство собственный вредоносный навык для Alexa. Подмена удаленного навыка собственным открывала перед преступником немало возможностей, в зависимости от навыков, установленных на устройстве пользователя. К примеру, можно было получить доступ к голосовой истории жертвы, а затем к именам пользователей, номерам телефонов, домашним адресам, банковским данным (Alexa не записывает учетные данные для входа в банкинг, однако фиксирует прочие взаимодействия).

«Умные колонки и виртуальные помощники кажутся настолько непримечательными, что, порой, мы упускаем из виду их роль в управлении умным домом, а также то, сколько личных данных они хранят. По этой причине, хакеры рассматривают подобные приложения, как точки входа в жизнь людей, благодаря которым они могут получить доступ к личным данным, подслушивать разговоры и совершать иные вредоносные действия без ведома пользователя, — говорит Одед Вануну (Oded Vanunu), глава отдела исследования уязвимостей Check Point Software Technologies. — Цель нашего исследования — освещение необходимости обеспечения безопасности таких устройств, как Alexa. К счастью, специалисты Amazon быстро исправили уязвимости в поддоменах Amazon/Alexa. Мы надеемся, что производители подобных устройств последуют примеру Amazon и проверят свои продукты на наличие уязвимостей, которые потенциально могут компрометировать конфиденциальность пользователей».

В настоящее время инженеры Amazon уже исправили все обнаруженные уязвимости. Также представители компании заявили, что им неизвестно о каких-либо случаях использования этих проблем или о раскрытии какой-либо информации о клиентах». ***(Мария Нефёдова. Из-за багов данные пользователей***

Amazon Alexa были доступны для посторонних // Хакер (https://xakep.ru/2020/08/17/alexa-subdomains/). 17.08.2020).

***

«Процесс с низким уровнем привилегий на уязвимой машине может позволить сбор данных и DoS.

Программное обеспечение IBM для управления данными следующего поколения страдает от уязвимости совместно используемой памяти, которая, по словам исследователей, может привести к другим угрозам, что продемонстрировал новый экспериментальный эксплойт для этой ошибки.

IBM Db2 - это семейство гибридных продуктов для управления данными, содержащих искусственный интеллект, которые можно использовать для анализа и управления как структурированными, так и неструктурированными данными на предприятиях.

По словам исследователей из Trustwave, недавно обнаруженная ошибка (CVE-2020-4414) возникает из-за того, что разработчики платформы забыли установить явную защиту памяти для общей памяти, используемой средством трассировки Db2. В случае эксплуатации это может привести к отказу в обслуживании (DoS) или раскрытию информации.

Средство трассировки - это функция, которая позволяет пользователям изолировать определенные точки данных путем мониторинга выбранных параметров. Это дает пользователям то, что по сути является журналом информации о потоке управления (функции и связанные значения параметров), который может быть полезен при разрезании, нарезании кубиками и разделении данных для анализа. Таким образом, данные, подверженные риску из-за эксплойта, могут быть буквально любыми, созданными в целевой организации. Например, для поставщика медицинских услуг киберпреступники могут скрыться с информацией о пациентах, защищенной HIPAA; тем временем финансовая компания может подвергнуться риску взлома данных кредитной карты.

Что касается DoS, Карл Сиглер, старший менеджер по исследованиям в области безопасности SpiderLabs в Trustwave, сказал Threatpost, что «базы данных часто развертываются как критически важная система. Злоумышленник, закрепившийся в системе, может последовательно вывести из строя базу данных и прервать работу любой системы, которая зависит от нее и ее данных».

Суть проблемы в том, что он позволяет локальное повышение привилегий и сбой устройства. Отсутствие явной защиты памяти «позволяет любым локальным пользователям читать и писать доступ к этой области памяти», - заявили исследователи Trustwave в своем отчете об уязвимостях PoC, опубликованном в четверг. «В свою очередь, это позволяет им получить доступ к критически важным данным, а также возможность изменять работу подсистемы трассировки, что приводит к отказу в обслуживании в базе данных».

Они добавили: «Излишне говорить, что и то, и другое не должно быть возможным для обычных пользователей».

Хотя технически злоумышленник должен быть локальным, можно удаленно выполнить такой процесс с низким уровнем привилегий (например, вредоносное

ПО) на уязвимой машине, чтобы запустить эксплойт: «Процессы с низким уровнем привилегий, выполняемые на том же компьютере, что и база данных Db2, может изменять следы Db2 и захватывать конфиденциальные данные - и использовать их позже для последующих атак», - пояснили исследователи.

PoC запущен

Чтобы воспользоваться ошибкой, злоумышленники могут отправить специально созданный запрос в средство трассировки.

PoC Trustwave начинается с запуска Process Explorer или другого подобного инструмента в Windows для проверки открытых дескрипторов основного процесса Db2. Затем исследователи создали простое консольное приложение, которое пытается открыть заданный раздел памяти по имени. После этого злоумышленник может включить трассировку Db2, что откроет дверь для атаки.

«И теперь мы можем видеть, что было записано в эти разделы памяти», согласно анализу Trustwave. «В конце концов, это означает, что непривилегированный локальный пользователь может злоупотребить этим, чтобы вызвать условие отказа в обслуживании, просто записав неверные данные в этот раздел памяти ... нет абсолютно никаких разрешений, назначенных общей памяти, чтобы любой мог читать из и напиши ему. "

Мартин Рахманов, менеджер по исследованиям безопасности SpiderLabs в Trustwave, подробно остановился на PoC для Threatpost. «Я показываю Process Explorer только для того, чтобы показать, что разделяемая память не защищена. Совершать атаку не требуется», - сказал он. «Консольное приложение просто читает общую память и, таким образом, может получить доступ к информации трассировки Db2. Его можно изменить (приложение), чтобы изменить трассировку Db2. Наконец, злоумышленнику нужен доступ с низким уровнем привилегий к компьютеру, на котором работает сервер Db2».

Он добавил: «Это не то же самое, что иметь контроль над машиной. Таким образом, любой, кто может подключиться к компьютеру, на котором запущен сервер Db2, может прочитать / изменить трассировку Db2, что нехорошо: напротив, средство трассировки требует особых привилегий внутри Db2, но уязвимость позволяет обойти это».

Эта уязвимость совместно используемой памяти очень похожа на уязвимость, обнаруженную в мартовском клиенте Cisco WebEx Meetings для Windows (CVE-2020-3347), где любой пользователь может читать память, выделенную для данных трассировки, пояснили исследователи Trustwave. В этом случае любой злонамеренный локальный пользователь или вредоносный процесс, запущенный на ПК, на котором установлен WebEx, может отслеживать файл с отображением памяти на предмет токена входа. После обнаружения токен, как и любые утекшие учетные данные, можно куда-то передать, чтобы его можно было использовать для входа в соответствующую учетную запись WebEx, загрузки записей, просмотра / редактирования собраний и т. Д.

Все уровни пакетов исправлений выпусков IBM Db2 V9.7, V10.1, V10.5, V11.1 и V11.5 на всех платформах подвержены этой последней уязвимости совместно используемой памяти, и пользователям следует выполнить обновление до последней версии, чтобы "решить проблему", - заявила компания.

«Эта атака могла быть широко распространенной, так как были затронуты все экземпляры Db2 последней версии (11.5) в Windows», - отмечают исследователи Trustwave». ***(Tara Seals. IBM AI-Powered Data Management Software Subject to Simple Exploit // Threatpost (https://threatpost.com/ibm-ai-powered-data-management-software-subject-exploit/158497/). 20.08.2020).***

***

«Был выпущен патч для исправления недостатка в широко используемом модуле, и исследователи призывают производителей Интернета вещей как можно скорее обновить свои устройства.

Исследователи призывают производителей подключенных устройств убедиться, что они применили исправления, устраняющие недостаток в модуле, используемом миллионами устройств Интернета вещей (IoT). Исследователи предположили, что в случае использования уязвимости злоумышленники могут вывести из строя городское электричество или даже вызвать передозировку у медицинского пациента.

Уязвимость существует в широко используемом модуле Cinterion, небольшом электронном устройстве, встроенном в устройства IoT, которое подключается к беспроводным сетям и отправляет и принимает данные. Модуль производится французской компанией Thales, которая проектирует и производит электрические системы для аэрокосмических рынков.

Исследователи обнаружили недостаток в модуле Cinterion EHS8, однако дальнейшее тестирование показало, что были затронуты пять других моделей из той же линейки продуктов (BGS5, EHS5 / 6/8, PDS5 / 6/8, ELS61, ELS81, PLS62). Уязвимость может быть использована для кражи конфиденциальной информации, получения контроля над устройствами, получения доступа к сетям управления и многого другого.

«[Модули] хранят и запускают код Java, часто содержащий конфиденциальную информацию, такую как пароли, ключи шифрования и сертификаты», - сказал Адам Лори из IBM X-Force Threat Intelligence в своем сообщении в среду. «Используя информацию, украденную из модулей, злоумышленники могут потенциально управлять устройством или получить доступ к центральной сети управления для проведения широкомасштабных атак - в некоторых случаях даже удаленно через 3G».

Уязвимость (CVE-2020-15858) была впервые обнаружена в сентябре прошлого года, и Thales выпустила исправление в начале 2020 года, но, хотя исправления доступны, исследователи предупреждают, что многим производителям критически важной инфраструктуры потребуется некоторое время, чтобы применить их к своим устройствам. Исследователи обнаружили уязвимость в среду после работы с Thales, «чтобы пользователи знали об исправлении и предпринимали шаги для защиты своих систем».

Исследователи нашли способ обойти проверки безопасности, которые скрывают файлы или рабочий код от неавторизованных пользователей.

Дэн Кроули, директор по исследованиям IBM X-Force Red, сообщил Threatpost, что ошибка существует в способе обработки AT-команд модулем. Это

связано со строкой кода Java, которая подсчитывает количество символов в подстроке пути.

