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

№ 10 (жовтень)

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– №10 (жовтень) . – 267с.

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

«Без взаємодії держави та приватного сектору неможливо побудувати ефективну систему кіберзахисту. На цьому наголосив заступник Секретаря Ради національної безпеки і оборони України Сергій Демедюк під час виступу на Третьому міжнародному форумі «Кібербезпека. Захистимо бізнес - захистимо державу»…

"На думку Демедюка, саме бізнес має формувати правила, за якими ми маємо жити в кіберпросторі, перед державою же поставлено завдання забезпечувати дотримання цих правил", - інформують у пресслужбі.

"Чим більше ми будуватимемо спеціальних центрів кіберзахисту, тим швидше ми проходитимемо етап становлення ринку кіберзахисту", - сказав він.

Так, зі слів Демедюка, провідну роль у питанні розбудови державно-приватного кібербезпекового партнерства відведено Національному координаційному центру кібербезпеки при РНБО України.

"НКЦК - це перший робочий орган РНБО, що був створений після потужних атак, яких зазнала Україна за останні роки. Ми довели, що у необхідний час можемо без бюрократичних перепон долучити до захисту держави приватний сектор. Тому що без бізнесу неможливо будувати ефективний кіберзахист", - сказав він.

За словами заступника Секретаря РНБО, ключові суб'єкти забезпечення кібербезпеки виконують свої функції, водночас вони через законодавчі обмеження надають послуги переважно державному сектору. НКЦК має об'єднати зусилля держави та приватного сектору на одному майданчику для спільної та ефективної співпраці і подолання цих обмежень, сказав він.

"НКЦК став єдиним національним хабом для взаємодії держави і приватного сектору. У Центрі є штатні посади для фахівців з приватного сектору, які можуть поділитися своїми знаннями та навичками для захисту держави", - сказав він, додавши, що спільна взаємодія "дозволить не лише відбивати атаки, але й розробляти продукт, який ми можемо пропонувати партнерам".

За інформацією пресслужби, в рамках форуму, з метою налагодження більш ефективного кібербезпекового співробітництва між державою та бізнесом, заступник Секретаря РНБО України та президент Торгово-промислової палати України Чижиков підписали Меморандум про співпрацю між Апаратом РНБО України та Торгово-промисловою палатою України…». ***(Саша Картер. РНБО: саме бізнес має формувати правила, за якими ми маємо жити в кіберпросторі // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1895663-rnbo-same-biznes-maye-formuvati-pravila-za-yakimi-mi-mayemo-zhiti-v-kiberprostori). 06.10.2020).***

***

«У Національному університеті кораблебудування імені адмірала Макарова відбулося відкриття Навчально-наукового аналітичного центру дослідження гібридних загроз національної безпеки на Півдні України.

Мета Центру — створити науковий контент та певні напрацювання, які б допомогли півдню України протистояти гібридним загрозам і викликам. Так, в першу чергу організація сприятиме налагодженню співпраці з іншими подібними центрами в Україні і за її межами, створенню інтелектуального продукту, направленого на вирішення поставлених завдань, співпраці зі студентами і науковцями інших навчальних закладів, а також протидії гібридним загрозам національної безпеки в регіональному аспекті.

Відкриття такої організації на базі НУК для нашого регіону є надзвичайно важливою подією, адже на півдні України немає ані спеціальності, пов'язаної з національною безпекою, ані центрів, які б досліджували саме гібридну тематику. Так вважає доктор політичних наук, професор кафедри соціально-гуманітарних дисциплін НУК Наталія Ніколаєнко. «Це не буде суто політологічний центр. Ми поєднуємо науковців із державного управління, політологів, істориків. Також багато в нашому університеті фахівців з економічної безпеки; у нас гарно розвивається спеціальність «Кібербезпека». Тому поєднання таких потужних інтелектуальних зусиль з різних галузей знань дадуть нам змогу створювати справді корисні рекомендації щодо подолання певних негативних явищ», — розповіла пані Наталія.

Варто звернути увагу, що створити Центр в Національному університеті кораблебудування вирішено не випадково, адже у виші існують потужні умови для цього. Це підтвердив проректор з науково-педагогічної роботи НУК Сергій Слободян. Він зазначив, що на сьогоднішній день НУК єдиний в Україні заклад, який плідно співпрацює з Військово-морськими силами ЗСУ. Свого часу в нас була військово-морська кафедра, тобто залишилися фахівці. Ми маємо справи з різноманітними технотеоріями оборонного призначення. У нас є свій спецвідділ, який все це відслідковує».

Цього ж дня, одразу після відкриття, відбувся перший круглий стіл з питання протидії гібридним загрозам. Її учасники ухвалили резолюцію, яку направили до Миколаївської міської ради, Миколаївської облдержадміністрації, Миколаївської обласної ради та Міністерства освіти і науки України. Очолила перший на Півдні України Центр професор Наталія Ніколаєнко». ***(У Миколаєві відкрили Центр дослідження гібридних загроз // Баба Клава дает добро (https://blin.mk.ua/news/136514). 07.10.2020).***

***

«7 октября Центральная избирательная комиссия запустила чат-бот (https://t.me/cvk_elections_bot), с помощью которого можно получить практически в полном объеме справочную информацию относительно местных выборов 25 октября 2020 года, сообщает пресс-служба ЦИК.

Для удобства пользователей информация в чат-боте систематизирована по блокам для конкретной категории субъектов избирательного процесса: избирателей, членов комиссий, кандидатов и политических партий.

В частности, избиратели будут иметь возможность не только получить в доступной форме почти любую информацию, связанную с будущими выборами, но

и быстро найти место расположения избирательного участка, где они должны голосовать.

Важно, что чат-бот пригодится и избирателям с инвалидностью. Ведь его программа позволяет проверить доступность всех без исключения помещений, где будет происходить голосование.

Отмечается, что для членов избирательных комиссий, кандидатов и политических партий чат-бот должен стать своеобразным путеводителем на все время избирательной кампании. Собранный для данной категории субъектов избирательного процесса массив информации позволит получить ответы и советы как относительно общих вопросов, так и относительно конкретных процедур.

Актуален также раздел, связанный с мерами по предупреждению распространения COVID-19 на избирательных участках. Данный блок содержит конкретные рекомендации по безопасной организации голосования в условиях пандемии коронавируса.

Кроме того, все пользователи чата-бота ЦИК смогут подписаться на календарь выборов, а также воспользоваться поисковой системой, что ускорит получение необходимой информации.

Кроме Телеграмм, чат-бот будет также доступен в Фейсбук.

Программное обеспечение чат-бота ЦИК разработано в рамках проекта "Повышение кибербезопасности и прозрачности избирательных процессов в Украине", который Координатор проектов ОБСЕ в Украине реализует совместно с ЦИК». ***(ЦИК запустила чат-бот о местных выборах // Інформаційне агенство "ЛІГА:ЗАКОН" (https://jurliga.ligazakon.net/news/198791_tsik-zapustila-chat-bot-o-mestnykh-vyborakh). 08.10.2020).***

***

«Полковник поліції Олександр Гринчак взяв участь у ІІІ Міжнародному форумі «Кібербезпека – захистимо бізнес, захистимо державу». Форум відбувся в рамках Місяця кібербезпеки і об’єднав представників державних, громадських і бізнесових кіл.

Учасники обговорили шляхи державно-приватної взаємодії в розбудові безпечного кіберпростору в Україні.

Олександр Гринчак повідомив, що підрозділ розробив концепцію розвитку та трансформації до 2025 року. Кіберполіція має на меті розширити штат фіхівців з кібербезпеки, оперативно взаємодіяти з міжнародними гравцями кіберпростору, збудувати системну роботу як зі стандартними алгоритмами кібербезпеки, так і створити інноваційні підходи у боротьбі з кіберзлочинністю.

Ключовий фокус зусиль направлений на створення закритого циклу протидії кіберзлочинам (розвідка, профілактика, реагування), відточення нішевої експертизи у роботі в кіберпросторі з банківською лінією, протиправним контентом та надання необхідної підтримки активним користувачам кіберпростору, іншим підрозділам поліції.

Під час своєї промови очільник підрозділу підкреслив, що разом із розвитком вільного Інтернет-простору набирає обертів і кіберзлочинність, тому Департамент кіберполіції України має відігравати одну із стрижневих ролей у створенні

безпечного кіберпростору для громадян України, українського суспільства і держави в цілому». ***(Очільник Департаменту кіберполіції Олександр Гринчак представив стратегію трансформації підрозділу // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/ochilnyk-departamentu-kiberpolicziyi-oleksandr-grynchak-predstavyv-strategiyu-transformacziyi-pidrozdil-4088/). 08.10.2020).***

***

«Міністерство цифрової трансформації заплатить більше мільйона гривень "білим хакерам", які зможуть знайти недоліки в додатку "Дія". Про це сказав віцепрем'єр-міністр - міністр цифрової трансформації України Михайло Федоров на брифінгу "Цифровізація банківських послуг: перші перемоги та плани"…

"Дія" безпечна. Перед тим, як Національний банк прийняв постанову, яка дозволяє відкривати рахунки онлайн та шерити документи, ми отримали сертифікат КСЗІ – це комплексна система захисту інформації, це, скажімо, "оскар" у напрямку кібербезпеки у нашій країні. Також ми пройшли два пентести – це такий аудит команій разом з USAID та Естонською академією е-урядування, тобто потужні партнери, які дбають про продукти, які вони підтримують", - сказав Федоров.

Він нагадав, що Міністерство у листопаді запускає bug bounty – можливість для "білих хакерів" знайти недоліки в "Дії".

"Ми будемо платити більше 1 млн грн тим, хто знайде ці недоліки", - завив міністр…» ***(Саша Картер. Хакнути "Дію" буде коштувати понад 1 млн грн – Федоров // Інформаційне агентство «Українські Національні Новини»(https://www.unn.com.ua/uk/news/1896865-khaknuti-diyu-bude-koshtuvati-ponad-1-mln-grn-fedorov). 13.10.2020).***

***

«Американская компания McAfee и группа компаний БАКОТЕК провели онлайн-форум по кибербезопасности в финансовом секторе. Главными темами форума стали состояние отрасли информационной безопасности в условиях пандемии, состояние кибербезопасности банковской системы Украины и решения McAfee для защищенной удаленной работы в облаке.

В рамках форума доклад о текущем уровне безопасности украинского рынка представила территориальный менеджер по работе с клиентами McAfee Айзада Кыдырбекова. Она отметила, что в условиях мировой пандемии старые методы и подходы в защите данных уже не столь эффективны. Например, по количеству целенаправленных атак за последние несколько месяцев Украина занимает 6-ое место в мире, а самих атак происходит в 2 раза больше, чем, к примеру, на Великобританию. В ходе своего доклада Айзада представила отчеты KPMG, Interpol и глобальной лаборатории McAfee, где выделила три негативных тенденции:

— стремительный рост фишинг-атак на 59% в период карантина;

— увеличение количества попыток входа в рабочие аккаунты одновременно из разных географических точек;

— растущий интерес мошенников к мобильным устройствам пользователей.

Отдельное внимание было уделено отсутствию нормативного регулирования требований к защите информации и киберзащиты в сфере перевода средств, а также наличие уязвимых мест к кибератакам программного обеспечения платежных систем и оперативных услуг платежной инфраструктуры.

По словам инженера McAfee Ивана Яковлева, проблемы в инфраструктуре цифровой безопасности есть:

— Нехватка кадровых ресурсов все еще актуальная проблема современности.

— Использование отдельных технологий для защиты конкретных данных. Одиночно такие технологии могут быть эффективны, но они не учится совокупно распознавать подозрительные активности.

— Не в пользу своевременного обнаружения и реагирования на атаку играет проблема перегрузки специалистов ручной работой. Это происходит из-за постоянно растущих для обработки объемов данных, количества консолей для управления и настройки защит сетевых безопасностей.

— Усложненные атаки. Сегодня атаки становятся все более комплексными. Цель злоумышленников — как можно быстрее произвести атаку (в 1-2 шага).

— Цифровая трансформация. Облачные решения упрощают работу, но не гарантируют безопасное хранение данных, а проблема теневого IT набирает обороты.