Эта строка кода проверяет, является ли четвертый символ подстроки пути точкой. Обычно любая попытка доступа к скрытым файлам с префиксом точки будет отклонена (пример: a: /. Hidden_file) - однако замена косой черты на двойную косую черту (пример: a: //.hidden_file) приведет к сбою условия. Таким образом, злоумышленник может использовать имя файла с префиксом точки, чтобы обойти условие проверки безопасности.

«Реальный злоумышленник может пойти на дозвон, чтобы попытаться идентифицировать модемы в сотовой сети, пытаясь выдать AT-команду, которая использует уязвимость», - объяснил Кроули. «Некоторые из них будут уязвимыми модулями, и злоумышленник получит набор телефонных номеров и соответствующий код, полученный с устройства по этому номеру. Вставляя бэкдоры в код и записывая их обратно, злоумышленник будет контролировать различные устройства IoT по всему миру.”

В случае использования злоумышленники потенциально могут получить доступ к огромному количеству конфиденциальных данных, хранящихся в модулях. Это может включать интеллектуальную собственность (IP), учетные данные, пароли, ключи шифрования и многое другое. И из-за огромного количества подключенных устройств, которые питаются от этого модуля - от медицинских устройств до подключенных коммунальных служб - исследователи предупреждают, что потенциальное воздействие недостатка может быть ужасным, если его не исправить.

Например, недостаток может быть использован в медицинских устройствах, которые используют модуль для манипулирования показаниями с устройств мониторинга, для сокрытия показателей жизнедеятельности или создания ложной паники.

«В устройстве, которое обеспечивает лечение на основе входных данных, таком как инсулиновая помпа, киберпреступники могут вводить передозировку или занижать дозировку пациентов», - заявили исследователи.

А в служебных помещениях его можно использовать для взлома интеллектуальных счетчиков для получения ложных показаний, которые увеличивают или уменьшают ежемесячный счет.

«Имея доступ к большой группе этих устройств через сеть управления, злоумышленник может также отключить счетчики для всего города, вызывая широкомасштабные отключения электроэнергии, требующие индивидуальных посещений для ремонта, или, что еще хуже, повреждение самой сети, - сказали исследователи.

Уязвимости и проблемы безопасности продолжают преследовать подключенные устройства - даже несмотря на то, что количество подключенных к Интернету устройств, используемых во всем мире, по прогнозам, вырастет до 55,9 миллиарда к 2025 году. Более половины всех устройств IoT уязвимы для атак средней или высокой степени серьезности, то есть исследователи предупредили ранее в этом году, что предприятия сидят на «бомбе замедленного действия IoT».

Исследователи безопасности X-Force со своей стороны заявили, что этот конкретный патч может администрироваться производителями Интернета вещей двумя способами - либо путем подключения USB для запуска обновления через программное обеспечение, либо путем администрирования обновления по беспроводной сети (OTA). Однако более жестко регулируемые устройства, в том числе подключенные медицинские устройства или промышленное оборудование, столкнутся с большими трудностями при применении патча, поскольку для этого может потребоваться повторная сертификация, что часто требует больших затрат времени, сказали они.

«Процесс исправления этой уязвимости полностью зависит от производителя устройства и его возможностей - например, наличие у устройства доступа к Интернету может усложнить работу с ним», - заявили они». ***(Lindsey O'Donnell. Researchers Warn of Flaw Affecting Millions of IoT Devices // Threatpost (https://threatpost.com/flaw-affecting-millions-iot-devices/158472/). 19.08.2020).***

***

«Федеральное бюро расследований США (ФБР) предупредило партнеров из частного сектора о повышенных рисках безопасности, влияющих на инфраструктуру компьютерной сети из-за устройств, все еще работающих под управлением Windows 7 после того, как операционная система достигла конца срока службы 14 января.

«ФБР обнаружило киберпреступников, нацеленных на инфраструктуру компьютерной сети после того, как операционная система достигнет статуса истечения срока службы», - говорится в опубликованном вчера уведомлении частной отрасли (PIN) ФБР .

«Продолжение использования Windows 7 на предприятии может предоставить киберпреступникам доступ к компьютерным системам.

«Со временем Windows 7 становится более уязвимой для эксплуатации из-за отсутствия обновлений безопасности и обнаруженных новых уязвимостей».

После завершения поддержки в начале этого года Windows 7 больше не получает бесплатных обновлений программного обеспечения и обновлений безопасности или исправлений, если клиенты не получат подписку на программу расширенных обновлений безопасности (ESU), которая позволит им получать обновления безопасности в течение дополнительных трех лет.

Программа расширенных обновлений безопасности доступна для Windows 7 Professional, Windows 7 Enterprise и Windows 7 Ultimate только через программы корпоративного лицензирования и не включает и не предоставляет клиентам новые функции, запрошенные пользователем обновления, не связанные с безопасностью, или запросы на изменение конструкции. .

Несмотря на то, что Microsoft заявляет, что бесплатное обновление до Windows 10 с Windows 7 было доступно только до 29 июля 2016 г., бесплатные обновления до Windows 10 все еще актуальны, если вы выполните эту пошаговую процедуру обновления до Windows 10, которая включает запуск Media Creation Tool и выбрав опцию «Обновить этот компьютер сейчас» на компьютерах с Windows 7.

Организации посоветовали обновить устройства с Windows 7

ФБР предупреждает, что активно поддерживаемая управляемая система - лучший способ смягчить недавно обнаруженные недостатки безопасности, поскольку она автоматически получает обновления безопасности, как только они доставляются поставщиком.

Несмотря на то, что процесс миграции всего парка устройств Windows 7 на поддерживаемую ОС сопряжен со своими проблемами, включая затраты на программное обеспечение и оборудование, эти препятствия незначительны по сравнению с рисками безопасности, с которыми сталкиваются организации, если они не обновят такие системы.

«В сфере здравоохранения наблюдается рост количества компромиссов, когда операционная система достигла статуса истекшего срока службы», - сообщает ФБР. «После окончания срока службы Windows XP 28 апреля 2014 года в отрасли здравоохранения в следующем году значительно увеличилось количество открытых записей»…

Недостатки Windows 7, на которые были направлены предыдущие атаки

Служба внутренней разведки и безопасности США также напоминает о прошлых уязвимостях в Windows 7, которые были исправлены Microsoft и позже использовались злоумышленниками в атаках на уязвимые устройства, подключенные к Интернету.

Среди них ФБР упоминает критическую уязвимость удаленного выполнения кода (RCE) BlueKeep, влияющую на платформу Windows Remote Desktop Services (RDS), которая была исправлена Microsoft в мае 2019 года, а также растущий интерес со стороны злоумышленников к компрометации устройств, на которых не установлены исправления. Недостатки протокола удаленного рабочего стола (RDP).

Агентство также сообщает о программе-вымогателе WannaCry, которая использовала эксплойт ETERNALBLUE NSA и эксплойт DOUBLEPULSAR для ядра Windows Ring-0 для распространения и заражения более 57000 устройств по всему миру в 2017 году.

Microsoft исправила уязвимость, использованную ETERNALBLUE в марте 2017 года, но это не остановило атаки, поскольку пользователи Windows 7 не смогли вовремя обновить свои системы, и, как следствие, «98 процентов систем, зараженных WannaCry, использовали операционные системы на базе Windows 7», по данным ФБР.

«С меньшим количеством клиентов, которые могут поддерживать исправленную систему Windows 7 после ее окончания, киберпреступники будут продолжать рассматривать Windows 7 как легкую мишень», - заключает ФБР». ***(Sergiu Gatlan. FBI: Networks exposed to attacks due to Windows 7 end of life // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-networks-exposed-to-attacks-due-to-windows-7-end-of-life/). 04.08.2020).***

***

«Команда специалистов из IBM обнаружила уязвимость в компоненте, который используется в миллионах девайсов, подключенных к интернету

вещей (IoT). Речь идет о небольшой плате, которая обеспечивает подключение девайса к IoT. Этот модуль хранит и запускает написанный на Java код, и оперирует такими данными, как пароли или ключи дешифрования.

Модули, в которых обнаружили уязвимость — Thales Cinterion EHS8 M2M, EHS8, включая BGS5, EHS5/6/8, PDS5/6/8, ELS61, ELS81 и PLS62. Если злоумышленник сможет получить доступ к информации, хранящейся в модуле, он сможет контролировать все устройство и даже получить доступ к сети, к которой оно подключено.

Опасность представляет также то, что указанные модули используются в некоторых медицинских устройствах. Взломав их, киберпреступник сможет манипулировать данными, поступающими от датчиков и менять их, транслируя фейковые жизненные показатели.» ***(В IBM обнаружили уязвимость в компоненте для IoT девайсов // SecureNews (https://securenews.ru/ibm-discovered-a-vulnerability-in-a-component-for-iot-devices/). 20.08.2020).***

***

«Метод широкого охвата помог вовлечь начинающих специалистов в исследования и улучшить их навыки.

Исследователи безопасности с любым уровнем знаний добиваются большего успеха благодаря усовершенствованному автоматизированному анализу, который лучше распределяет человеческие ресурсы во время поиска уязвимостей, считают военные исследователи США из Агентства национальной безопасности, Киберкомандования, ВМФ, ВВС и армии.

«В хакерском сообществе существует когнитивная предвзятость, чтобы выбрать часть программного обеспечения и вложить значительные человеческие ресурсы в поиск уязвимостей в этом программном обеспечении без каких-либо предварительных признаков успеха», — отмечают исследователи.

Такой подход называется «поиск в глубину» (Depth-first search, DFS), и, по словам экспертов, ложится большим бременем на опытных исследователей, в то время как новички теряются в беспорядке.

С целью протестировать новый автоматизированный метод «поиска в ширину» (Breadth-first search, BFS) исследователи набрали 12 добровольцев из Кибернетического командования США и разделили их на две команды по шесть человек. Одна команда протестировала метод «поиска в ширину», в котором добровольцы используют метод автоматического тестирования программного обеспечения, называемый фаззингом, а другая — метод «поиска в ширину», когда все группы работали над одним и тем же программным обеспечением одновременно.

Исследователи обнаружили, что в подавляющем большинстве случаев автоматизированный метод «поиска в ширину» позволяет добровольцам находить больше уязвимостей в программном обеспечении, чем при использовании «поиска в глубину». Метод широкого охвата также помог начинающим хакерам участвовать в исследованиях и улучшать свои навыки, поскольку команды могли сочетать уровни знаний с задачами на протяжении всего процесса обнаружения уязвимостей.

«Метод поиска в ширину побуждает хакеров-новичков сдаваться, когда достижение конкретной цели требует значительных временных затрат. Ученики записывают любую относящуюся к делу информацию о цели, прежде чем перемещать ее в отдельную очередь. Это дает возможность более опытным специалистам ознакомиться с материалами, прежде чем применять свои способности», — пояснили исследователи.

Исследователи обнаружили, что не только поиск новых ошибок, но и подход, основанный на расширении, позволил хакерам-добровольцам получить больше удовлетворения от своей работы.

Поиск в глубину — один из методов обхода графа. Стратегия поиска в глубину состоит в том, чтобы идти «вглубь» графа, насколько это возможно, тогда как в результате поиска в ширину находится путь кратчайшей длины в невзвешенном графе, то есть путь, содержащий наименьшее число ребер». ***(Военные США нашли более продуктивный способ обнаружения уязвимостей // SecurityLab.ru (https://www.securitylab.ru/news/511443.php). 25.08.2020).***

***

«ИТ-компания «Инфосистемы Джет» предупреждает об опасной уязвимости (7,5 баллов из 10 по шкале CVSS v2) в системах мониторинга виртуальной инфраструктуры LPAR2RRD и STOR2RRD Virtual Appliance от производителя Xorux. Проблема (CVE-2020-24032) затрагивает версии LPAR2RRD и STOR2RRD Virtual Appliance с 2.01 по 2.70 и заключается в недостаточной фильтрации данных в параметрах POST-запроса при установке временной зоны. Для эксплуатации уязвимости необходим доступ к функции set timezone через веб-интерфейс продукта. В результате злоумышленники могут получить возможность по внедрению и выполнению команд на сервере решения.

«Уязвимое приложение выполняет внедренные злоумышленником команды в принимающей их операционной системе и позволяет в отдельных случаях полностью скомпрометировать систему, а также обойти средства защиты, применяемые в организации для предотвращения несанкционированного доступа во внутреннюю сеть. CVE-2020-24032 может стать отличным плацдармом для дальнейшего развития атаки на внутреннюю сеть.

До устранения уязвимости производителем специалисты «Инфосистемы Джет» рекомендуют ограничить доступ к сценарию /cgi-bin/tz.pl наложенными средствами либо временно ограничить доступ к веб-панели на сетевом уровне.

LPAR2RRD и STOR2RRD Virtual Appliance — программное обеспечение с открытым исходным кодом для мониторинга серверной инфраструктуры и систем хранения данных от чешской компании Xorux. Согласно информации на сайте производителя, данными решениями пользуются финансовые компании, государственные организации, ИТ- и телеком-компании, предприятия сферы энергетики, а также организации в области здравоохранения». ***(Уязвимость в системах мониторинга Xorux может привести ко взлому корпоративной сети // SecurityLab.ru (https://www.securitylab.ru/news/511402.php). 24.08.2020).***

***

«Более 70% уязвимостей в АСУ ТП, обнаруженных в первой половине 2020 года, можно использовать удаленно. Исследовательская группа из компании Claroty представила отчет, который включает оценку 365 уязвимостей в АСУ ТП, опубликованных в Национальной базе данных по уязвимостям (NVD), и 139 сообщений, выпущенных командой экстренного реагирования на киберугрозы промышленных систем управления (ICS-CERT), которые затрагивали 53 поставщика АСУ ТП.

По сравнению с первым полугодием 2019 года количество уязвимостей в АСУ ТП увеличилось на 10,3%, в то время как количество сообщений ICS-CERT увеличилось на 32,4%. Более 75% уязвимостей были оценены как опасные (53,15%) или критические (22,47%) по шкале CVSS.

Как отметили эксперты, более 70% уязвимостей, опубликованных NVD, можно эксплуатировать удаленно. Кроме того, наиболее частым потенциальным воздействием было удаленное выполнение кода, возможное путем эксплуатации 49% уязвимостей, за которым следует чтение данных приложений (41%), вызов отказа в обслуживании (39%) и обход механизмов защиты (37%).

Энергетическая сфера, критическое производство и инфраструктуры водоснабжения в наибольшей степени пострадали от уязвимостей, обнаруженных в первом полугодии 2020 года. Из 385 уникальных уязвимостей, занесенных в базу данных Common Vulnerabilities and Exposures, в энергетическом секторе было обнаружено 236 проблем, в критически важных производственных предприятиях — 197, а в системах водоснабжения — 171». ***(Более 70% уязвимостей в АСУ ТП могут быть проэксплуатированы удаленно // SecurityLab.ru (https://www.securitylab.ru/news/511354.php). 20.08.2020).***

***

«Исследователь ответственно раскрыл в Slack несколько уязвимостей, которые позволили злоумышленнику захватить компьютер пользователя, и получили лишь жалкие 1750 долларов.

Используя эти уязвимости, злоумышленник может просто загрузить файл и поделиться с другим пользователем или каналом Slack, чтобы запустить эксплойт в приложении Slack жертвы.

В своем подробном описании, предоставленном Slack в частном порядке в январе 2020 года, инженер по безопасности Оскарс Вегерис из Evolution Gaming поделился подробными сведениями об уязвимости.

«С любым перенаправлением внутри приложения - логическим / открытым перенаправлением, HTML или javascript-инъекцией можно выполнить произвольный код в настольных приложениях Slack. Этот отчет демонстрирует специально созданный эксплойт, состоящий из HTML-инъекции, обхода контроля безопасности и полезной нагрузки RCE Javascript. Этот эксплойт был протестирован как работающий на последних версиях Slack для настольных компьютеров (4.2, 4.3.2) (Mac / Windows / Linux) », - сказал Вегерис.

Пятисекундная видеодемонстрация Vegeris, предоставленная с описанием HackerOne, показала, как он использовал файл JSON для запуска собственного приложения-калькулятора через настольное приложение Slack…

Множественные критические уязвимости

Отчет HackerOne, опубликованный компанией на этой неделе, показывает, как инженер перечисляет несколько способов использования приложений Slack.

Конечным результатом эксплойта будет выполнение произвольного кода на стороне клиента, то есть на компьютере пользователя, а не на сервере Slack.

Злоумышленник может осуществить внедрение HTML, выполнение произвольного кода, а также выполнение межсайтовых сценариев (XSS) из-за внутренней слабости кода files.slack.com .

Всего один эксплойт HTML / JavaScript Proof-of-Concept (PoC), опубликованный Vegeris, показывает, насколько легко запустить собственное приложение-калькулятор или что-то еще, что они захотят, загрузив полезную нагрузку в Slack.

Если URL-адрес этого HTML-файла будет вставлен в тег области представления сообщения Slack JSON, то на компьютере пользователя будет активирован "RCE одним щелчком".

«URL-ссылка в теге области будет содержать этот HTML / JS-эксплойт для приложений Slack Desktop, который выполняет любую команду, предоставленную злоумышленником», - заявил инженер.

В еще одном комментарии Вегерис сказал: «Ранее сообщалось, что кейлоггинг также может быть применим», ссылаясь на отчет об ошибке 2019 года, поданный Мэттом Ланглуа.

Это награда?

Тот факт, что Vegeris отказался от вознаграждения за ошибку всего в 1750 долларов после того, как потратил много времени на ответственное раскрытие информации, не устраивал информационную безопасность. сообщество.

По общему мнению в Twitter, компания Slack, создающая приложение для обмена сообщениями стоимостью 20 миллиардов долларов, используемое крупными корпорациями, столкнулась бы с серьезными последствиями, если бы эксплойт такого рода был продан на незаконных рынках темной сети (что принесло бы инженеру намного больше, чем 1750 долларов).

Mashable сообщил о таких случаях, когда пользователи набросились на Slack, например:

Дэниел Катберт, хакер и соавтор стандарта OWASP ASVS, сказал в ветке Twitter : «Slack, который миллионы и миллионы используют для критически важных обсуждений проектов, DevOps, безопасности, слияний и поглощений, черт возьми, список бесконечен. недостатки, обнаруженные этим исследователем, приводят к выполнению произвольных команд на компьютере пользователя. TL; DR - вау ».

Катберт умолял Slack «правильно платить» за подобные сообщения, поскольку такие эксплойты будут продаваться намного дороже на черных рынках.

«За все эти усилия они получили 1750 долларов. Семнадцатьсот пятьдесят баксов. @SlackHQ: во-первых, недостатки представляют собой довольно серьезную проблему, я имею в виду, что проверка сложна, но давай, потом плати должным образом, пожалуйста. Потому что это будет стоить намного больше. на exploit.in "

В рекламном сообщении блога, выпущенном Slack два месяца назад, в котором отмечалось его «песочница приложения», вместо того, чтобы раскрывать подробности уязвимости, которые привели к его разработке, компания также забыла указать Vegeris (теперь это исправлено).

Именно тогда Вегерис потребовал публичного раскрытия информации на HackerOne на этой неделе, что вызвало искренние извинения от Slack.

«Меня зовут Ларкин Райдер, и в настоящее время я исполняю обязанности начальника службы безопасности здесь, в Slack. @Brandenjordan сообщил мне об этой оплошности, и я пишу, чтобы принести свои искренние извинения за любые недосмотры при оценке вашей работы. Мы очень признательны время и усилия, которые вы вложили в повышение безопасности Slack », - заявил Райдер в своем отчете.