В начале этого года пандемия внесла свои коррективы, заставив многие компании пересмотреть ценность защиты корпоративных данных от кибератак. Если раньше компании ограничивались старыми, многоконсольными системами анализа и защиты, выполняя все вручную и тратя на это больше нужного времени, сегодня это время может сыграть не в пользу компании…» ***(Онлайн-форум по кибербезопасности в финансовом секторе БАКОТЕК и McAfee: атаки становятся сложнее и оперативнее // СофтПресс (https://hi-tech.ua/onlajn-forum-po-kiberbezopasnosti-v-finansovom-sektore-bakotek-i-mcafee-ataki-stanovyatsya-slozhnee-i-operativnee/). 14.10.2020).***

***

«Государственное предприятие «Отраслевой центр цифровизации и кибербезопасности» Министерства инфраструктуры Украины перенесло свои сервисы в облако GigaCloud. Переход в частное облако позволит предприятию продолжить развитие виртуального центра обработки данных Industry Cloud внедрением собственных сервисов обеспечения информационной безопасности, а также повысит стабильность работы инфраструктуры в целом.

«В нашем сотрудничестве с GigaCloud прослеживается этапность. Мы стартовали с небольшого объема ресурсов для проекта Е-транспорт. Впоследствии начали развиваться, увеличивалось количество проектов, и сейчас мы вышли на новый этап. Объем ресурсов стал достаточно большим, и мы задумались о переходе с публичного облака на частное решение. Это дало нам возможность

быстро запускать новые сервисы, наращивать обороты не в виде объема памяти, процессоров или дисков, а именно увеличивать количество серверов», – говорит Александр Ткаченко, начальник центра сопровождения информационных систем ОЦЦК.

Процесс переноса длился один месяц и включал поэтапный перенос сервисов предприятия. Начали с биллинговой системы PayGovUa – это набор сервисов для оплаты гражданами государственных и административных услуг. Биллинговая система непосредственно взаимодействует с банками и соответствует отраслевым стандартам банковской сферы, в частности, сертификату PCI DSS. Одно из требований прохождения этой сертификации – площадка, на которой размещена платежная система должна соответствовать требованиям физической и информационной безопасности. Благодаря тому, что облачная инфраструктура GigaCloud имеет международный сертификат ISO/ IEC 27001:2013 и аттестат соответствия КСЗИ, процесс прохождения сертификации ОЦЦК занял полтора месяца вместо полугода.

Следующим в облако перенесли транспортный портал электронных услуг «Е-транспорт». Это хаб с онлайн-услугами отрасли и дополнительными инструментами для граждан, перевозчиков, государственных служащих. Его задача – бронирование разрешений на перевозку в онлайн-режиме. Ранее такое разрешение можно было получить только в специальных сервисных центрах, разбросанных по всей Украине: приехать в сервисный центр, заполнить большое количество документов, заплатить сборы.

Еще один важный проект – сервис открытых данных транспортной отрасли, которое собирает статистические и аналитические данные о реализованных и нереализованных разрешений на международные грузовые перевозки. Также совместно с GigaCloud ОЦЦК запустило электронный кабинет моряка. Этот сервис похож на портал «Е-транспорт», поскольку также предназначен для переноса административных функций в онлайн. В электронном кабинете можно посмотреть собственные документы, подать онлайн-заявку на прохождение «Государственной квалификационной комиссии» (ГКК).

Последний проект, который ОЦЦК запустило совместно с GigaCloud – сервис SmartTicket – единый электронный билет на различные виды транспорта на выбранном маршруте (сейчас для киевского транспорта, поездов дальнего следования, а вскоре – для авиатранспорта, автотранспорта, муниципального транспорта других городов и такси). Теперь пользователю не нужно покупать разные билеты для различных видов транспорта в различных сервисах. Достаточно зайти на сайт SmartTicket и купить все необходимые билеты в составе единого электронного билета.

«Мы, как облачный оператор, отвечаем за безотказную работу облачной IT-инфраструктуры клиента, особенно в моменты пиковых нагрузок на сервисы, – говорит Кирилл Науменко, CTO GigaCloud. – Обеспечение ее оптимальной работы, обслуживание, эксплуатация и модернизация ресурсов – задача наших технических специалистов. Технические специалисты ОЦЦК занимаются непосредственным развитием своих сервисов и разработкой новых. Используя онлайн-сервисы Министерства инфраструктуры, граждане нашей страны смогут экономить время и

средства при оформлении различных разрешений, оплаты государственных услуг и быть уверенными в надежной защите их персональных данных». ***(«Отраслевой центр цифровизации и кибербезопасности» Мининфраструктуры перенес свои сервисы в GigaCloud // Компьютерное Обозрение (https://ko.com.ua/occk_perenes_svoi_servisy_v_chastnoe_oblako_gigacloud_135031). 27.10.2020).***

***

Національна система кібербезпеки

«На новоствореній кафедрі захисту інформації та кібербезпеки Житомирського військового інституту імені С. П. Корольова відкрили кіберполігон. Про це повідомляє пресслужба Сухопутних військ ЗСУ…

“Кіберполігон — це хаб, де курсанти та студенти можуть проводити дослідження та відпрацьовувати заходи протидії гібридним впливам у кіберпросторі, де можна займатись науковими розробками, проводити практичні заняття та організовувати змагання. Це реальна можливість ще під час навчання практично відпрацювати особливості протидії інформаційним загрозам у кіберпросторі: від створення та випробування новітніх технологій, тестування комп’ютерних систем і мереж на проникнення до відпрацювання заходів протидії гібридним впливам в кіберпросторі”, — йдеться в повідомленні…». ***(Наталія Затуливітер. У Житомирському військовому інституті відкрили кіберполігон // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1895237-u-zhitomirskomu-viyskovomu-instituti-vidkrili-kiberpoligon). 04.10.2020).***

***

«Держспецзв’язку разом із Міністерством цифрової трансформації, Радою національної безпеки та оборони України та Службою безпеки України РНБО, СБУ започаткувала роботу Експертної ради з інформаційної та кібербезпеки. Про це повідомив голова Держспецзв’язку Юрій Щиголь, передає пресслужба.

Експертна рада має стати платформою для «мозкового штурму» і механізмом для державно-приватного партнерства в сфері інформаційної безпеки та кібербезпеки.

«Її робота буде спрямована на вирішення таких завдань: розвиток організаційної системи забезпечення кібербезпеки, модернізацію законодавчої бази, посилення функціональної спроможності технологічної інфраструктури кібербезпеки та удосконалення системи підготовки кадрів», – зазначив Юрій Щиголь.

Він також запросив долучатись всіх бажаючих до складу Експертної ради…». ***(Держспецзв’язку започаткувала роботу Експертної ради з інформаційної та кібербезпеки // ДЕТЕКТОР МЕДІА***

(https://detector.media/infospace/article/181312/2020-10-06-derzhspetszvyazku-zapochatkuvala-robotu-ekspertnoi-radi-z-informatsiinoi-ta-kiberbezpeki/). 06.10.2020).

***

«Майже рік на базі 179-го навчально-тренувального центру військ зв'язку діє навчально-тренувальний комплекс захисту інформації та кібербезпеки…

Очолює комплекс капітан Геннадій Мягких. За словами офіцера, базовий курс навчання за цей період уже пройшли близько 300 зв'язківців.

"Головна мета підготовки спеціалістів за цим напрямком — навчити курсантів класифікувати та визначати типи мережевих атак та спосіб їхнього блокування, — зазначив офіцер. — Реалізація алгоритму здійснюється внесенням змін до інформаційної системи та відповідним налаштовуванням мережевого обладнання для забезпечення захисту інформації на об'єктах інформаційно-телекомунікаційних систем. Це потребує певних знань і навичок, ґрунтовної загальноосвітньої бази. Першу апробацію нових методик здійснили торік улітку. 24 строковики успішно опанували навчальну програму й отримали сертифікати про проходження курсів мережевої академії CISCO".

Цього року вирішено вдосконалити програму й доповнити фахову та базову підготовку спеціалістів розширеною курсовою. Тобто на базі навчально-тренувального комплексу створили систему навчання від простого до складного, щоб до цієї програми допустили тих, хто пройшов дві попередні. Навчання розраховане на 250 годин й орієнтоване на вишкіл контрактників.

Курсова підготовка спеціалістів кібербезпеки має блок "технології кібернетичної безпеки", де за основу використано матеріал онлайн-курсу Cisco Certified Network Associate Security мережевої академії Cisco. Навчальний процес охоплює теоретичний та практичний комплекси з урахуванням бойового досвіду АТО/ООС, стандартів і військово-нормативних документів НАТО.

Головна особливість організації занять, за словами керівника навчально-тренувального комплексу, полягає у моделюванні обстановки, максимально наближеної до реальної й пов'язаної із захистом інформації на об'єктах критичної інфраструктури та інформаційно-телекомунікаційних систем ЗСУ та оборонної сфери.

"Апробацію курсової програми підготовки фахівців захисту інформації та кібернетичної безпеки планують здійснити вже до кінця поточного року", – йдеться у повідомленні». ***(Володимир Лазарєв. У Полтаві контрактники апробують нову програму з кібернетичної безпеки // Новини Полтавщини (https://np.pl.ua/2020/10/u-poltavi-kontraktnyky-aprobuiut-novu-prohramu-z-kibernetychnoi-bezpeky/). 02.10.2020).***

***

«В этом месяце страна отпраздновала один из государственных праздников – на 14 октября указом Петра Порошенко был назначен День защитника Украины. Этот же документ, подписанный в 2014 году, отменил празднование Дня защитника отечества 23 февраля…

Сейчас решающим фактором является не только огневая мощь, а войны зачастую ведутся в киберпространстве. Регулярно совершаются хакерские атаки – ранее хакеры нацеливались лишь на грабежи, а сейчас это полноценный элемент государственного противостояния. Взламываются электронные переписки, блокируются сайты госструктур. Одной из важных задач для армии стала защита государственных интересов и в Интернете. С целью проведения полной модернизации осуществляются не только реформы, но и закупки необходимых средств. Так обновляются подразделения информационно-психологических операций Украины. Тендеры Минобороны размещаются в системе электронных закупок «Прозоро». Уже за первое полугодие на приобретение современной о техники для специалистов информационно психологического противодействия было затрачено около 10 млрд. грн. Части активно доукомплектовываются принтерами, ноутбуками, видеокамерами, проекторами и различной спецаппаратурой. В Украине на сегодняшний момент создано несколько крупных центров информационно-психологических операций – сокращенно ЦИПСО. Так под Киевом в Броварах находится 72 центр, во Львове – 74, в Одессе – 83. Вот уже несколько лет подряд специалисты в сфере кибербезопасности регулярно повышают свой уровень. Для этого их отправляют на всевозможные курсы, в том числе за границу. Украинские военные консультируются с инструкторами из стран НАТО. Командование спецоперациями США еще в начале года утвердило программу по совместным специальным операциям, в рамках которой проводятся курсы и семинары для военных из Украины. Так офицеры из 16, 72 и 83 центров принимали активное участие в семинаре по информационным возможностям. Основные занятия были посвящены анализу пропаганды теории влияния и стратегическим коммуникациям. Американские эксперты отметили хороший уровень украинских специалистов.

Все меру, которые принимаются руководством Украины для повышения квалификации специалистов, приносят свои плоды. Подобные активные действия проводятся уже не только в Украине, но и за ее пределами. Так офицеры из ЦИПСО-16 призывали блокировать работу на белорусских предприятиях, и на некоторых из них смогли вызвать временную остановку производства. Но наибольшее внимание специалисты уделяют все же проведению таких операций на своих территориях, в частности в Крыму. Многие офицеры ЦИПСО имеют опыт ведения боевых действий в составе миротворческих сил в Ираке и Сьерра-Леоне. Сейчас же основной их задачей является создание псевдоличностей в Сети, которые активно освещают события, происходящие на Донбассе и в Крыму. Внимание уделяется различным бытовым проблемам с формированием общественного мнения и перенаправлением его на критику агрессора.

Украинская армия активно реформируется и всегда должна быть готова не только к отражению хакерских атак и информационных угроз, но и к нанесению ответных превентивных ударов. В связи с этим повышение квалификации специалистов центров ИПСО является достаточно важной задачей для Минобороны. Уже в ближайшее время это позволит значительно повысить эффективность украинских военных в информационной войне против агрессора».