"Хотя группа безопасности не была автором этого сообщения в блоге, и автор не видит вашей работы в H1, мы должны предпринять дополнительные шаги, чтобы гарантировать признание всех, кто внес вклад в усилия по улучшению в этой области. Я буду исследовать, внося соответствующие обновления к нашему сообщению в блоге ... Опять же, я очень сожалею о любой ошибке с нашей стороны, - продолжил Райдер, поблагодарив инженера.

Запатентованная платформа бизнес-коммуникации Slack хвастается наличием более 10 000 000 активных пользователей в день и является узнаваемым брендом среди многих рабочих мест.

Хотя Slack, возможно, устранили уязвимости чуть более чем за пять недель после отчета, подобные случаи подчеркивают потенциальный ущерб, который может возникнуть из-за приложений для обмена сообщениями, поскольку они продолжают расширять свой список функций (например, загрузка файлов) и количество клиентов, если появится слабость безопасности». ***(Ax Sharma. Slack pays stingy $1,750 reward for a desktop hijack vulnerability // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/slack-pays-stingy-1-750-reward-for-a-desktop-hijack-vulnerability/). 30.08.2020).***

***

«Исследователи обнаружили больше уязвимостей в решении Microsoft для безопасности Интернета вещей.

Подробности, связанные с парой ошибок удаленного выполнения кода в платформе безопасности Microsoft IoT под названием Azure Sphere, были опубликованы в понедельник. Также были обнародованы особенности, связанные с двумя дополнительными недостатками повышения привилегий, влияющими на ту же платформу облачной безопасности.

Публичное раскрытие всех четырех ошибок в сочетании с шестью уязвимостями, обнаруженными в июле, также повлияло на Microsoft Azure Sphere. Исследователи кибербезопасности в Cisco Talos обнаружили каждую из ошибок и опубликовали технические подробности уязвимостей только после того, как Microsoft выпустила исправления.

«Cisco Talos работала с Microsoft, чтобы гарантировать, что эти проблемы решены, и что обновление доступно для затронутых клиентов. Однако Microsoft

отказалась выпускать какие-либо CVE», - говорится в аналитическом отчете, опубликованном в понедельник.

Azure Sphere, дебютировавшая на конференции RSA Conference 2018, представляет собой решение безопасности IoT от Redmond, предназначенное для защиты устройств микроконтроллеров (MCU), которые обычно встречаются в сетях IoT. Платформа использует MCU со встроенной технологией безопасности, использующей аутентификацию на основе сертификатов для защиты от угроз.

Первая из двух ошибок выполнения кода, раскрытых в понедельник, описывается как «обычная уязвимость выполнения неподписанного кода личности READ_IMPLIES_EXEC». Версия ошибки TDLR, затрагивающая Azure Sphere 20.06, заключается в том, что специально созданный шелл-код, введенный в платформу, может привести к тому, что куча процесса (данные, хранящиеся в памяти) станут исполняемыми. Например, согласно Cisco Talos, «злоумышленник может выполнить шелл-код, который устанавливает личность READ_IMPLIES_EXEC, чтобы активировать эту уязвимость».

Насколько серьезна эта уязвимость и другая ошибка удаленного выполнения кода (RCE)?

«Уязвимости удаленного выполнения кода могут привести к полной компрометации системы. К ним нужно относиться очень серьезно и по возможности исправлять. В случае, если серьезная проблема не может быть исправлена, потребуется многоуровневая стратегия смягчения последствий », - написал Крейг Уильямс, директор Talos Outreach в Cisco, в интервью по электронной почте.

Некоторое беспокойство снижает тот факт, что обе ошибки RCE необходимо использовать локально и не могут быть вызваны за пределами доверенной среды Azure Sphere.

«В нашем сценарии атаки мы предполагаем, что злоумышленник уже закрепился на устройстве и использует эти уязвимости для выполнения удаленного неподписанного кода, что, согласно модели безопасности Microsoft, не должно быть возможным», - сказал Уильямс.

Вторая уязвимость выполнения кода, описанная исследователями, затрагивает Microsoft Azure Sphere 20.07 и основана на предположении, что локальный злоумышленник может внедрить скомпрометированное приложение в экосистему IoT.

«Специально созданный шелл-код может вызвать запись в незаписываемую память процесса. Злоумышленник может выполнить шелл-код, который изменяет программу во время выполнения через / proc / thread-self / mem, чтобы вызвать эту уязвимость», - говорится в описании Cisco Talos.

Уязвимость, по мнению исследователей, может быть использована приложением, которое скрывается в Azure Sphere и выполняет процесс в специальной ОС Microsoft на базе Linux, которая является частью Azure Sphere. «Проблема связана с уже взломанным приложением», - пишут исследователи. Псевдокод в этом сценарии будет реализован с помощью гаджетов, ориентированных на возврат (ROP).

Псевдокод - это способ написания программного кода на простом английском языке, а не реальный язык программирования. Гаджеты ROP - это отдельные последовательности инструкций, которые можно объединить в цепочку для атаки.

«[Эта] последовательность команд перезаписывает функцию, на которую указывает func, произвольным шелл-кодом и может быть использована злоумышленником для запуска неподписанного кода после компрометации приложения», - заявили исследователи.

Исследователи Cisco Talos также выявили две уязвимости, связанные с повышением привилегий, обе из которых имеют высокий уровень серьезности и влияют на Microsoft Azure Sphere 20.06. Обе ошибки также исправлены.

«В функциональных возможностях управления доступом существует уязвимость повышения привилегий», - пишут исследователи. «Набор специально созданных системных вызовов ptrace можно использовать для получения расширенных возможностей. Злоумышленник может написать шелл-код, чтобы активировать эту уязвимость».

Ptrace - это жаргон, который описывает один системный вызов, а системный вызов - это действие, которое компьютерная программа выполняет при запросе службы из ядра операционной системы компьютера (ядра).

«Злоумышленник может использовать API ptrace для выполнения в другом процессе Azure Sphere и использовать свои возможности Azure Sphere для доступа к совершенно новому набору запросов IOCTL (управление вводом / выводом)», - пишет Cisco Talos.

Вторая привилегии ошибка эксплуатирует недостаток в устройствах ИТНЫ и их уникальный идентификатор (UID) числах.

«Уязвимость повышения привилегий существует в функциональности uid_map Microsoft Azure Sphere 20.06. Специально созданный файл uid_map может привести к тому, что нескольким приложениям будет назначен один и тот же UID, что расширит поверхность атаки. Злоумышленник может изменить файл uid_map, чтобы активировать эту уязвимость», - говорится в описании.

За каждую из обнаруженных в понедельник ошибок приписывают Клаудио Боззато, Дэйва МакДэниела и «Лилит> _>» из Cisco Talos. Microsoft сообщила об ошибках своим клиентам 10 августа, а публичное раскрытие информации было в понедельник». ***(Tom Spring. Four More Bugs Patched in Microsoft's Azure Sphere IoT Platform // Threatpost (https://threatpost.com/four-more-bugs-patched-in-microsofts-azure-sphere-iot-platform/158643/). 25.08.2020).***

***

«Компания «Elcore Украина», официальный дистрибьютор Trend Micro, сообщила о том, что решение вендора XDR официально выпущено в регионе AMEA, куда входит и наш рынок.

Отмечается, что Trend Micro XDR — первое решение в отрасли, которое предлагает клиентам комплексную систему обнаружения угроз, выходящую за рамки стандартных возможностей EDR (системы обнаружения и реагирования на угрозы на конечных устройствах). XDR собирает и анализирует данные о потенциальных угрозах из электронной почты, с конечных точек, серверов, из «облачной» и сетевой инфраструктуры, что позволяет специалистам оперативных центров безопасности (SOC) выявлять, изучать и реагировать на возникающие угрозы более эффективно.

Аналитики SOC в наше время сталкиваются с комплексными угрозами, которые способны обойти даже наиболее передовые системы кибербезопасности. Также проблем добавляют колоссальные объёмы оповещений о потенциальных атаках, которые они вынуждены ежедневно изучать. Низкая удовлетворённость работой и нехватка специалистов в сфере кибербезопасности — типичные проблемы для SOC во всем регионе AMEA.

Платформа Trend Micro XDR разрабатывалась специально для решения этих проблем, и по сравнению с другими решениями на рынке, по уверениям производителя, она обладает тремя главными преимуществами:

— Снижение «событийной усталости»: XDR автоматически выявляет зависимости и анализирует данные из нескольких эшелонов защиты, чтобы показать ИТ-специалистам максимально полную картину. Благодаря XDR аналитикам SOC первого уровня больше не нужно просматривать огромные объёмы оповещений и журналов событий, чтобы обнаружить потенциальную атаку — XDR делает это самостоятельно и в результате генерирует всего несколько оповещений с высокой степенью достоверности вместо тысяч.

— Мощная рабочая среда, обеспечивающая контекст и большую видимость оповещений: панель управления XDR позволяет визуализировать атаки, чтобы аналитики SOC могли видеть их текущую стадию, понимать векторы атак, их продолжительность, а также распространение в инфраструктуре компании и степень влияния на неё. XDR также предлагает варианты ответных действий с учётом текущей ситуации, поэтому аналитики SOC могут быстрее реагировать на атаки.

— Расширение возможностей SIEM и простота интеграции: Trend Micro XDR помогает расширить и дополнить процессы SIEM (security information and event management — «управление информацией о безопасности / событиями безопасности») для специалистов SOC. Это происходит за счёт централизации нормализованных данных и возможности реагирования на атаки, что позволяет повысить продуктивность и эффективность команд SOC. В XDR уже есть встроенный SIEM-плагин для одной из популярных SIEM-систем, который

позволяет выводить оповещения о потенциальных атаках на панели управления SIEM. А для комфортной интеграции в другие системы, используемые клиентами, предусмотрен общедоступный программный интерфейс.

В рамках Trend Micro XDR также доступен сервис MDR, что позволяет ещё больше снизить нагрузку на внутренние команды SOC. В этом случае комплексным анализом угроз и их выявлением, подготовкой планов реагирования и рекомендаций по восстановлению инфраструктуры после атак на постоянной основе занимаются специалисты Trend Micro.