(Кибербезопасность для украинской армии // Українські Новини (https://job-sbu.org/kiberbezopasnost-dlya-ukrainskoy-armii-17161.html). 22.10.2020).

***

Правове забезпечення кібербезпеки в Україні

«Кабінет міністрів України у п’ятницю підтримав проект акту, яким передбачається створити правові засади для визначення об’єктів критичної інфраструктури...

“Проектом акту передбачається створити правові засади для визначення об’єктів критичної інфраструктури. Це стратегічно важливі для держави підприємства, установи, організації незалежно від форми власності. Це дозволить покращити рівень кібербезпеки в цьому напрямку”, — пояснив міністр цифрової трансформації Михайло Федоров.

З його слів, документом пропонується визначити механізм і критерії віднесення об’єктів до об’єктів критичної інфраструктури, перелік секторів основних послуг критичної інфраструктури, категорій критичності об’єктів критичної інфраструктури, органи влади, відповідальні за кожен сектор, порядок визначення рівня негативного впливу у разі пошкодження або знищення об’єкта критичної інфраструктури.

Уряд підтримав проект акту з доопрацюванням в одноденний термін…». ***(Саша Картер. Уряд зробив крок щодо визначення об’єктів критичної інфраструктури // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1896302-uryad-zrobiv-krok-schodo-viznachennya-obyektiv-kritichnoyi-infrastrukturi). 09.10.2020).***

***

Кібервійна проти України

«Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України під час моніторингу кіберпростору виявив витік інформації з однієї із найбільших приватних клінік міста Дніпро. Про це повідомляє пресслужба РНБО…

"Серед інформації, що опинилася у відкритому доступі, - персональні дані працівників та клієнтів цієї клініки, зокрема ПІБ, дати народження, адреси проживання, телефон, e-mail, діагнози, дані медичної картки (що становить медичну таємницю), включаючи результати аналізів, діагнози, інформація про захворювання, результати проведення ПЛР-тестів, списки хворих на COVID-19", - йдеться у повідомленні.

Зазначається, що аналіз інформації витоку показав, що до вільного доступу потрапили десятки тисяч записів про пацієнтів. За результатами дослідження було

встановлено, що витік стався внаслідок помилок конфігурації в інформаційних системах та базах даних медичного закладу, які мали доступ до мережі Інтернет.

"Слід зазначити, що вільний доступ до баз даних надавав можливість не тільки викрадення персональної інформації, але й несанкціонованого внесення змін, включно з модифікацією призначень ліків, результатів аналізів та обстежень, редагування записів в протоколі "Надання медичної допомоги для лікування коронавірусної хвороби (COVID-19)". З моменту виявлення витоку клініка пасивно реагувала на повідомлення фахівців НКЦК щодо витоку та вразливостей і не докладала зусиль до їх усунення. Дані щодо клієнтів приватної клініки досить довго перебували у вільному доступі", - зазначили у РНБО.

Вказується, що фахівці НКЦК підкреслюють, що Міністерство охорони здоров'я впроваджує електронну систему eHealth з урахуванням вимог законодавства про захист персональних даних, проте деякі суб'єкти господарювання нехтують заходами безпеки для захисту персональних даних клієнтів, зокрема через неповне розуміння законодавчих стандартів та вимог, які передбачають обов'язковість дотримання правил щодо збереження даних від зламів та витоків.

"НКЦК при РНБО України попередив медичний заклад про необхідність усунення вразливості та нагадав, що недбале відношення до збереження персональних даних клієнтів є приводом для притягнення правоохоронними органами керівництва приватної клініки до відповідальності", - резюмується у повідомленні…». ***(Марк Омелянюк. РНБО виявила витік персональних медданих однієї з найбільших клінік Дніпра // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1894921-rnbo-viyavila-vitik-personalnikh-meddanikh-odniyeyi-z-naybilshikh-klinik-dnipra). 02.10.2020).***

****

«В Україні почала діяти нова шахрайська схема з використанням QR-кодів, щоб заразити телефони жертв вірусом. В результаті цього, зловмисники отримують доступ до соціальних мереж жертви або до банківського застосунка.

«До мене буквально тиждень тому зверталися з кіберполіції щодо консультацій про такий вид шахрайства. Через карантин в більшості кафе і ресторанів використовують QR-код замість традиційного меню, це може призвести до зростання випадків шахрайства».

Олеся Данильченко, заступник директора ЕМА

Однак, говорити зараз про те, що така схема поширена, передчасно. «Вже були випадки в Європі. У нас це поки не так поширено», – зазначила Олеся Данильченко.

При цьому схема обману нічим не відрізняється від вже добре відомих, коли українцям пропонують перейти за шкідливими посиланнями або завантажити спеціальний додаток. Щоправда, раніше потрібно було зацікавити і вмовити перейти за посиланням, то зараз достатньо всього лише відсканувати QR-код.

Експерт з кібербезпеки розповіла, як працює схема з QR-кодом

Перше – шахраї залишають листочки з QR-кодами на стовпах, в кафе і ресторанах (щоб відвідувачі сплутали їх з меню).

Друге – людина переходить за посиланням і відразу потрапляє або на шкідливий сайт, який пропонує завантажити вірус, або відразу на сторінку із завантаженням програми;

Третє – погодившись відкрити або завантажити програму, телефон заражається вірусом, який може блокувати різні додатки, красти всі збережені паролі.

«Мета завжди одна і та сама – отримати доступ до коштів, зламати пошту, банківський додаток, зняти кошти з картки. Тут немає нічого нового. Все починалося з того, що такі посилання просто надсилали в повідомленнях у соцмережах. Потім, коли повідомлення перестали відкривати, почали зламувати сторінки і відправляти списку контактів і друзів те саме посилання. Зараз, коли і українці стали більш обережними користувачами, і соціальні мережі вдосконалили механізм верифікації та оперативно реагують на скарги, шахраї користуються QR-кодами». ***(Маргарита Січкар. В Україні почала діяти нова шахрайська схема з використанням QR-кодів // Pingvin Pro (https://pingvin.pro/gadgets/news-gadgets/v-ukrayini-pochala-diyaty-nova-shahrajska-shema-z-vykorystannyam-qr-kodiv.html). 09.10.2020).***

***

«Українських користувачів забороненої російської соцмережі ВКонтакті поставлять на облік. В Україні упродовж шести місяців - мають бути затверджені Стратегії кібербезпеки та інформаційної безпеки держави. Тоді Рада нацбезпеки та оборони обговорить питання обліку користувачів забороненої соцмережі ВКонтакті.

Про це розповіли в апараті РНБО на запит, яким чином буде здійснюватися такий облік, пише "Суспільне".

"Відповідно до затвердженої Стратегії національної безпеки України протягом півроку буде розроблено нову Стратегію кібербезпеки України, а також стратегію інформаційної безпеки. Питання створення "системи обліку українських користувачів російської соціальної мережі ВКонтакті та, за необхідності, інших соцмереж, що знаходяться під контролем держави-агресора, обговорюватиметься в рамках реалізації згаданих стратегій", – йдеться у повідомленні РНБО.

У відомстві зауважують, що доступ до російських заборонених соцмереж з території України становить реальну загрозу національній безпеці, тому "потребує зусиль щодо нейтралізації".

"Російська соцмережа ВКонтакті, яка перебуває під санкціями з 2017 року, є одним з інформаційно-психологічних засобів цієї гібридної війни, тому користування її ресурсами та розповсюдження відповідного російського контенту в інформаційному просторі України розцінюється як загроза національній безпеці України, що потребує нейтралізації", – зазначається у повідомленні РНБО». ***(Коли українських користувачів ВКонтакті поставлять на облік: названо дату // Знай. ua (https://chronicle.znaj.ua/342000-koli-ukrajinskih-koristuvachiv-vkontakti-postavlyat-na-oblik-nazvano-datu). 06.10.2020).***

***

«Служба безпеки України викрила в Дніпропетровській області регіональне відділення всеукраїнської мережі "тролів", які поширювали в соцмережах матеріали, що впливають на виборчий процес.

Пропагандисти також закликали до порушення територіальної цілісності України, повідомляє пресслужба СБУ.

Слідчі СБУ і фахівці з кібербезпеки викрили жителів Дніпра, Кривого Рогу та Павлограда - адміністраторів груп в соцмережах і розповсюджувачів антиукраїнські матеріали.

Розслідування велося протягом останнього місяця, а за його підсумками заблокована протиправна діяльність кількох інтернет-провокаторів.

Правоохоронці також встановили, що зловмисники активно вели переписку з жителями Росії і так званих ОРДЛО, які ставили перед ними завдання з розповсюдження фейковий матеріалів щодо майбутніх виборів в Україні і кандидатів в органи місцевого самоврядування. Вони планували ескалацію соціальної напруженості в регіоні і провокацію масових порушень громадського порядку.

"Кіберспеціалісти СБУ встановили особу одного з координаторів, який є уродженцем Дніпропетровської області і приєднався до сепаратистів "ДНР"в травні 2014 року", - уточнюється в повідомленні.

За даними фахівців з інформаційної безпеки, використання в якості "тролів" жителів населених пунктів, підконтрольних українській владі, дає кураторам можливість адаптувати матеріал і коментарі під реальну ситуацію.

Слідчі продовжують досудове розслідування по кримінальним виробництвам, розпочатим за ст. 110 (посягання на територіальну цілісність і недоторканність України) Кримінального кодексу України. Інтернет-агітаторам загрожує позбавлення волі на строк від п'яти до десяти років.

30 вересня СБУ блокувала діяльність "ботоферми", яка поширювала неправдиву інформацію.

Її діяльність контролювалася з Росії і "ДНР".

Організатори використовували телекомунікаційні платформи для створення і просування фейкових акаунтів і спільнот. Через них вони поширювали вигадану інформацію з метою дестабілізації ситуації в Україні напередодні місцевих виборів.

Також в січні-серпні 2020 українські правоохоронці відкрили 636 виробництв через завідомо неправдиві повідомлення про загрозу безпеці громадян.

Уточнюється, що правоохоронці закрили 44 виробництва. До суду направили 99 виробництв, в тому числі 87 - з обвинувальним актом.

126 особам повідомили про підозру». ***(У Дніпропетровській області діяла група проросійських інформаційних "тролів" // Дзеркало тижня. Україна (https://zn.ua/ukr/UKRAINE/u-dnipropetrovskij-oblasti-dijala-hrupa-prorosijskikh-informatsijnikh-troliv.html). 06.10.2020).***

***

«Система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала 1 024 429 підозрілих подій. Це на 6% менше, ніж попереднього тижня. Переважна більшість

зафіксованих підозрілих подій стосується спроб мережевого сканування (91%) та застосування нестандартних протоколів (7%).

Система кіберзахисту також заблокувала 62 380 атак різних видів, що на 27% більше, ніж попереднього тижня. Переважна більшість – це мережеві атаки прикладного рівня (95%) та атаки типу «Harvest Attack» (3%). Також зафіксовано і заблоковано 15 DDoS-атак. Переважна більшість стосується веб-ресурсів Офісу Президента України.

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 1 961 кіберінцидент, що на 26% менше, ніж попереднього тижня. Переважна більшість опрацьованих інцидентів стосується недержавного сектору (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (98%).