«EDR — только часть общей системы обнаружения и реагирования на атаки. Это прекрасный инструмент, но он обладает ограниченным охватом, так как обрабатывает только данные, поступающие с конечных устройств. А ведь полная видимость и понимание источников атак в условиях множественных вертикалей защиты — это важнейшая задача для специалистов SOC. Поэтому мы предлагаем им платформу XDR, которая способна справиться с такой задачей, — отмечает Даня Таккар (Dhanya Thakkar), старший вице-президент Trend Micro в регионе AMEA. — Наши клиенты в регионе выказывали огромный интерес к платформе ещё с прошлого года, и вот теперь они смогут полноценно воспользоваться всеми её возможностями». ***(Решение Trend Micro XDR стало доступно в нашем регионе // Компьютерное Обозрение (https://ko.com.ua/reshenie_trend_micro_xdr_stalo_dostupno_v_nashem_regione_134147). 14.08.2020).***

***

«Ряд новых и будущих функций безопасности, анонсированных Slack Technologies, должны помочь предприятиям защитить информацию, которой их служащие обмениваются в чат-каналах.

Это обновление также позволит Slack более уверенно конкурировать со своим главным соперником на корпоративном рынке, Microsoft Teams, во многих областях, включая шифрование и аналитику угроз.

Появившаяся в прошлом году опция защиты данных во внутренних чатах предприятий будет значительно дополнена. Компании получат возможность использовать свои приватные ключи для шифрования также каналов Slack Connect, по которым они общаются с внешними партнёрами, например, с поставщиками.

Кроме того, компании смогут использовать специальные ключи с инструментом Slack Workflow Builder, служащим для автоматизации сбора информации (отзывов сотрудников, обращений в техподдержку), которую в некоторых организациях предпочитают хранить в зашифрованном виде, чтобы избежать утечек.

Помимо шифрования конфиденциальных записей, законами или внутренними политиками часто оговаривается регион их хранения. Slack позволяет настраивать страну хранения и добавила в список доступных локаций Канаду. Кроме того, заказчики теперь могут указать, где должны храниться их ключи шифрования.

На такие организации, как банки ориентирована функция «информационного барьера» Slack. Она служит для ограничения коммуникаций между отделами или

пользователями (например, между отделом биржевых торгов и отделом инвестиций).

Завершает перечень платформенных апдейтов, новые интеграционные возможности. Из Slack можно будет экспортировать журналы активности в популярную аналитическую платформу Splunk для поиска признаков нарушения защиты. Интеграция с инструментом Microsoft Intune позволит администраторам дистанционно стирать связанные с работой файлы на утерянных или похищенных устройствах сотрудников предприятия». ***(В Slack дебютируют новые опции безопасности для предприятий // Компьютерное Обозрение (https://ko.com.ua/v_slack_debyutiruyut_novye_opcii_bezopasnosti_dlya_predpriyatij_134116). 13.08.2020).***

***

«Компания NWU, официальный дистрибьютор решений Beyond Security в Украине, сообщила о том, что вендор добавил в свой флагманский продукт beSECURE функцию сканирования с использованием агентов.

Это позволит предприятиям выполнять полный обзор своих сетей и всех подсоединенных конечных устройств, включая IoT, OT и BYOD. С помощью новой функции администраторы смогут проводить мониторинг всей своей инфраструктуры с единой панели. Стала возможной также проверка подлинности конечных устройств, не подключенных непосредственно к сети, например, неуправляемых устройств, используемых удаленными сотрудниками, или в системах, которые не всегда включены.

«Мы горды тем, что предлагаем лучший сканер уязвимостей на рынке. Расширенные возможности сканирования beSECURE позволят нашим клиентам решать задачи, возникающие в период смены технологий и усиления значения вопросов безопасности, - заявил Авирам Дженик, генеральный директор и соучредитель Beyond Security. - Новые технологии порождают новые угрозы, в то время как старые не исчезли. Теперь благодаря расширенной функциональности наших решений мы можем обнаружить все из них».

Использованием агента дало новые возможности пользователям beSECURE, которые хотят избежать сложной задачи получения учетных данных для выполнения аутентифицированного сканирования в гетерогенных средах. Благодаря легковесным агентам на конечных устройствах пользователей клиенты могут сканировать как локальные, так и внешние устройства в любое время.

Агенты beSECURE могут быть установлены на любом подключенном в сеть Windows-устройстве. Помимо сканирования на наличие уязвимостей и вредоносных программ, новые агенты предлагают дополнительные опции, такие как защита от утечек данных, веб-фильтрация, управление устройствами и многое другое». ***(beSECURE реализовала сканирование уязвимостей с помощью агентов // Компьютерное Обозрение (https://ko.com.ua/besecure_realizovala_skanirovanie_uyazvimostej_s_pomoshhyu_agentov_134111). 12.08.2020).***

***

«Компания Eset представила новое комплексное решение Remote Workforce Offer для обеспечения всесторонней защиты корпоративной сети и конфиденциальной информации в условиях удаленного режима работы. Это решение обеспечивает обнаружение программ-вымогателей и атак нулевого дня, а также улучшает безопасность важных корпоративных данных.

В состав решения входят: защита рабочих станций; защита файловых серверов; анализ в облачной песочнице; полнодисковое шифрование; управление защитой на основе облачных технологий.

Переход на удаленный режим работы многих компаний поспособствовал увеличению рисков для их кибербезопасности. Среди опасностей, с которыми столкнулись организации, – утечка или похищение конфиденциальных данных, перехват информации злоумышленниками на уровне интернет-трафика, заражение вредоносным ПО и получение несанкционированного доступа к корпоративной сети. В частности, с начала года вдвое увеличилось количество сетевых атак через RDP и существенно выpос процент выявленных веб-угроз и вредоносных электронных писем.

Для защиты корпоративной среды Eset разработала Remote Workforce Offer, который обеспечивает эффективное обнаружение неизвестных угроз с помощью решений для защиты рабочих станций и файловых серверов в сочетании с продуктом Eset Dynamic Threat Defense, который осуществляет анализ подозрительных образцов в облачной песочнице.

Кроме этого, в состав нового решения входит продукт Eset Full Disk Encryption, который обеспечит дополнительную защиту корпоративной информации с помощью полнодискового шифрования. Благодаря этому продукту зашифрованные данные будут недоступны для прочтения без специального пароля, что поможет предотвратить несанкционированный доступ к конфиденциальной информации в случае кражи или заражения устройства.

Управление продуктами и обзор безопасности сети осуществляется с помощью облачной консоли Eset Cloud Administrator. Этот сервис простой в использовании и не требует покупки дополнительного оборудования, что позволяет сэкономить средства организации и упростить обеспечение защиты корпоративной сети». ***(Eset представила комплексное решение для защиты организаций в условиях удаленной работы // Компьютерное Обозрение (https://ko.com.ua/eset_predstavila_kompleksnoe_reshenie_dlya_zashhity_organizacij_v_usloviyah_udalennoj_raboty_134027). 06.08.2020).***

***

«Компания McAfee объявила о выпуске проактивного решения безопасности McAfee MVISION Insights, которое позволяет реагировать и настраивать компенсирующие меры защиты до начала атак. Данное решение отвечает за оперативный сбор новейших сведений об угрозах в глобальном масштабе.

Злоумышленники находят все новые способы оставаться незамеченными и осуществлять более сложные атаки. Чтобы помочь организациям быть на шаг

впереди, компания McAfee модернизировала свою платформу по защите конечных точек и дополнила возможностями MVISION Insights.

Используя глобальную телеметрию, поступающую от миллиарда датчиков, передовые исследования McAfee по угрозам, а также данные получены с помощью искусственного интеллекта, MVISION Insights позволяет автоматически отслеживать новые атаки в различных регионах и даже на отдельные отрасли. Благодаря этому, решение предоставляет организациям актуальную и упреждающую информацию об угрозах и активных глобальных кампаниях, включая описания и признаки взлома. Данная информация важна для оценки того, насколько те или иные угрозы распространены, какие последствия они могут иметь, и могут ли специалисты ИБ их заблокировать. Оценка степени защищенности с помощью MVISION Insights в сочетании со способностью принимать упреждающие меры до начала атак, дает возможность оперативно и заблаговременно повышать надежность защиты.

Интеграция MVISION Insights значительно расширяет возможности платформы McAfee для защиты конечных точек, помогая подразделениям ИБ быстрее реагировать на сложные атаки и расследовать их более эффективно.

Платформа McAfee для защиты конечных точек включает в себя MVISION Insights и другие технологии, которые обеспечивают: управление поверхностью атаки – предотвращение новых угроз в упреждающем режиме; предотвращение атак – реализация многоуровневой защиты от сложных вредоносных программ; обнаружение угроз – обнаружение сложных угроз и повышение скорости реагирования; проведение расследований – расширенные возможности по расследованию благодаря XDR (Extended Detect&Response); реагирование на инциденты – реагирование на угрозы за секунды; снижение совокупной стоимости эксплуатации систем и упрощение процессов». ***(McAfee выпускает проактивное решение безопасности MVISION Insights // Компьютерное Обозрение (https://ko.com.ua/mcafee_vypuskaet_proaktivnoe_reshenie_bezopasnosti_mvision_insights_133978). 03.08.2020).***

***

«Все знают, что хороший пароль должен быть длинным и сложным, но по-прежнему предпочитают более простые решения: уже семь лет подряд самые популярные пароли в интернете — 123456 и password.

Теперь, когда многие из нас работают дома и отключены от корпоративной сети, количество нужных паролей значительно увеличилось. Запомнить их трудно, но для этого есть менеджер паролей — он не только записывает кодовые слова, но также генерирует их и управляет автозаполнением форм. Публикуем список лучших сервисов для хранения паролей по версии журнала Wired.