В разі будь-яких кіберінцидентів, кібератак або підозрілих дій щодо інформаційно-телекомунікаційних систем інформуйте урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA». ***(Державна система кіберзахисту зафіксувала 15 DDoS-атак і понад 1 млн підозрілих подій // Pingvin Pro (https://pingvin.pro/gadgets/news-gadgets/derzhavna-systema-kiberzahystu-zafiksuvala-15-ddos-atak-i-ponad-1-mln-pidozrilyh-podij.html). 20.10.2020).***

***

«Перший заступник міністра закордонних справ України Еміне Джапарова відреагувала на рішення судових властей США висунути звинувачення проти ймовірних співробітників ГРУ, відповідальних у тому числі за кібератаки на енергосистему України…

"Велике федеральне журі у Піттсбурзі (США) звинуватило 6 російських офіцерів ГРУ у зловмисній кібер-активності в усьому світі. Як стверджується, вони несуть відповідальність за цинічні комп'ютерні атаки на електромережний, фінансовий і державний сектори України у 2015-2017 роках. Нехай восторжествує справедливість", - написала Джапарова у Twitter…». ***(Саша Картер. Кібератаки на енергосистему України: МЗС відреагувало на звинувачення російських шпигунів у США // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1898119-kiberataki-na-energosistemu-ukrayini-mzs-vidreaguvalo-na-zvinuvachennya-rosiyskikh-shpiguniv-u-ssha). 20.10.2020).***

***

«Фахівці з кібербезпеки державного концерну "Укроборонпром" з початку року виявили та успішно відбили 38 цільових кібератак на інформаційно- телекомунікаційну систему Концерну…

"Щодня наша система знаходиться під ударом кіберзловмисників. Втім, завдяки удосконаленню нашого серверного обладнання та програмного забезпечення, ми успішно відбиваємо не лише поодинокі напади, але й скоординовані, складні атаки. Лише цього року ми відбили 38 цільових кібератак на електронні поштові скриньки Концерну. У більшості випадків зловмисники намагалися вразити нашу систему за допомогою так званих атак "нульового дня" та

вірусів типу "троян". Втім, безуспішно", - наголосив заступник гендиректора з безпеки концерну Костянтин Бушуєв.

Як зазначається, для посилення кіберзахищеності Укроборонпром пройшов незалежну оцінку Державної служби спеціального зв'язку та захисту інформації України та втілив усі рекомендації, пов'язані з удосконаленням інформаційної системи та програмного забезпечення.

За інформацією пресслужби, дані про всі кібератаки на інформаційні системи Концерну регулярно систематизуються та надсилаються уповноваженим державним інституціям: Ситуаційному центру забезпечення кібербезпеки СБУ та Національному координаційному центру кібербезпеки РНБОУ.

Крім того, для пошуку кращих сучасних практик кіберзахисту фахівці Укроборонпрому проводять консультації з провідними гравцями ринку.

"Атаки на Концерн мають на меті не лише блокування роботи наших систем, але й отримання комерційної інформації про озброєння та військову техніку, які виготовляють наші підприємства для сил безпеки та оборони України, а також іноземних замовників. Кібершпіонаж - явище доволі поширене, але разом із провідними фахівцями з кібербезпеки з приватного сектору ми вже тестуємо пілотний варіант Операційного центру безпеки і незабаром визначимося із найкращим технологічним рішенням для Концерну на наступний рік", - зазначив Бушуєв.

В Укроборонпромі нагадали, що навесні фахівці з кібербезпеки концерну успішно відбили масовану кібератаку типу brute-force, коли було зафіксовано більш ніж мільйон намагань отримати доступ до електронних поштових скриньок працівників Концерну, які надходили з 18 країн Європи. А у липні Укроборонпром виявив та запобіг намірам зловмисників інфікувати інформаційно-телекомунікаційну систему концерну вірусом типу "троян" Trojan.Delf.FareIt.Gen.7». ***(Укроборонпром з початку року відбив близько 40 цільових кібератак // Эксперт-Центр (http://expert.org.ua/armiya/2020/ukroboronprom-z-pochatku-roku-vidbiv-blizko-40-cilovih-kiberatak). 28.10.2020).***

***

«Інтернет-видання Liga.net повідомило, що з 24 жовтня зазнає кібератаки – зараз сайт працює з перебоями.

Хакери влаштували масовану атаку не на сервера Liga.net, а на канал провайдера. У виданні припустили, що атака йде з РФ.

Спершу сайт Liga.net перестав працювати 24 жовтня, о 18:25. «У цей же час адміністратори соціальних мереж Liga.net отримали анонімне повідомлення, яке в загальних рисах описувало технічну суть проблеми, яка сталася з сайтом. Трохи пізніше аноніми повідомили, що цю атаку їм нібито замовили, але вони готові нам допомогти за невелику, регулярну, винагороду», – розповіли в Liga.net та додали, що керівництво видання вирішило не платити зловмисникам.

Технічним фахівцям вдалося відновити роботу сайту 24 жовтня, проте атака відновилася 26 жовтня. «На даний момент технічні фахівці групи компаній Liga.net прикладають максимум зусиль, щоб вирішити проблему. Якщо у вас є змістовні

ідеї, як можна прискорити відновлення роботи сайту, будемо раді вашій допомозі. Пишіть на N.Koteneva@liga.net», – додали в Liga.net…». ***(Liga.net зазнає кібератаки // ДЕТЕКТОР МЕДІА (https://detector.media/infospace/article/181907/2020-10-26-liganet-zaznae-kiberataki/). 26.10.2020).***

***

«Сайт інформаційно-аналітичного видання «Четверта влада» 22 жовтня зазнав DDoS-атаки, яка зупинила роботу ресурсу на кілька годин. Про це в редакції агенції повідомили представниці IMI.

Журналісти припускають, що атака пов'язана із розслідуванням, яке вийшло напередодні – видання написало про кандидата в мери Рівного Віктора Шакирзяна.

«Наша агенція робить розслідування і досьє на кандидатів в міські голови і депутати, яким це не дуже подобається, м'яко кажучи. Не виключаю, що це пов'язано з одним із цих кандидатів, про якого ми опублікували розслідування напередодні, яке підтверджує його зв'язок із людьми, які мали чи мають стосунок до криміналу та корупційних схем», – розповів головний редактор «Четвертої влади» Володимир Торбіч.

Адміністраторка сайту видання Наталія розповіла, що під час атаки зловмисники робили запити на головну сторінку таким способом, щоб оминути кеш сайту і збільшити навантаження. Користувачі в цей час не могли користуватися сайтом, адже він просто не завантажувався.

Пан Торбіч додав, що на проблему доволі швидко відреагували. «Адмін заблокував всі айпі, з яких навантажували сайт, і поставив автоматичну систему захисту від таких атак. Хіба що я втратив кілька годин на розбирання з усім цим і журналісти, які працювали із сайтом, мусили зробити паузу на годинку», – розповів він.

Нагадаємо, увечері 22 лютого 2018 року в місті Рівне підпалили редакцію інформаційно-аналітичного порталу «Четверта влада». Головний редактор Володимир Торбіч вважає, що підпал пов'язаний виключно з професійною журналістською діяльністю. 25 липня правоохоронці повідомили про затримання двох підозрюваних у підпалі «Четвертої влади» та участі в організованій злочинній групі.

Під час слідства справу двічі перекваліфіковували – спочатку провадження було відкрито за ч.1 ст.347 (умисне знищення або пошкодження майна журналіста), потім її змінили на ч.2 ст. 194 (умисне знищення або пошкодження чужого майна), пізніше знов – на ч.1 ст.347». ***(Видання «Четверта влада» зазнало кібератаки після розслідування про кандидата в мери Рівного // vybory.detector.media (https://vybory.detector.media/2020/10/23/vydannya-chetverta-vlada-zaznalo-kiberataky-pislya-rozsliduvannya-pro-kandydata-v-mery-rivnoho/?fbclid=IwAR24o5tU3T6GpDJnq2hjiV2JmaEP0ASopwYqtlnP3whWEriJSxKkoUe0e8A). 23.10.2020).***

***

«Україна закликає міжнародну спільноту продовжити тиск на Російську Федерацію через порушення у кіберпросторі. Про це йдеться в коментарі Міністерства закордонних справ України у зв'язку із заявою державного секретаря США щодо висунення звинувачень посадовцям російського ГРУ в кіберзлочинах. Україна повністю довіряє оприлюдненим мін'юстом США підсумкам розслідування й звинуваченням шести співробітникам генштабу армії РФ у скоєнні кібератак у всьому світі, зокрема в Україні, США, Франції, Грузії та Південній Кореї, йдеться в документі. МЗС повністю підтримує заяву держсекретаря США Майка Помпео про необхідність жорсткого засудження постійної підривної, деструктивної та дестабілізаційної діяльності РФ у кіберпросторі, яка демонструє повну неповагу до громадської безпеки й міжнародної стабільності.

«Звертаємося до міжнародної спільноти із закликом продовжити скоординований тиск на РФ для припинення систематичного порушення з її боку норм та принципів міжнародного права, зокрема у використанні кіберінструментів із зловмисною метою», — заявили в МЗС». ***(МЗС проти кіберзлочинності // Урядовий кур'єр (https://ukurier.gov.ua/uk/news/mzs-proti-kiberzlochinnosti/). 22.10.2020).***

***

Боротьба з кіберзлочинністю в Україні

«СБУ виявила у програмному забезпеченні податкової служби помилку, яка допомагала ухилятись від податків та коштувала бюджету десятки мільярдів.

За словами начальника управління кібербезпеки СБУ Іллі Вітюка, помилку в алгоритм системи моніторингу критеріїв оцінки ризиків при реєстрації податкових накладних внесли спеціально.

«Була спеціально закладена неточність, математична і логічна помилка функціонування системи. Через цю помилку система сприймала незаконні податкові операції, як операцію, яку здійснює великий платник податків. І вона її не блокувати апріорі, тому що вважала, що така компанія не може бути протизаконною», – пояснив фахівець.

Він додав, що СБУ працювала над схемою з весни 2020 року, а наприкінці травня нормальна робота СМОКР була відновлена. Після ліквідації багу держбюджет отримав 22 млрд грн додатково…». ***(У податковій викрили програмний збій, який дозволяв ухилятись від податків // UA.NEWS (https://ua.news/ua/v-nalogovoj-razoblachyly-programmnyj-sboj-kotoryj-pozvolyal-uklonyatsya-ot-nalogov/). 10.10.2020).***

***

«Мошенники не дремлют и уже придумали новый способ, как выманить у людей их потом и кровью заработанные деньги. При этом, им самим ничего делать не приходиться люди сами попадаются на "крючок". Достаточно скачать

фейковое приложение Приват24 и украинцев оставят без копейки. Не дайте себя облапошить, срочно удаляйте приложение!

Аферисты запустили в Интернет фейковое приложение Приват24, которое не имеет никакого отношения к государственному банку, сообщает hyser.com.ua.

Клиентов крупнейший в Украине банк ПриватБанк предупредил, чтобы они не пытались скачивать их приложение на телефон из сомнительных ресурсов. Также стоит помнить, что передача личных данных третьим лицам категорически запрещена. Если вдруг по доверчивости гражданин передаст свои личные банковские данные мошенникам, и он лишится своих денег, вернуть их потом может вообще не получиться.

Специалисты по кибербезопасности наткнулись в Сети на приложение, в котором красочно рассказывается о выгодных кредитах, разыгрываются призы и проводятся розыгрыши якобы от ПриватБанка. Приложение нужно скачать через социальную сеть Instagram.

Наверняка, увидев такие заманчивые предложения доверчивые граждане стали массово скачивать приложение и вводить свои данные от личных кабинетов в системе "Приват24".

В итоге мошенники просто после ввода личных данных воруют у граждан деньги с их счета. На удочку аферистов попали более сотни человек, они обратились в полицию с надеждой вернуть свои деньги.

Пресс-служба ПриватБанка предупреждает, что ни в коем случае не стоит устанавливать на свой смартфон сторонние приложения, скачивать Приват24 нужно с официального сайта или же с других надежных ресурсов…» ***(Не дайте себя облапошить: фейковое приложение Приват24 оставляет украинцев без копейки, немедленно удаляйте // Стена (https://kyiv.ukrainianwall.com/56013-ne-dayte-sebya-oblaposhit-feykovoe-prilozhenie-privat24-ostavlyaet-ukraincev-bez-kopeyki-nemedlenno-udalyayte). 12.20.2020).***

***

«Зловмисники розповсюджували «вірус» та отримували логіни і паролі до різних систем інтернет-банкінгу, акаунтів соцмереж, електронних скриньок громадян. Виявлено більше 100 мільйонів дискредитованих облікових записів користувачів Інтернету.

Працівники кіберполіції в Харківській області спільно зі слідчими слідчого управління поліції Харківщини, під процесуальним керівництвом обласної прокуратури, викрили організовану злочинну групу хакерів, які несанкціоновано втручалися в роботу комп’ютерів та електромереж.

Кіберполіція встановила, що правопорушники, володіючи фаховими знаннями у сфері ІТ, розповсюджували шкідливе програмне забезпечення. Воно давало можливість отримати логіни і паролі до онлайн-сервісів громадян.

За оперативною інформацією, до протиправної діяльності було залучено хакерів з Києва та Харкова, а також осіб, які наразі перебувають в США, Німеччині, Китаї, Росії та В’єтнамі.

Зловмисники отримували логіни та паролі від вебсервісів, які збережені у налаштуваннях браузера. Зазвичай це вхідні дані до різних систем інтернет-

банкінгу, акаунтів соцмереж, електронних скриньок тощо. Після чого, використовуючи логін та пароль жертви, хакери виводили гроші з електронних гаманців, ігрових акаунтів та банкінгу зі спрощеним входом.

Правоохоронці провели обшуки за місцями мешкання фігурантів. За результатами вилучено комп'ютерну техніку, мобільні телефони, банківські картки та гроші. Речові докази направлено на проведення експертних досліджень.

Під час попереднього огляду техніки було виявлено шкідливе програмне забезпечення, відділені сервера, близько 100 мільйонів дискредитованих логінів та паролів до різних систем інтернет-банкінгу, соціальних мереж користувачів українського та міжнародного сегменту мережі Інтернет.

Фігурантам оголошено про підозру у вчинені правопорушень, передбачених за ч. 3 ст. 28, ч. 2 ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Санкція статті передбачає позбавлення волі на строк до шести років. Підозрюваним обрано запобіжний захід - тримання під вартою. Досудове розслідування триває». ***(Кіберполіція викрила злочинну хакерську групу у розповсюдженні шкідливого програмного забезпечення // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-zlochynnu-xakersku-grupu-u-rozpovsyudzhenni-shkidlyvogo-programnogo-zabezpechennya-162/). 09.10.2020).***

***

«У Харкові та Києві викрили групу з трьох осіб, які зламували поштові скриньки та акаунти в соцмережах. Про це повідомляє пресслужба Харківської обласної прокуратури.

За місцем мешкання та роботи фігурантів у Харкові та Києві було проведено 17 обшуків. Правоохоронці виявили та вилучили комп'ютерну техніку, жорсткі диски, мобільні телефони, сім-картки, банківські картки та інші ймовірні докази протиправної діяльності.

Трьом особам повідомили про підозру за фактом несанкціонованого втручання в роботу автоматизованих систем, комп'ютерних мереж організованою групою осіб (ч. 3 ст. 28, ч. 2 ст. 361 КК України). Санкція статті передбачає покарання у вигляді позбавлення волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Наразі вирішується питання щодо обрання запобіжного заходу…» ***(У Харкові та Києві викрили групу осіб, які зламували поштові скриньки та акаунти в соцмережах – прокуратура // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/25693/2020-10-09-u-kharkovi-ta-kievi-vikrili-grupu-osib-yaki-zlamuvali-poshtovi-skrinki-ta-akaunti-v-sotsmerezhakh-prokuratura/). 09.10.2020).***

***

«Служба безпеки України з початку року нейтралізувала 460 кіберінцидентів і кібератак на органи державної влади та критично важливі об'єкти інфраструктури. Також за цей період заблоковано 2,5 тисячі вебресурсів, які використовувалися зі злочинною метою, та діяльність 20 хакерських угруповань. Про це інформує пресслужба органу.

«Серед масштабних спецоперацій, пов'язаних із цифровими сервісами, – викриття несанкціонованого втручання у роботу інформаційно-телекомунікаційних систем Державної податкової служби. Спочатку було викрито незаконну схему формування сум податкових кредитів з ПДВ. Вона щомісяця завдавала до 2 млрд гривень збитків державі. А згодом – викрито конвертцентр з обігом до 15 млрд грн, через який окремі підприємства ухилялися від сплати податків», - йдеться у повідомленні.

Загалом за 9 місяців 2020 року за матеріалами кіберпідрозділів СБУ розпочато 408 кримінальних проваджень. Із них – 106 справ саме за несанкціоноване втручання у роботу комп'ютерів та автоматизованих мереж (ст. 361, 362, 363 Кримінального кодексу України).

За цей період було притягнуто до кримінальної відповідальності 20 громадян і засуджено 3 особи.

«Інший напрям кібербезпеки – протидія ботофермам, які поширюють деструктивний контент, зокрема з РФ. Із січня зусиллями СБУ було нейтралізовано 16 мереж потужністю у понад 60 тисяч ботів. Одну з таких ботоферм, що працювала на замовлення РФ і терористичну «ДНР», оперативники СБУ викрили наприкінці вересня», - зазначили в СБУ.

За інформацією, подібні ботоферми значно активізувалися напередодні місцевих виборів.

Загалом у 2020 році за матеріалами Служби розпочато 42 справи за злочини проти основ національної безпеки, 24 осіб засуджено». ***(Із початку року СБУ нейтралізувала 460 кібератак на держоргани та 20 хакерських угруповань // Судово-юридична газета (https://sud.ua/ru/news/ukraine/182421-z-pochatku-roku-sbu-neytralizuvala-460-kiberatak-i-20-khakerskikh-ugrupovan). 19.10.2020).***

***

«Чоловік за допомогою шкідливого програмного забезпечення зібрав базу логінів та паролів для входу в електронні системи. Далі цю інформацію правопорушник формував у бази та збував через месенджер. Йому загрожує до п'яти років позбавлення волі.

Співробітники кіберполіції Одещини спільно зі слідчими Приморського відділу поліції, під процесуальним керівництвом місцевої прокуратури № 3, викрили місцевого мешканця у несанкціонованому збуті інформації з обмеженим доступом.

Кіберполіція встановила, що до зазначених дій причетний 47-річний чоловік. Він на хакерських ресурсах придбав шкідливе програмне забезпечення та власноруч «удосконалив» його. Шляхом сканування мережі на предмети вразливості та шляхом грубого підбору паролів, чоловік отримував доступ до

інформації з обмеженим доступом. Отриману інформацію він об’єднував у бази та продавав через месенджер.

Правоохоронці провели обшук за місцем мешкання чоловіка та вилучили речові докази: комп’ютерну техніку, флеш-накопичувачі, мобільні телефони, банківські картки, які використовувалась у злочинній діяльності. Усе вилучене направлено на проведення відповідних експертиз.

Фігуранту оголошено про підозру у вчиненні правопорушення, передбаченого ч. 2 ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України. Санкція статті передбачає до п’яти років позбавлення волі. Слідство триває…». ***(Кіберполіція викрила жителя Одещини у викраденні та збуті інформації з обмеженим доступом // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-zhytelya-odeshhyny-u-vykradenni-ta-zbuti-informacziyi-z-obmezhenym-dostupom-2241/). 20.10.2020).***

***

«Слідчі СБУ разом з фахівцями із кібербезпеки блокували у Миколаєві та Івано-Франківську діяльність трьох «ботоферм», через які поширювався деструктивний контент напередодні місцевих виборів. Про це повідомляє пресслужба СБУ.

У Миколаєві оперативники спецслужби встановили, що з початком передвиборчої кампанії зловмисники почали через дві «ботоферми» активно розміщувати матеріали для дискредитації дій державної та обласної влади. Максимальна активізація поширення деструктивних матеріалів планувалась напередодні та безпосередньо в день проведення місцевих виборів.

Зазначається, що для поширення неправдивої інформації вони використовували низку бот-акаунтів. «Ботоферми» забезпечували технічну можливість віддаленої реєстрації облікових записів у загальнодоступних та соціально-орієнтованих ресурсах через російську вебплатформу.

За версією слідства, один із зловмисників також адміністрував у соцмережах групи із загальною аудиторією понад 300 тисяч учасників. Там він розміщував матеріали, які, згідно із висновком лінгвістичної експертизи, містили заклики до зміни меж території чи кордонів України.

«У межах розпочатого кримінального провадження правоохоронці вилучили докази протиправної діяльності фігурантів: комп’ютерну техніку, засоби зв’язку і символіку країни-агресора. Також вилучено обладнання „ботоферм“ — 5 сім-банків на 32 порти кожен, майже 4 тисячі сім-карток операторів зв’язку», — йдеться у повідомленні.

Наразі тривають першочергові слідчі дії, спрямовані на встановлення обставин зафіксованого злочину, а також встановлення можливих зав’язків фігурантів з «кураторами» із спецслужб РФ.

Слідчі органів безпеки готують повідомлення зловмиснику про підозру за ч. 2 ст. 110 Кримінального кодексу України.

Водночас, в Івано-Франківську місцевий мешканець через «ботоферму» упродовж 3 років надавав замовникам послуги зі створення десятків тисяч фейкових профілів у соцмережах та месенджерах.

За оперативними даними СБУ, напередодні місцевих виборів в Україні клієнтами зловмисника стали переважно абоненти з РФ. Вони використовували анонімні профілі для незаконного впливу на громадську думку, поширення неправдивої та деструктивної інформації.

Під час обшуку за місцем роботи зловмисника вилучено 2 VoIP шлюзи, 7 USB-модемів, понад тисячу сім-карток та комп'ютер, з якого він здійснював керування ботофермою.

Розпочато досудове розслідування за ч. 3 ст. 109, ч. 1 ст. 110 Кримінального кодексу України». ***(СБУ заблокувала три «ботоферми», які поширювали передвиборчі фейки // Високий Замок Online (https://wz.lviv.ua/news/422819-sbu-zablokuvala-try-botofermy-iaki-poshyriuvaly-peredvyborchi-feiky). 23.10.2020).***

***

«Ученик 3-го курса профессионального лицея из Черновцов увлекся вопросами компьютерной безопасности. В течение первой половины 2020 года он взламывал крупные онлайн-ресурсы, чтобы получить доступ к учетным записям их пользователей.

Например, первый из описанных в материалах суда эпизодов, заключался во взломе одного из сервисов криптовалютных кошельков, в результате чего хакер получил доступ к данным аккаунтов 10 тысяч пользователей.

Полученные незаконным образом данные с ограниченным доступом, он продал одному из пользователей хакерского форума bhf.io.

Точная сумма сделки неизвестна, но в целом, данный ресурс является трешовой помойкой, на которой относительно недорого можно приобрести краденные игровые аккаунты, бот-аккаунты в социальных сетях и даже персональные ID иностранных граждан. В «умелых руках» такая информация может причинить куда больший ущерб.

Спустя пару месяцев, он выложил на продажу учетные записи пользователей криптовалютной биржи blockchain.com, а также 100 тысяч учетных записей пользователей различных сервисов электронной почты.

Еще спустя пару дней, предприимчивый хакер выставил на продажу около 700 учеток зарегистрированных пользователей сайта американского оператора мобильной связи Verizon. Далее, в течение месяца он взломал и продал данные игроков Minecraft (официальный сайт mojang.com), а также пользователей сервиса Gmail, Amazon и других.

В общей сложности, одаренный ученик профессионального лицея незаконно добыл и реализовал более 1,1 млн учетных записей десятка интернет-ресурсов. Развив такую активную деятельность, молодой человек привлек внимание компетентных органов, в следствие чего, по нему была проведена оперативная разработка.

Киберполиции не составило большого труда выяснить, что в профиле предприимчивого хакера на форуме указан его персональный телеграм-аккаунт,

закрепленный за личным номером телефона. Дальнейшее установление личности анонимуса и поиск места его проживания был всего лишь вопросом времени. Поэтому перед сотрудниками прокуратуры юный гений предстал уже в конце июня.

Пообщавшись с правоохранителями, молодой человек полностью признал свою вину и раскаялся. За несанкционированный сбыт и распространение информации с ограниченным доступом, а также за те же действия, осуществленные повторно с причинением значительного ущерба, ему грозило 3 года на малолетке.