Почему не стоит использовать браузер

У большинства браузеров есть хотя бы примитивное управление паролями. Это лучше, чем использовать один и тот же пароль для всех сервисов, но возможности браузеров ограничены — все-таки они создавались для других целей. Большинство из них не сгенерируют надежный пароль.

Поэтому эксперты по безопасности рекомендуют использовать специализированные сервисы. Они имеют одно назначение и год за годом получают новые полезные функции, поэтому смогут лучше обеспечить вашу безопасность в сети.

1Password — лучший вариант

1Password появился как инструмент управления паролями для Apple, но сейчас доступен для iOS, Android, Windows и ChromeOS. У него даже есть командная строка, которая может работать на любой платформе. Недавно было объявлено о предварительном выпуске клиента для Linux. У 1Password есть плагины для браузеров, которые позволяют легко генерировать и редактировать новые пароли.

Этот менеджер паролей отличается от других количеством дополнительных услуг. Например, его можно использовать для аутентификации, как Google Authenticator. Он обеспечивает дополнительную защиту, создавая пароль к своему ключу шифрования, без которого никто не сможет раскрыть ваши пароли. Однако если вы его потеряете, то пароли не расшифрует никто, даже 1Password.

Еще одна причина, по которой 1Password занимает первое место в рейтинге — его интеграция с другими мобильными приложениями. Вам не придется копировать и вставлять пароли из менеджера в другие приложения — 1Password может автоматически заполнять их. Это заметнее на iOS, где взаимодействие между приложениями более ограничено.

Еще одна причина любить 1Password — это его режим путешествия, который позволяет вам удалять любые конфиденциальные данные с ваших устройств перед поездкой, а затем восстанавливать их одним щелчком мыши после пересечения границы. Таким образом, никто, даже правоохранительные органы на международных границах, не сможет получить доступ к полному хранилищу паролей.

У 1Password есть 30-дневная бесплатная пробная версия, так что можно проверить его перед покупкой. Стоимость приложения — $3 в месяц ($36 в год, $60 в год для семей).

После регистрации загрузите приложение для Windows, MacOS, Android, iOS, ChromeOS или Linux. Также есть расширения для Firefox, Chrome и Edge.

Bitwarden — лучший бесплатный сервис

Bitwarden популярен среди поклонников ПО с открытым исходным кодом. И можно понять, почему — инструмент бесплатен, у него нет каких-либо ограничений, и он так же совершенен и удобен в использовании, как и вышеупомянутый 1Password.

И у него открытый исходный код. Это означает, что код Bitwarden доступен для любого, кто может проверить программу, найти недостатки и исправить их. Теоретически чем больше людей просматривают код, тем безупречнее он становится. В 2020 году Bitwarden также прошел аудит, который подтвердил его безопасность. Bitwarden можно установить на вашем сервере, чтобы создать собственный хостинг, если вы предпочитаете работать с облаком.

Есть приложения для Android, iOS, Windows, MacOS и Linux, а также расширения для всех основных браузеров, в том числе менее популярных Opera,

Brave и Vivaldi (все они поддерживают расширения Chrome). С недавних пор приложения Bitwarden для Windows и macOS поддерживают Windows Hello и Touch ID, что обеспечивает дополнительную безопасность этих систем.

Еще у сервиса есть полуавтоматический инструмент заполнения паролей. Если вы посещаете сайт, для которого сохранили учетные данные, значок Bitwarden в браузере показывает количество сохраненных логинов и паролей с него. Нажмите на значок, и он спросит, какую учетную запись вы хотите использовать, а затем автоматически заполнит форму входа. Это позволяет легко переключаться между профилями и избежать проблем с автозаполнением. Если вам нужно полностью автоматизировать заполнение форм, Bitwarden также подойдет.

У Bitwarden есть и платная подписка. Самый дешевый пакет Bitwarden Premium стоит $10 в год. В него входят 1 ГБ для зашифрованного хранения файлов, двухфакторная аутентификация с помощью YubiKey, FIDO U2F, Duo, а также отчет о безопасности паролей и работоспособности хранилища. Оплата также дает вам приоритетную поддержку клиентов.

После регистрации загрузите приложение для Windows, MacOS, Android, iOS или Linux. Есть также расширения для Firefox, Chrome, Safari, Edge, Vivaldi и Brave.

Dashlane — лучший многофункциональный менеджер

Еще несколько лет назад он мало чем отличался от конкурентов. Но в последних версиях, особенно в Dashlane 6, у сервиса появились новые уникальные функции. Одна из лучших — предупреждение о вторжении на сайт. Dashlane активно отслеживает темные уголки интернета, ищет утечки и кражи личных данных, а затем предупреждает, если ваша информация была скомпрометирована.

В версии для ПК легко ориентироваться, а мобильные приложения обеспечивают доступ к вашим данным из любого места. Синхронизация между устройствами доступна только в премиум-версии ($5 в месяц). Тем не менее, сервис просто настраивать. Как и 1Password, для шифрования ваших паролей он использует ключ.

Также есть возможность не хранить пароли на серверах Dashlane. Используя эту функцию, вы сами несете ответственность за управление хранилищем паролей и его синхронизацию между устройствами. Это менее удобно, но ваши пароли остаются у вас. 1Password или LastPass такой функции не предоставляют. В плане премиум есть и другие приятные дополнения, которых нет у других сервисов, например, бесплатный VPN.

Обычный план Dashlane Premium стоит $5 в месяц ($60 в год), семейный (до пяти пользователей) — $7,5 в месяц. Есть также Premium Plus, который стоит $10 в месяц ($120 в год) для индивидуальных пользователей и $15 в месяц — для семей. Расширенная версия предоставляет инструменты для восстановления личных данных и их защиты от кражи. Dashlane предлагает 30-дневную бесплатную пробную версию для любого плана.

После регистрации загрузите приложение для Windows, MacOS, Android, iOS или Linux. Также есть расширения для Firefox, Chrome и Edge.

KeePassXC — лучший вариант для самостоятельной настройки (с собственным сервером)

Хотите сохранить больший контроль над данными в облаке? Попробуйте использовать программу для ПК, например KeePassXC. Она помещает зашифрованные версии ваших паролей в зашифрованное цифровое хранилище, которое защищается с помощью мастер-пароля, ключевого файла или и того, и другого. Сервисы наподобие 1Password хранят данные на стороннем хостинге и синхронизируют его для ваших целей, а здесь вы синхронизируете базы данных самостоятельно, используя такой сервис, как Dropbox или рекомендованный Эдвардом Сноуденом SpiderOak. Как только файл окажется в облаке, к нему можно будет получить доступ с любого устройства, на котором есть клиент KeePassXC.

Зачем делать это самостоятельно? Для повышения прозрачности. Как и Bitwarden, KeepassXC — программа с открытым исходным кодом, то есть ее можно проверить на наличие критических дефектов.

KeePassXC бесплатен. Загрузите десктопное приложение для Windows, MacOS или Linux и создайте свое хранилище. Есть также расширения для Firefox и Chrome, но не Edge. У него нет официальных приложений для телефона. Создатели рекомендуют KeePass2 для Android или Strongbox для iPhone.

NordPass — новичок на рынке

NordPass — это относительно новый менеджер паролей, но он создан компанией с именем. NordVPN — хорошо известный VPN-провайдер, и его менеджер паролей отличается такой же простотой в использовании, как и более известное приложение. Его очень легко установить и настроить. Есть приложения для всех основных платформ (включая Linux), браузеров и устройств.

Бесплатная версия NordPass ограничена одним устройством, синхронизация недоступна. Для премиум-версии есть семидневный бесплатный пробный период, который позволяет протестировать синхронизацию устройств. Но чтобы получить эту функцию, вам придется перейти на план стоимостью $36 в год. (Как и в своем VPN-сервисе, здесь NordPass принимает платежи в криптовалютах.)

NordPass использует метод нулевого разглашения, при котором все данные шифруются на вашем устройстве и только потом отправляются на серверы компании. Другие приятные функции: поддержка двухфакторной аутентификации и встроенный генератор паролей (подберет подходящий вариант даже для тех сайтов, которые предъявляют странные требования к вашему паролю).

Недавно в нем также появилась возможность хранить личную информацию: адрес, номер телефона и другие данные будут оставаться в безопасности, но при необходимости к ним легко предоставить доступ. NordPass бесплатен, можно перейти на премиум-план ($36 в год).

После регистрации загрузите приложение для Windows, MacOS, Android, iOS или Linux. Также есть расширения для Firefox, Chrome и Edge.

Сервисы для особых потребностей

Менеджеры паролей — это не универсальное решение. Подборка выше отвечает потребностям большинства пользователей, но вам, возможно, потребуется что-то иное. К счастью, существует множество очень хороших менеджеров паролей.

LastPass (бесплатно, премиум-план стоит $36 в год): это один из самых популярных менеджеров паролей. Он работает практически на всех платформах и

устройствах, хотя недавно отказался от разработки приложения для macOS из-за изменений в инструментах Apple для разработчиков. У LastPass было несколько крупных ошибок и несколько утечек . Однако в целом он остается хорошим выбором для тех, чей бюджет ограничен. Недавно компания представила службу мониторинга, которая позволит узнать, что ваши данные были скомпрометированы.

Remembear ($36 в год): делает все, чего можно ожидать от менеджера паролей. Вообще, менеджеры паролей — это, возможно, самая скучная программа, которая может быть на вашем устройстве. Remembear успешно справляется с этой проблемой, используя в интерфейсе симпатичного медведя и множество забавных каламбуров. У Remembear есть все необходимое для начинающих, в том числе понятный интерфейс. В нем отсутствуют некоторые функции, которые могут понадобиться продвинутым пользователям, например, двухфакторная аутентификация (Remembear поддерживает ее для входа на сайты, но не для самого приложения) и проверка надежности пароля. Существует бесплатная пробная версия, но она не предполагает синхронизации. Премиум-аккаунт стоит $36 в год и предоставляет синхронизацию со сквозным шифрованием, безопасное резервное копирование и приоритетное обслуживание клиентов.