Однако ввиду чистосердечного раскаяния, приговор заменили на 2 года условно, с принудительным посещением исправительной пробационной программы «Изменение криминального мышления». ***(Андрей Майданик. Киберполиция: несовершеннолетний хакер украл и продал более миллиона учетных записей // Internetua (https://internetua.com/kiberpoliciya-nesovershennoletnii-haker-ukral-i-prodal-bolee-milliona-ucsetnyh-zapisei). 21.10.2020).***

***

«Суд приговорил к двум годам тюрьмы украинца за установку нелицензионного программного обеспечения на компьютеры пользователей…

Орджоникидзевский районный суд города Мариуполя установил, что обвиняемый в сентябре 2019 года с целью получения вознаграждения устанавливал и активировал с помощью специального ПО лицензионный продукт "ArchiCAD 20", авторские права на который принадлежат компании "Graphisoft SE" (Венгрия), тем самым нанеся материальный ущерб компании на сумму 3850 евро.

Таким образом подсудимый совершил умышленное нарушение авторского права, а именно незаконное воспроизведение компьютерных программ и несанкционированное вмешательство в работу автоматизированной системы, что привело к искажению процесса обработки информации, то есть преступления предусмотренные ч.1 ст.176 УК Украины и ч.1 ст. 361 УК Украины.

В судебном заседании обвиняемый вину в инкриминируемом уголовном правонарушении признал полностью.

Суд признал мужчину виновным в совершении уголовного правонарушения, предусмотренного ч.1 ст.176 УК Украины и ч.1 ст.361 УК Украины и назначил наказание в виде 2 лет лишения свободы с испытательным сроком один год.

Также подсудимый должен оплатить в пользу государства расходы на проведение экспертиз в сумме 1884 грн. 12 коп». ***(Артем Сереженок. Украинец получил два года тюрьмы за установку нелицензионного ПО на компьютеры пользователей // Internetua (https://internetua.com/ukrainec-polucsil-dva-goda-tuarmy-za-ustanovku-nelicenzionnogo-po-na-kompuatery-polzovatelei). 23.10.2020).***

***

«Кіберфахівці Служби безпеки України блокували продаж на хакерському форумі персональних даних громадян напередодні місцевих виборів.

Співробітники СБ України встановили, що на одному із спеціалізованих хакерських форумів зловмисник пропонував придбати базу даних, яка за багатьма ознаками співпадає з інформацією, що зберігається в АІТС «Державний реєстр виборців». Дані із зазначенням місця проживання та номерів виборчих дільниць користуються великим попитом у «даркнеті» напередодні проведення виборів до органів місцевого самоврядування. Адже ця інформація може бути використана замовниками для впливу на електоральні вподобання виборців.

Оперативники СБУ встановили особу зловмисника та провели низку слідчих дій. Правоохоронці вилучили комп'ютерну техніку та засоби зв'язку із доказами протиправної діяльності.

Наразі встановлюються всі обставини злочину та перелік «клієнтів», що придбали персональні дані виборців. Вирішується питання щодо повідомлення зловмиснику про підозри за ст. 361-2 (несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України.

Триває досудове слідство». ***(У Дніпрі СБУ блокувала продаж персональної бази даних громадян напередодні місцевих виборів // Служба безпеки України (https://ssu.gov.ua/novyny/u-dnipri-sbu-blokuvala-prodazh-personalnoi-bazy-danykh-hromadian-naperedodni-mistsevykh-vyboriv). 22.10.2020).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Європейський Союз продовжить допомагати Україні протидіяти поширенню дезінформації, зокрема, з боку Росії.

Про це йдеться у заяві за підсумками саміту Україна-ЄС в Брюсселі…

«Європейський Союз продовжуватиме підтримувати Україну у протидії гібридним загрозам та у боротьбі з дезінформацією, в тому числі шляхом посилення незалежних ЗМІ, стратегічної комунікації щодо медіаграмотності, з метою зміцнення стійкості України», - сказано у тексті заяви.

В документі окремо підкреслюється, що дезінформаційні кампанії проти ЄС та Україні здійснюються з боку Росії.

Крім того, ЄС дав згоду започаткувати з Україною формат діалогу з питань кібербезпеки. Зараз ЄС має такий формат лише з шістьма найвагомішими державами, Україна буде сьомою». ***(ЄС продовжить допомагати Україні боротись з російськими фейками // Чорноморські новини (https://www.blackseanews.net/read/169094). 07.10.2020).***

***

«Заступник Міністра енергетики України з питань європейської інтеграції Ярослав Демченков провів нараду із міжнародними компаніями-лідерами у сфері кібербезпеки та цифрових трансформацій.

Участь у нараді взяли представники таких провідних компаній, як: CISCO, HEWLETT PACKARD ENTERPRISE, DELL, TRENDMICRO, MCAFEE, MICROFOCUS, FORTINET, HUAWEI, MICROSOFT, PALO ALTO NETWORKS.

Команда Міністерства вже розпочала роботу із гармонізації законодавства у сфері енергетичної кібербезпеки. Формується політика з кібербезпеки, яка має забезпечити належний рівень захисту енергетичного сектору України відповідно до рекомендацій та вимог ЄС. Цю ініціативу підтримують міжнародні партнери розвитку – USAID, British Council, Європейська Комісія, Світовий банк, ЄБРР тощо.

У Міненерго провели три донорські конференції і отримали попередні пропозиції технічної допомоги за напрямками розбудови кібербезпеки, які відповідають узгодженому баченню Міністерства, Energy Community та національних стейкхолдерів, представники яких є членами Робочої групи.

Ярослав Демченков, висловив подяку суб'єктам галузі у сприянні розвитку кіберзахисту об'єктів критичної інфраструктури, а також закликав учасників наради до конкретних заходів, спрямованих на розбудову кіберзахисту об'єктів критичної інфраструктури енергетичної галузі.

Співпраця з міжнародними компаніями – лідерами у сфері кібербезпеки та цифрових трансформацій на початкових етапах ініціативи є загальноприйнятою європейською практикою. У Міненерго особливо цінують, що до роботи Робочої групи долучились представники таких відомих компаній.

Окрему увагу було приділено обговоренню питання підготовки фахівців у сфері кіберзахисту, а саме створення на базі профільних інститутів навчальних курсів для фахівців галузі за напрямом «Забезпечення кібербезпеки об'єктів критичної інфраструктури енергетичної галузі», оскільки питання професійного кадрового забезпечення стоїть дуже гостро не лише у галузі, а й в Україні в цілому.

Залучення міжнародного досвіду впровадження сучасних систем кібербезпеки в енергетичному секторі в інших країнах, організація процесів та підготовка персоналу із суворою відповідністю всім стандартам є надзвичайно важливим і дозволить значно прискорити процеси розбудови кібербезпеки та цифрових трансформацій в енергетичній галузі України». ***(У Міненерго триває робота над підвищенням рівня кібербезпеки енергетичного сектору України // Офіційно (https://oficiyno.com.ua/2020/10/19/u-minenergo-trivae-robota-nad-pidvishchennjam-rivnja-kiberbezpeki-energetichnogo-sektoru-ukrajini-42154/). 19.10.2020).***

***

«Державна служба спеціального зв'язку та захисту інформації України підписала меморандум з компанією "Хуавей Україна" співпраці у сферах кібербезпеки, кіберзахисту і телекомунікацій.

"Ми готові тісно співпрацювати з компанією "Хуавей" для забезпечення і підвищення кіберзахисту і кібербезпеки в Україні. Держспецзв'язку глибоко цінує, що компанія світового рівня працюватиме з нами над проектами у сфері безпеки інформації. Переконаний, що наша взаємодія зміцнить обороноздатність держави

перед кіберзагрозами", - зазначив глава Держспецзв'язку Юрій Щиголь, якого цитує прес-служба.

На думку підписантів, меморандум також відкриває нові можливості для реалізації спільних наукових проектів, навчання і підвищення кваліфікації кадрів у сферах кібербезпеки, кіберзахисту й телекомунікацій.

"Ми впевнені, що через взаємодію держави та приватного сектора можна побудувати ефективну систему кіберзахисту в Україні", - зазначив директор "Хуавей Україна" Ма Ці…» ***(Держспецзв'язку співпрацюватиме з "Хуавей" в питаннях кібербезпеки // iPress(https://ipress.ua/news/derzhspetszvyazku_spivpratsyuvatyme_z_huavey_v_pytannyah_kiberbezpeky_314560.html). 16.10.2020).***

***

«Україна та Словенія провели перші в історії двосторонніх відносин міжвідомчі кіберконсультації. Про це повідомляє пресслужба МЗС України…

“23 жовтня 2020 року під головуванням заступника міністра Василя Боднара та Державного секретаря МЗС Словенії Тоне Кайзера відбулися перші в історії двосторонніх відносин міжвідомчі українсько-словенські кіберконсультації у режимі відеоконференції”, — йдеться в повідомленні.

Зазначається, що до складу української делегації увійшли представники Національного координаційного центру кібербезпеки, Служби безпеки, Міністерства оборони, Департаменту кіберполіції, Служби зовнішньої розвідки та Державної служби спеціального зв’язку і захисту інформації.

Делегація Словенії, у складі представників Міністерства закордонних справ, Адміністрації з питань інформаційної безпеки та Національного центру реагування на кіберінциденти, ознайомила українських колег із причетних органів державної влади із досягненнями Словенії у моніторингу та нейтралізації проблем кібернетичного характеру, а також із стратегією кібербезпеки цієї держави.

“Сторони обговорили сучасні тенденції у сфері кібербезпеки, основні механізми її зміцнення, а також перспективні напрями подальшої співпраці обох держав у зазначеній галузі. Українська сторона ознайомила словенських колег із окремими аспектами масштабних кібератак на електронні та урядові ресурси нашої держави з боку Російської Федерації упродовж 2014-2020 років, відзначивши, що кібератаки, підтримувані та фінансовані РФ, стали одним із головних елементів „гібридної війни“ проти України”, — повідомили в МЗС України.

Додається, що окремою темою консультацій стала співпраця України та Словенії у посиленні глобальної кібербезпеки на майданчиках таких міжнародних організацій, як НАТО, ОБСЄ і ООН. Делегації також обговорили посилення взаємодії у секторах кібербзахисту держав». ***(Наталія Затуливітер. Україна та Словенія провели перші в історії кіберконсультації // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1898856-ukrayina-ta-sloveniya-proveli-pershi-v-istoriyi-kiberkonsultatsiyi). 24.10.2020).***

***

«Заступник міністра закордонних справ України Василь Боднар обговорив з послом Японії Такаші Кураі питання ядерного роззброєння, протидію кіберзагрозам та співпрацю у безпековій сфері.

…про це повідомляє пресслужба МЗС…

За даними МЗС, співрозмовники домовилися продовжити практику проведення українсько-японських консультацій у сфері протидії кіберзагрозам, а також зміцнювати взаємодію в оборонній та безпековій галузях». ***(Україна і Японія обговорили спільні кроки до вільного від ядерної зброї світу // Укрінформ (https://www.ukrinform.ua/rubric-polytics/3124667-ukraina-i-aponia-obgovorili-spilni-kroki-do-vilnogo-vid-adernoi-zbroi-svitu.html). 27.10.2020).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Исследователи безопасности из компании Interstrust проанализировали 100 общедоступных мобильных приложений для iOS и Android в сфере здравоохранения по таким категориям, как телемедицина, медицинское оборудование, торговля и отслеживание распространения коронавирусной инфекции. Они выявили следующие моменты:

— 91% приложений имеют неправильное/слабое шифрование;

— 85% COVID-приложений допускают утечки данных;

— 83% обнаруженных угроз высокого уровня можно было бы смягчить с помощью таких технологий защиты приложений, как обфускация кода, обнаружение несанкционированного доступа и криптография белого ящика;

— 71% приложений имеют по крайней мере одну уязвимость высокого уровня безопасности.

Кроме того, большинство мобильных приложений для здравоохранения содержат множество проблем безопасности хранения данных. Например, 60% протестированных Android-приложений собирают информацию в SharedPreferences, оставляя незашифрованные данные доступными для чтения и редактирования злоумышленникам и вредоносным приложениям.

Все 100 приложений были проанализированы с использованием ряда методов статического тестирования безопасности приложений (SAST) и динамического тестирования безопасности приложений (DAST), основанных на рекомендациях по безопасности мобильных приложений проекта OWASP…». ***(85% анти-COVID-приложений допускают утечки данных // РосКомСвобода (https://roskomsvoboda.org/64709/). 02.10.2020).***

***

«Из-за пандемии мировые технологические лидеры также вынуждены были переместить в виртуальное пространство свои ключевые масштабные конференции и партнерские мероприятия, которые обычно посещают сотни и тысячи людей. Не стала исключением и корпорация IBM, которая в начале мая

провела в режиме онлайн свой ежегодный саммит, задавший тон череде региональных мероприятий.