Enpass (бесплатно, $12 в год или одноразовый взнос в $60 за премиум-план): как и KeePassXC, сервис не хранит никаких данных на своих серверах. Синхронизация осуществляется через такие сторонние сервисы, как Dropbox или NextCloud. У Enpass есть приложения для всех платформ. Когда вы настроете синхронизацию, он заработает так же, как и любой другой менеджер паролей. И вам не нужно беспокоиться о том, что Enpass будет взломан, потому что ваши данные не находятся на его серверах. Если вам удобно самостоятельно настраивать безопасную синхронизацию, Enpass — отличный вариант.

Keeper (бесплатно, премиум-план стоит $36 в год): Keeper предлагает множество инструментов, обеспечивающих онлайн-безопасность, включая менеджер паролей. Keeper работает так же, как 1Password и прочие сервисы: хранит только зашифрованные данные, а для входа в учетную запись предлагает двухфакторную аутентификацию. Как и у Dashlane, у Keeper есть множество дополнительных функций, включая мониторинг дарквеба. Сервис будет проверять публичные данные, чтобы убедиться, что ваша информация защищена.

Основные параметры менеджера паролей

Хорошее приложение хранит, генерирует и обновляет пароли для вас одним нажатием кнопки. Если вы готовы тратить несколько долларов в месяц, менеджер может синхронизировать ваши пароли на всех устройствах. Вот как это работает.

Чтобы получить доступ ко всем паролям, вам нужно запомнить только один ключ. Когда вы вводите его в менеджер, он открывает хранилище, содержащее все ваши пароли. Необходимость запоминать только один пароль — это здорово, но это означает, что от него очень много зависит. Убедитесь, что это хороший пароль.

Если вам трудно его придумать, изучите советы по улучшению безопасности паролей. Вы также можете рассмотреть метод Diceware.

Приложения и расширения. Большинство менеджеров паролей являются полноценными системами, а не отдельными программами. Они состоят из

приложений или расширений браузера для каждого из ваших устройств (Windows, Mac, Android-телефонов, iPhone и планшетов), в которых есть инструменты, помогающие создавать пароли, хранить их и оценивать надежность существующих паролей. Вся эта информация затем отправляется на центральный сервер, где ваши пароли шифруются, хранятся и передаются между устройствами.

Исправление скомпрометированных паролей. Хотя менеджеры паролей могут помочь вам создать более безопасные пароли и защитить их от посторонних глаз, они не смогут защитить ваш пароль, если сайт будет взломан. Однако это не означает, что они не помогают. Все упомянутые облачные менеджеры предлагают инструменты для оповещения о потенциально скомпрометированных паролях. С ними легче изменить кодовое слово и проверить, что оно не используется на других сайтах.

Автоматическое заполнение форм. Некоторые менеджеры паролей будут автоматически заполнять и даже отправлять за вас данные — это очень удобно, но не совсем безопасно. Возможно, эту функцию стоит отключить, так как в прошлом из-за автозаполнения менеджеры паролей оказались уязвимыми для атак.

Не паникуйте по поводу взломов: в любой программе есть ошибки. Нужно знать что делать, когда обнаружится уязвимость менеджера. Ответ таков: во-первых, не паникуйте. Обычно ошибки обнаруживаются и исправляются до того, как ими удастся воспользоваться. Даже если кто-то и сможет получить доступ к серверам вашего менеджера паролей, вы все равно будете в порядке. Все перечисленные нами сервисы хранят только зашифрованные данные, и ни один из них не хранит ваш ключ шифрования, то есть все, что злоумышленник получает от компрометации серверов, — это зашифрованные данные». ***(Елена Лиханова. Менеджеры паролей, которые лучше всего защитят ваши данные // Rusbase (https://rb.ru/story/pass-managers/). 20.08.2020).***

***

«Проект Tor предложил несколько схем защиты, которые можно было бы использовать в будущем для ограничения воздействия распределенных атак типа «отказ в обслуживании» (DDoS), которые годами преследовали защищенные сайты даркнета (Onion) [1, 2].

Эти параметры защиты будут поддерживать как удобство использования, так и безопасность после их применения, что позволяет серверам, на которых размещены луковые службы, больше не зависать, когда они подвергаются атаке отказа в обслуживании (DoS).

Внутренняя работа DoS-атак на луковые сайты

DoS-атаки, нацеленные на луковые сайты (также известные как DoS-атаки с вводным наводнением), предназначены для использования протокола рандеву луковых служб путем отправки небольших сообщений, побуждающих луковые службы расходовать много ресурсов для реагирования на запрос.

Злоумышленники могут воспользоваться этим, чтобы перегружать луковую службу сотнями или тысячами запросов, истощая ресурсы ЦП сервера, заставляя его согласовывать безопасные сетевые каналы Tor, которые никогда не будут использоваться.

«Атаки используют присущую асимметричному характеру протокола рандеву луковых сервисов, и это затрудняет защиту от них», - сказал разработчик ядра Tor Project Core Джордж Кадианакис .

«Эта асимметрия открывает протокол для DoS-атак, а анонимный характер нашей сети делает чрезвычайно сложной задачей отфильтровать хороших клиентов от плохих».

Эту проблему нельзя решить простым изменением или настройкой кода, но вместо этого потребуются фундаментальные изменения в кодовой базе Tor, чтобы полностью решить эту проблему.

Тем не менее, проект Tor уже некоторое время обсуждает решения для повышения доступности луковых сервисов во время DoS-атак, и ряд из них был предложен более года назад (в том числе представленные Кадианакисом):

• Внедрение анонимных токенов на уровне приложений, которые позволяют законным клиентам получить приоритет над атакующим DoS.

• PoW подходит как argon2.

• Подходы CAPTCHA, такие как введение сервера токенов, выдающего токены reCAPTCHA.

• Скрытие вводных точек путем ограничения скорости их поиска клиентами.

• Наличие вступлений для проверки того, что клиенты не используют один и тот же IP-адрес снова и снова.

• Платите биткойн, чтобы познакомиться.

Предлагаемые решения проблемы DoS

Варианты, предложенные Кадианакисом, могут обеспечить «долгосрочную защиту от проблемы, сохраняя при этом удобство использования и безопасность луковых сервисов».

Один из способов убедиться, что запросы злоумышленников не имеют приоритета над запросами хороших клиентов, - это реализовать систему анонимных токенов, настроив сервер CAPTCHA, который будет препятствовать способности злоумышленников сбивать серверы луковых служб.

Такие токены (которые будут эквивалентом учетных данных) также могут быть использованы в будущем для «ограничения злонамеренного использования выходных узлов Tor спамом и автоматическими инструментами», «для регистрации запоминающихся человеком имен для луковых сервисов» и для «получения частные мосты и узлы выхода для дополнительной безопасности ».

Tor может также принять систему Proof-Of-Work (POW) (предложение для нее уже доступно здесь), чтобы решить текущую проблему DoS, сделав практически невозможным для злоумышленника сбой луковой службы, "при этом делая ее доступной для нормальные клиенты с небольшой задержкой ".

«Большим преимуществом этого подхода является то, что предлагаемая система PoW является динамичной и автоматически адаптирует свою сложность в зависимости от объема вредоносной активности, поражающей службу», - пояснил Кадианакис.

«Следовательно, когда есть большая волна атаки, сложность увеличивается, но она также автоматически уменьшается, когда волна проходит».

Как объясняет Кадианакис, хотя оба эти варианта имеют некоторые недостатки и ограничения, они дополняют друг друга и могут применяться вместе.

«Никто не хочет, чтобы сеть Tor была заполнена CAPTCHA или головоломками PoW, запрещающими мобильные устройства», - добавил он.

«Здесь жизненно важны настройка параметров и тщательный дизайн. В конце концов, устойчивость к DoS-атакам - это экономическая игра: цель не в том, чтобы быть идеальным; цель - поднять планку настолько, чтобы финансовые затраты злоумышленника на поддержание атаки были выше чем выигрыш "…». ***(Sergiu Gatlan. Tor Project shares proposals to limit DDoS impact on Onion sites // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/tor-project-shares-proposals-to-limit-ddos-impact-on-onion-sites/). 19.08.2020).***

***

«Исследователь разработал Killswitch, использующий переполнение буфера в Emotet, предотвращающий заражение системы вредоносным ПО в течение шести месяцев.

Исследователь смог использовать уязвимость в Emotet, что привело к сбою печально известной вредоносной программы и не позволило ей заразить системы в течение шести месяцев.

Emotet, который впервые появился в 2014 году и с тех пор превратился в полноценный ботнет, предназначенный для кражи учетных данных и загрузки дополнительных вредоносных программ, таинственным образом исчез с февраля до своего недавнего повторного появления в начале августа.

В пятницу Джеймс Куинн из Binary Defense рассказал, почему: в начале этого года он разработал выключатель, получивший название «EmoCrash», который использовал уязвимость переполнения буфера, обнаруженную в процессе установки Emotet.

Он не единственный, кто пытается помешать Emotet: новости появились вскоре после того, как исследователи обнаружили, что таинственный линчеватель боролся с акторами угрозы, стоящими за возвращением вредоносной программы, заменяя вредоносные полезные нагрузки Emotet причудливыми гифками и мемами.

Killswitch часто используется защитниками для отключения сетей от Интернета во время кибератак, но также может использоваться против семейств вредоносных программ как способ удалить их из систем и остановить все запущенные процессы.

«Подобно тому, как злоумышленники могут использовать недостатки в законном программном обеспечении для нанесения вреда, защитники могут также перепроектировать вредоносное ПО, чтобы обнаружить его уязвимости, а затем использовать их для уничтожения вредоносного ПО», - сказал Куинн в недавнем сообщении.

В начале февраля Emotet выпустил капитальный ремонт кодовой базы, который стал заголовком, позволившим образцу вредоносного ПО Emotet распространиться в небезопасные сети Wi-Fi, расположенные рядом с зараженным устройством.

Частью этого капитального ремонта была модификация различных методов установки и сохранения Emotet. Разработчики вредоносного ПО удалили список слов и алгоритм генерации файлов, ранее использовавшийся Emotet, и заменили его новым алгоритмом с новым подходом к сохраняемости.

Этот новый алгоритм генерировал случайно выбранное системное имя файла .exe или .dll, а затем зашифровывал имя файла с помощью ключа исключающего ИЛИ (XOR) и сохранял его как ключ реестра.

Куинн обнаружил простое переполнение буфера в этой процедуре установки и создал переключатель для устранения этой проблемы с помощью сценария PowerShell. Сценарий содержал буфер размером 0x340 (832) байта, который Emotet пытался сохранить в качестве ключа реестра, что в конечном итоге приводило к его сбою во время процесса установки (до его полной установки) и полностью предотвращало установку вредоносного ПО в системах.

«Этот крошечный буфер данных был всем, что нужно было для выхода из строя Emotet, и его можно было даже развернуть до заражения (например, вакцины) или в середине заражения (например, Killswitch)», - сказал Куинн.

Затем Куинн незаметно поделился выключателем с членами сообщества информационных систем, избегая общедоступных каналов, чтобы обеспечить максимальное время безотказной работы эксплойта, прежде чем злоумышленники, стоящие за Emotet, исправят свое вредоносное ПО, чтобы закрыть уязвимость.

«Благодаря невероятной координации между сообществами информационной безопасности и CERT, особенно теми из Team Cymru, которые очень помогли в этом, Binary Defense начала распространять сценарий эксплойта EmoCrash среди защитников по всему миру 12 февраля 2020 года со строгими инструкциями не запрещать опубликовать это публично», - сказал он.

Killswitch был активен с 6 февраля по 5 августа - в этот момент разработчики Emotet разослали обновление основного загрузчика, чтобы удалить код уязвимого значения реестра, что убило killswitch. Именно тогда Emotet снова появился после пятимесячного исчезновения, когда получателям электронной почты по всему миру было отправлено более 250 000 сообщений с вредоносным спамом». ***(Lindsey O'Donnell. 'EmoCrash' Exploit Stoppered Emotet For 6 Months // Threatpost (https://threatpost.com/emocrash-exploit-emotet-6-months/158414/). 17.08.2020).***

***

«Juniper выявляет фишинговые кампании, нацеленные на бизнес-клиентов с помощью вредоносных программ, используя, среди прочего, защиту паролем, чтобы избежать обнаружения.

Злоумышленники усовершенствовали банковский троян, который широко использовался во время пандемии COVID-19, новыми функциями, которые помогают избежать обнаружения потенциальными жертвами, и стандартными средствами защиты.

Согласно новому отчету исследователя безопасности Juniper Networks Пола Кимайонга, злоумышленники реализовали несколько новых функций, в том числе защищенное паролем вложение, обфускацию ключевых слов и минималистичный

макрокод, в недавней фишинг-кампании с использованием документов, троянизированных широко используемым банковским трояном IcedID.

Кампания, которую исследователи обнаружили в июле, также использует библиотеку динамической компоновки (DLL) - библиотеку Microsoft, которая содержит код и данные, которые могут использоваться более чем одной программой одновременно - в качестве загрузчика второго уровня. Это «показывает» новый уровень зрелости этого субъекта угрозы», - заметил он.

Последняя версия IcedID, определенная командой Juniper, распространяется с использованием скомпрометированных бизнес-аккаунтов, получатели которых являются клиентами тех же компаний. Это повышает вероятность успеха кампании, поскольку отправитель и получатель уже имеют налаженные деловые отношения, отметил Кимайонг.

Исследователи из IBM впервые обнаружили IcedID еще в 2017 году как троян, нацеленный на банки, поставщиков платежных карт, поставщиков мобильных услуг, платежные ведомости, веб-почту и сайты электронной коммерции.

Вредоносная программа развивалась на протяжении многих лет и уже имеет историю умной обфускации. Например, он появился во время кампании COVID-19 с новой функциональностью, которая использует стеганографию или практику сокрытия кода внутри изображений для скрытого заражения жертв, а также другие улучшения.

В отчете Кимайонга подробно описан пример новой кампании IcedID и ее тактики уклонения от взлома PrepNow.com, частной общенациональной компании по обучению студентов, которая работает в ряде штатов США.

Злоумышленники отправляли потенциальным жертвам фишинговые электронные письма, в которых якобы есть счет-фактура. Они якобы из бухгалтерии, с прикрепленным файлом ZIP, защищенным паролем. Он отметил, что эта защита паролем позволяет файлу избежать защиты от вредоносных программ. Пароль включен в тело письма, чтобы жертвы могли найти и использовать его для открытия файла.

Кампания является новинкой в том, что она разными способами скрывает слово «прикрепленный» в электронном письме, пишет Кимайонг. По его словам, маловероятно, что злоумышленники сделают это, чтобы попытаться обойти спам-фильтры или обнаружение фишинга, поскольку наличие вложения очевидно.

«Во всяком случае, мы ожидали, что обфускация запутает слово «пароль», потому что это явный признак того, что происходит что-то фишинговое», - написал Кимайонг. «С другой стороны, даже незначительное изменение тела электронного письма может изменить некоторые решения для защиты электронной почты с нечеткими хэшами, которые вычисляются для выявления массовых почтовых кампаний».

Кампания также включала любопытное поведение, заключающееся в изменении имени файла, используемого для вложения внутри ZIP-файла, что кажется «бесполезной» попыткой обойти меры безопасности, «поскольку защита паролем должна препятствовать открытию и проверке большинством решений безопасности. содержание, - заметил он.

Как бы то ни было, электронная почта не была заблокирована службой безопасности Google Gmail, что, по-видимому, доказывает, что тактика уклонения сработала, согласно отчету.

Если жертвы открывают вложение, кампания запускает трехэтапную атаку, чтобы запустить троян IcedID, пишет Кимайонг.

Расширенный ZIP-файл представляет собой документ Microsoft Word, содержащий макрос, который выполняется при открытии документа, с «обычной попыткой социальной инженерии заставить жертв включить макросы», - написал он. «После включения макросов сценарий VB загрузит DLL, сохранит ее в формате PDF и установит как службу, используя regsvr32, чтобы гарантировать постоянство».

Этот этап также показывает, насколько злоумышленники «минималистичны» в использовании макрокода, который «очень прост и понятен», даже несмотря на то, что ему все еще удается скрывать строки и вызовы функций, чтобы избежать обнаружения, пишет Кимайонг.

На втором этапе атаки DLL загружается с сайта 3wuk8wv [.] Com или 185.43.4 [.] 241, размещенного на хостинг-провайдере в Сибири в России. После загрузки вредоносная DLL сохраняется в виде PDF-файла, а затем, согласно отчету, макрос выполняет его посредством вызова regsvr32.exe.

DLL загружает следующий этап атаки из домена loadhnichar [.] Co в виде файла PNG и расшифровывает его, пишет Кимайонг. Он отметил, что этот этап атаки также имеет тактику уклонения.

«Этот загрузчик смешивает свой трафик с запросами к безопасным доменам, таким как apple.com, twitter.com, microsoft.com и т.д., Чтобы песочницы пытались его проанализировать», - написал Кимайонг.

По его словам, на третьем этапе основной модуль IcedID загружается в виде файла PNG, запускается процесс msiexec.exe и внедряется в него основной модуль IcedID». ***(Tara Seals. IcedID Trojan Rebooted with New Evasive Tactics // Threatpost (https://threatpost.com/icedid-trojan-rebooted-evasive-tactics/158425/). 18.08.2020).***

***

«29 августа на Kickstarter закончился сбор заявок на электронный мультитул Flipper Zero.

В Итоге Flipper Zero собрал $4 882 784. В проект вложились 37 987 человек на краудфандинговой платформе.

Первоначально при выходе на Kickstarter была задача собрать сумму $60 тысяч, которая была набрана за 8 минут. Спустя сутки после размещения у проекта было более $500 тыс. сборов, а через полтора дня был собран $1 млн.

По словам разработчиков, в одном устройстве объедено как можно больше аппаратных инструментов для тестирования проникновения в электронные системы.

Устройство имеет встроенные радиомодуль, который поддерживает прием и передачу сигналов на частотах 300-928 МГц. Flipper Zero способен записывать и воспроизводить сигналы с пультов управления и электронных ключей. Также

устройство имеет инфракрасный передатчик, способный отправлять сигналы на бытовую технику и другие приборы с инфракрасным управлением.

Минимальную цену для начала производства установили в 60 тысяч долларов. Flipper Zero стоит $169, но на Kickstarter его цена колебалась в районе $99-129. По словам разработчика, в будущем «тамагочи для хакеров» будет продаваться через интернет-магазины и торговых посредников». ***(«Тамагочи для хакеров» собрал почти 5 млн долларов // SecurityLab.ru (https://www.securitylab.ru/news/511575.php). 30.08.2020).***

***

«Некоммерческая организация MITRE Corp выпустила новое руководство под названием MITRE Shield, предлагающее техники и тактики по проактивной защите компьютерных сетей от кибератак.

Новый фреймворк представляет собой общедоступную базу знаний, с помощью которой ИБ-специалисты смогут сформировать стратегию взаимодействия с атакующими и предпринять меры по более активной защите от кибератак.

Руководство содержит восемь разделов, посвященным различным тактикам обеспечения защиты, включая API-мониторинг, поведенческий анализ, манипуляцию электронной почтой, создание приманок (фальшивых учетных записей, сетей, учетных данных), мониторинг активности систем и пр.

MITRE Corporation — крупная американская некоммерческая организация, специализирующаяся в области системной инженерии и ведущая разработки и исследования в интересах органов государственной власти США, таких как Министерство обороны США, Федеральное управление гражданской авиации США и т.д». ***(MITRE представила новое руководство по защите от кибератак // SecurityLab.ru (https://www.securitylab.ru/news/511444.php). 25.08.2020).***

***