По традиции в Украине главная конференция IBM проходит в начале бизнес-сезона. Только в этот раз Think Digital Summit Kyiv впервые собрал гостей в новом формате. Посетители виртуального форума получили возможность посмотреть выступления технических экспертов самой корпорации, а также ее партнеров и заказчиков. В рамках четырех тематических потоков, трех десятков презентаций и нескольких панельных дискуссий обсуждались пути повышения надежности ИТ и обеспечения непрерывности бизнеса в современных непростых условиях, ускорения внедрения новых стратегий, трансформации ИТ-инфраструктуры ради сохранения конкурентоспособности, а также защиты цифровых активов предприятия от актуальных киберугроз.

Открывая конференцию, Богдан Хорощак, генеральный директор «IBM Украина», отметил, что в 2020 г. бизнес и организации оказались в условиях, побуждающих ускорить процессы цифровой трансформации. Пандемия стала точкой принятия решений, которые до последнего момента откладывались многими компаниями. Изменения, что в нормальных условиях должны были происходить на протяжении лет, некоторые украинские компании вынужденно проходили за месяцы.

Между тем, нет худа без добра. Корона-кризис лишний раз подтвердил, что использование ИТ-технологий является конкурентным преимуществом. Во время карантина чаще всего имел место один из трех типовых сценариев. Некоторые компании не действовали и теряли конкурентные преимущества. Поскольку не были готовы к вызовам и не понимали, как именно переводить свой бизнес в онлайн. Другие приложили неимоверное количество усилий, чтобы за очень короткое время адаптироваться к новым условиям и изменить бизнес-модель. Также были предприятия, которые еще до кризиса сделали выбор в пользу цифровой трансформации. Последние спокойно пожинали плоды своей дальновидности.

Используя, в том числе разработки IBM, организации по всему миру имеют возможность несмотря ни на что развивать свои партнерские отношения, управлять удаленными командами и помогать работникам осваивать актуальные навыки. Розничные торговцы с помощью гибридных облачных решений могут поддерживать системы в рабочем состоянии в условиях перемещения множества заказов в онлайн. Личная информация пациентов остается конфиденциальной, даже когда врачи консультируют дистанционно. Цепочки поставок совершенствуются, упрощая доставку товаров в магазины. Искусственный интеллект и цифровые ассистенты помогают работникам оставаться продуктивными и эффективнее обслуживать клиентов.

Это яркий пример того, как лидеры думают на опережение, инвестируя в правильные стратегии для своих компаний. Открытость новым технологиям позволяет держать руку на пульсе при любых обстоятельствах. Подтверждением этого тезиса можно считать и сам IBM Think Digital Summit Kyiv, по воле обстоятельств переместившийся в виртуальное пространство.

Программа саммита включала четыре тематических кампуса, посвященные кибербезопасности, облачным технологиям и искусственному интеллекту, инфраструктурным решениям IBM и технической сессии для разработчиков.

Актуальную проблематику в области кибербезопасности обозначил Андрей Кузьменко, лидер подразделения IBM Security в Украине. Он констатировал, что сегодня руководители и специалисты отделов информационной безопасности пребывают в состоянии перманентного стресса. Им приходится параллельно заниматься множеством задач – внедрять решения, имплементировать политики, процедуры и стандарты, планировать бюджеты и стратегию развития ИБ, координировать ее с развитием бизнеса, справляться с огромным количеством уведомлений от различных систем и запросами от регуляторов. При этом помимо стандартных задач необходимо также находить время для работы на перспективу.

Так, например, по оценкам IBM и RedHat, подавляющее большинство приложений в ближайшие годы будут перенесены в контейнеры. И это порождает новые вызовы. Последние 10 лет специалисты занимались защитой, разбирались с SDLC (Software Development Life Cycle – жизненный цикл разработки ПО) и определяли место безопасности в нем. А теперь весь мир взялся переходить к контейнерам. Хотя у многих нередко до сих пор не до конца решены более простые задачи кибербезопасности.

Следующая проблема – данные. С имеющимися базами работают не только внутренние бизнес-аналитики или администраторы. Доступ к определенным срезам может потребоваться отделу маркетинга и PR, внешним подрядчикам, оказывающим те или иные аналитические услуги. И задачаимплементировать ИБ предоставить всем минимально необходимые для их работы привилегии, обеспечить мониторинг и плюс к этому выполнять требования регуляторов.

Наконец, инфраструктура. У подразделения IBM Security в Украине уже сейчас довольно много клиентов, у которых более половины всей вычислительной нагрузки приходится на облако. Обеспечение безопасности такой гибридной инфраструктуры также имеет свою специфику.

Вокруг этих направлений и был сформирован поток кибербезопасности. Причем организаторы стремились сделать акцент не на технических презентациях отдельных продуктов и сервисов, а на выступлениях партнеров и клиентов, которые делились опытом внедрения и использования тех или иных решений.

Тему построения безопасной микросервисной архитектуры развил Алексей Иванов, архитектор решений Red Hat. Он начал свою презентацию с утверждения, что приложения должны приносить компаниям прибыль, через реализацию заданной бизнес-логики. Однако традиционные подходы их создания имеют ряд недостатков. Среди которых длительный цикл разработки, развертывания и ввода в продуктивную эксплуатацию, сложность внесения изменений и пр. Кроме того, имеет место противоречие между командами разработки и администрирования, а также безопасности, относительно развития необходимой инфраструктуры для развертывания приложения и их свойств.

Решить эти противоречия хотя бы отчасти призваны контейнеры. Они объединяют все необходимые компоненты в одном файле. Благодаря чему достигается большая портативность, меньшее, чем у виртуальных машин,

потребление ресурсов и скорость запуска. В тоже время для автоматизации развертывания, масштабирования и управления большим количеством контейнеров нужна соответствующая платформа.

Одну из реализаций Kubernetes для корпоративного использования являет собой Red Hat OpenShift. Продукт развивается уже пять лет и работает одинаково в любом крупном облаке, а также локально. За это время его пользователями стали более 1700 компаний по всему миру.

По сути OpenShift 4 объединяет контейнерную платформу и операционную систему Red Hat CoreOS. Последняя представляет собой усеченный Red Hat Enterprise Linux, из которого убрали все лишнее, ненужное для работы с контейнерами. Это позволило в числе прочего существенно обезопасить ОС и уменьшить количество потенциальных векторов атаки. Причем в системе защищается не только хост от контейнеров, но и контейнеры друг от друга.

Три стандартных компонента, которые есть в каждом Linux и при правильном их использовании позволяют сделать ОС более безопасной – это SELinux (принудительный контроль доступа), Seccomp (ограничение системных вызовов) и root capabilities (привилегии суперпользователя).

Далее докладчик рассмотрел детальнее ряд сервисов платформы OpenShift для разработчиков и дал несколько базовых рекомендаций по созданию безопасной среды контейнерных приложений.

О возможностях оптимизации ЦОД и экономии ИТ-бюджетов за счет консолидации серверов на базе IBM Linux One рассказал Игорь Сорокин, лидер по продажам Z и LinuxOne в Центральной и Восточной Европе и СНГ. Аппаратная платформа Linux One непрерывно развивается с 1999 г. Это универсальное решение для ЦОДов, разработанное в соответствии с тенденциям в области оптимизации, плотности и гибкости. Модульные масштабируемые системы, включающие до четырех 19 дюймовых стоек, созданы для сокращения места, занимаемого в ЦОДе, и позволяют заменить большое количество устаревших x86 серверов. При этом актуальная линейка дополнительно обеспечивает рост производительности на 25% относительно семейства z14.

Конфигурация выбирается в зависимости от задач заказчика и может включать от 4 до 100 процессорных ядер и от 2 до 40 ТБ оперативной памяти. Внутри стойки расположены процессорные полки, радиатор, питание, ввод\вывод и коммутаторы. Все достаточно стандартно, сервер на поддержке и самой организации для его обслуживания не требуются специалисты высокой квалификации.

LinuxOne обеспечивает высокую производительность как для традиционных нагрузок, так и Open Source. Например, поддерживаются базы данных DB2, Oracle, MongoDB, MariaDB, Liberty и т.п. Консолидация подразумевает объединение на платформе LinuxOne значительного количества «железа». За счет этого снижается количество ядер и соответственно лицензионные выплаты за корпоративное ПО. Ведь, к примеру, Oracle лицензируется по ядрам, как и количество опций, плюс поддержка. Опыт заказчиков IBM разного масштаба из разных индустрий показывает, что средняя экономия по совокупной стоимости владения LinuxOne в пятилетнем периоде в сравнении с альтернативой на базе x86 составляет 47%

(разброс – от 15 до 80%). Причем, как правило, наиболее весомой частью в TCO является именно программное обеспечение.

За счет чего достигается сокращение количества ядер? В чем ключевая архитектурная разница IBM LinuxOne по сравнению с альтернативной платформой? В первую очередь дело в процессоре, тактовая частота которого составляет 5,2 ГГц, что в среднем вдвое выше конкурирующего предложения. Далее управление рабочей нагрузкой, утилизация процессора и всей платформы. LinuxOne утилизирует процессор на 80-90%. В то время, как средняя загрузка на сервере Intel x86, по данным докладчика, составляет 10-20%.

При этом еще и обеспечивается высокая надежность уровня шесть девяток. Внутри системы все дублируется. Если, к примеру, на площадке работает два Intel сервера, то при падении одного из них второй может подхватить нагрузку, а в случае проблем с площадкой есть еще и третий сервер в другом ЦОДе. В случае LinuxOne аналогичный результат достигается с помощью двух серверов – по одному на каждой площадке.

Таким образом, IBM LinuxOne благодаря высокому коэффициенту консолидации, который в зависимости от платформы составляет от 1 к 10 до 1 к 30, позволяет бизнесу получать выгоду за счет экономии на лицензиях и поддержке ПО, сокращения расходов на электроэнергию и экономии места в ЦОДе. К тому же, серверы вертикально масштабируемые и в период пиковых нагрузок дополнительно необходимые ресурсы можно получить в течение часа посредством изменения микрокода и включения в работу ресурса, который уже присутствует на процессорной полке.

Последние годы все более актуальной для многих розничных бизнесов становится тема чат-ботов. Преимуществам создания виртуального ассистента (ВА) с искусственным интеллектом на платформе Watson Assistant посвятил презентацию Сергей Данилюк, бизнес-аналитик Global Business Services.

За последние два десятилетия, буквально на наших глазах, произошла революция в коммуникациях. Если поначалу мобильные телефоны использовались преимущественно для голосового общения и отчасти для обмена текстовыми сообщениями, то сегодня последний составляет более половины общего объема, за ним следуют социальные сети и лишь около десятой части отводится традиционным звонкам. Это произошло в первую очередь из-за изменения образа жизни.

По некоторым данным, молодежь сегодня обменивается в среднем 67 текстовыми сообщениями в день. Американцы затрачивают на текстовые коммуникации впятеро больше времени, чем на голосовые звонки. Только через WatsApp и Facebook Messenger передается около 240 млрд. сообщений в год.

Широкое распространение обмена текстовыми сообщениями меняет также коммуникации клиентов с бизнесом. И последний немало теряет, если не использует в полной мере данный канал взаимодействия. Согласно опросам, трое из десяти потребителей услуг предпочли бы отказаться от телефонных звонков в пользу обмена сообщениями. Более 70% пользователей утверждают, что используют смартфоны для переписки больше, чем для разговоров.

Очевидно, что пандемия только усилит эту тенденцию, а ключевым фактором преобразований в обозримой перспективе станет автоматизация взаимодействия. Ведь виртуальные помощники создаются в первую очередь для обслуживания клиентских запросов. Создав ВА один раз, его можно разворачивать на нескольких платформах для получения омниканального клиентского опыта со схожей логикой. Причем в отличие от живых операторов, ВА способен оказывать клиентам поддержку 24x7x365.

По статистике 70-80% всех обращений в контакт-центры – это типовые повторяющиеся запросы. Поэтому их достаточно легко автоматизировать с помощью ВА, освобождая операторов для решения более сложных вопросов и экономя ресурсы. Такой подход позволяет снизить операционные расходы контакт-центров с одновременным улучшением клиентского опыта.

Также ВА могут использоваться внутри компании для получения консультаций, информации по отдельным продуктам и сервисам, доступа к документам по внутренней нормативной базе и пр. Кроме того, чат-боты позволяют автоматизировать отдельные процессы в области HR, ИТ и бухгалтерии.

Watson Assistant – это основанная на ИИ платформа для работы с пользовательскими запросами. Она помогает создавать ВА, быстро и точно предоставлять ответ в любом приложении, либо канале. Причем благодаря ИИ такой цифровой помощник может находить ответы в разных источниках, а также понимает когда нужно уточнить запрос или перенаправить клиента на оператора. Его можно развернуть в любом облачном или локальном окружении.

В общей сложности в рамках четырех тематических сессий виртуального IBM Think Digital Summit Kyiv 2020 вниманию слушателей было представлено три десятка презентаций и две панельные дискуссии. Ознакомиться с материалами конференции желающие могут до конца года, зарегистрировавшись на сайте. Участие в мероприятии дистанционно приняли около 300 человек – представители партнеров и заказчиков, технические специалисты, руководители департаментов ИТ, ИБ и разработки, управленцы». ***(Евгений Куликов. Технологии выживания // Компьютерное Обозрение (https://ko.com.ua/tehnologii_vyzhivaniya_134758). 09.10.2020).***

***

«Карантин, введений у низці країн через пандемію коронавірусу, повністю змінив наше буденне життя. Бізнес теж почав функціонувати по-новому: наприклад, сьогодні хмарні технології використовують навіть ті компанії, які до пандемії взагалі їх не визнавали. Водночас зловмисники теж користуються ситуацією і розробляють усе продуманіші стратегії кібератак.

За словами аналітика інвестиційної компанії "Фрідом Фінанс" Ансара Абуєва, віддалена робота, усенародний страх і тривога відкрили нові можливості для хакерів. Що відомо про кібератаки в період пандемії та про інвестиційні можливості на ринку хмарних технологій та інформаційної безпеки – читайте на Інвестиції24.

Трохи статистики

Ансар Абуєв наводить дані Інтерполу, згідно з якими з січня по квітень цього року кількість випадків інтернет-шахрайства зросла на 59%, зараження шкідливим програмним забезпеченням – на 36%, обсяг фейкових новин - на 14%. У дослідженні організації також йдеться про побоювання щодо погіршення ситуації з хакерськими атаками та поширенням неправдивої інформації в мережі.

Окрім того, люди, які вже тривалий час працюють з дому, уже звикли й не дуже хочуть повертатися в офіс. Зокрема, у Великій Британії провели опитування, результати якого свідчать, що 90% працівників задоволені дистанційною роботою і не хочуть повертатися до офісного режиму.

Найпоширеніші цілі хакерів

Згідно з даними компанії McAfee, яка спеціалізується на розробці антивірусних програм, найбільше від дій кіберзлочинців страждають корпоративні облікові записи, хмарний сервіс Microsoft 365, персональні комп'ютери працівників та їхні телефони.

Наприклад, фішинг переважно застосовувався для розсилки листів про коронавірус від медичних закладів та влади.

Також хакери використовували домени, які повністю копіювали зовнішній вигляд сайту того чи того банку. Відповідно, зловмисники могли отримувати персональні дані клієнтів цих фінустанов.

Окрім того, сьогодні розповсюджується чимало фейкової інформації, яку зловмисники поширюють у месенджерах. Часто неправдиві відомості опиняються і на сайтах ЗМІ, у повідомленнях відомих блогерів.

Кібербезпека й інвестиції: як це взаємопов'язано

Зростання кіберзлочинів змушує задумуватися над новини способами захисту. Відповідно, компанії, які працюють у сфері кібербезпеки, поліпшують свої технології, розробляють надійніше програмне забезпечення для захисту і корпоративних систем, і персональних комп'ютерів.

Експерт "Фрідом Фінанс" стверджує, що сьогодні продовжують зростати обсяги інвестицій у глобальні продукти й послуги, пов'язані з кібербезпекою попри те, що загалом капітальні витрати бізнесу останнім часом значно знизилися. Тобто інвестори зацікавлені акціями розробників хмарних рішень, антивірусів та іншого ПЗ, пов'язаного з кібербезпекою.

Ось кілька прикладів таких компаній, які наводить Ансар Абуєв. Саме на їхні акції слід звернути увагу інвесторам.

Crowdstrike (тікер CRWD)

Станом на сьогодні, американська компанія принесла інвесторам чотирикратних дохід. Підприємство надає послуги захисту кінцевих точок – ноутбуків, планшетів, смартфонів, які підключені до робочих сервісів. Тобто послуги компанії актуальні для організацій, які перевели своїх працівників на віддалений режим роботи.

За даними аналітика "Фрідом Фінанс", потенціал зростання акцій Crowdstrike – 15,8% (цільова ціна становить 160 доларів).

FireEye (FEYE)

Постачальник ПЗ для захисту від кібератак. Свій продукт надає як корпоративному сектору, так і державним структурам. Послуги й розробки FireEye

актуальну завжди: зі зростанням кількості кібератак = збільшується попит на сервіс підприємства.

У "Фрідом Фінанс" заклали потенціал зростання акцій компанії на рівні 33% (цільова вартість одного активу – 16,3 долара).

Cloudflare (NET)

Ще одна американська технокомпанія, яка надає послуги безпеки під час перегляду/отримання контенту, за допомогою яких можна захистити вебсторінки та мобільні додатки від кібератак. Сервіс підприємства використовують 27 мільйонів вебсайтів.

Потенціал зростання, за даними Ансара Абуєва, 20% (цільова вартість акції – 46,7 долара).

OKTA (OKTA)

Компанія займається захистом паролів і даних користувачів під час їхнього входу в особистий обліковий запис.

Потенціал зростання активів підприємства – 14%, а цільова ціна однієї акції – 235 доларів.

Zscaler (ZS)

Ще одна "хмарна" компанія, що надає послуги інформаційної безпеки. Її потенціал зростання у "Фрідом Фінанс" оцінюють на рівні 10% (цільова ціна акції – 148,62 долара).

ВООЗ вважає, що коронавірус ніколи не буде повністю знищений і стане частиною нашого життя. Поки достеменно невідомо, до чого в підсумку призведе пандемія, але це не скасовує того факту, що кібербезпека завжди буде важливою у сучасному житті. Можливо, в майбутньому витрати урядів на кіберзахист переважать витрати на озброєння своїх армій, але це вже буде інша історія, – додав аналітик "Фрідом Фінанс" Ансар Абуєв». ***(Як розвивається сфера кібербезпеки в реаліях 2020 року: тренди та гравці ринку // Телеканал новин «24» (https://investment.24tv.ua/kiberbezpeka-2020-yak-rozvivayetsya-trendi-gravtsi-novini-sogodni_n1429219). 05.10.2020).***

***

«Для формирования отчёта были опрошены более 500 канадских специалистов в области информационной безопасности.

Во время опроса треть респондентов заявила о кибератаках на их организации с использованием проблемы COVID-19. Среди средств атаки были выявлены фейковые приложения для отслеживания контактов и фишинговые атаки якобы с результатами теста на коронавирус.

Около 30% организаций заявили о всплеске атак с момента начала пандемии.

Чуть больше 50% организаций заявили о внедрении новых методов защиты.

Около четверти организаций заявили, что за год подвергались атакам и теряли данные своих сотрудников или клиентов. Ещё 38% организаций не уверены, подвергались ли они кибератакам.

Как утверждают исследователи, ситуация будет только ухудшаться. Только треть сотрудников ожидает увеличения человеческого ресурса в области кибербезопасности. Также около 10% сотрудников ожидают уменьшение

финансирования вопросов кибербезопасности». ***(Более четверти сотрудников канадских IT-компаний утверждают, что их организации подверглись кибератакам из-за COVID-19 // SecureNews (https://securenews.ru/more-than-a-quarter-of-canadian-it-employees-say-their-organizations-have-been-cyberattacks-due-to-covid-19/). 07.10.2020).***

***

«Атака на eResearchTechnology потенциально замедлила исследования коронавируса во всем мире, и исследователи предполагают, что за инцидентом может стоять субъект из национального государства.

Атака программ-вымогателей поразила eResearchTechnology, компанию по производству медицинского программного обеспечения, которая снабжает фармацевтические компании инструментами для проведения клинических испытаний, включая испытания вакцин против COVID-19. Исследователи предполагают, что злоумышленники могут иметь финансовую мотивацию - или их может поддержать национальное государство, стремящееся получить конкурентное преимущество.

Согласно сообщениям, кибератака на компанию из Филадельфии замедлила эти испытания за последние две недели, поскольку исследователи были вынуждены перейти на ручку и бумагу для отслеживания данных о пациентах.

ERT на своем веб-сайте отмечает, что ее программное обеспечение используется во всем мире в испытаниях лекарств и что оно участвовало в отслеживании 75 процентов испытаний на одобрение лекарств, проведенных FDA в прошлом году. Он не раскрывает, сколько из его клиентов пострадали от атаки вымогателя или какой штамм вымогателя виноват.

Однако, согласно New York Times, которая опубликовала эту историю на выходных, IQVIA и Bristol Myers Squibb были вовлечены в инцидент. Первый является подрядчиком, помогающим AstraZeneca в испытании вакцины против COVID-19, а второй производитель лекарств возглавляет совместные усилия по разработке лучшего экспресс-теста на вирус.

Оба заявили изданию, что благодаря резервным копиям данных влияние атаки было ограниченным. Однако другим клиентам ERT повезло меньше.

Дрю Бустос, вице-президент ERT по маркетингу, подтвердил СМИ, что атаки начались 20 сентября, после чего системы были отключены. По его словам, компания сейчас находится в режиме восстановления, и угроза «сдерживается», поэтому ERT постепенно возвращает системы в рабочее состояние.

Pfizer и Johnson & Johnson, обе из которых работают над вакциной COVID-19, объявили, что атака не повлияла на их испытания. Между тем IQVIA опубликовала заявление, в котором отметила: «Нам не известны какие-либо конфиденциальные данные или информация о пациентах, относящихся к нашим клиническим исследованиям, которые были удалены, скомпрометированы или украдены».

«Медицинские организации являются основной мишенью для программ-вымогателей, поскольку они содержат конфиденциальные данные о пациентах», - сказал Джеймс Маккуигган, защитник осведомленности в KnowBe4, по

электронной почте. «Для крупных прибыльных организаций киберпреступники знают, что у них есть средства для выплаты выкупа после кражи их данных. К сожалению, киберпреступники крадут интеллектуальную собственность, чтобы продать ее с аукциона в даркнете, чтобы увеличить свою финансовую прибыль от атаки».

Хотя неясно, какова в конечном итоге мотивация этой атаки с использованием программ-вымогателей, известно, что атаки на организации, ведущие медицинскую борьбу с пандемией коронавируса, продолжаются. В марте Всемирная организация здравоохранения стала мишенью для шпионских бригад, которые искали информацию о реакции на коронавирус; а в мае ФБР и Министерство внутренней безопасности предупредили, что шпионы национальных государств, поддерживаемые Китаем, активно занимаются кибер-охотой за клиническими исследованиями.

«Атаки были очень высококлассными, - сказала Threatpost Хлоя Мессдаги, вице-президент по стратегии Point3 Security. «Все, что связано с конфиденциальными данными для COVID-19, определенно находится под угрозой со стороны иностранных национальных государственных субъектов или иностранных конкурирующих компаний, которые стремятся найти полезную информацию. Или это может быть отдельный злоумышленник или группа злоумышленников, пытающихся собрать деньги. Злоумышленники понимают, что это имеет исключительную ценность, потому что компании имеют очень хорошее финансовое положение, и что клинические испытания очень выгодны для быстрой выплаты». ***(Tara Seals. COVID-19 Clinical Trials Slowed After Ransomware Attack // Threatpost (https://threatpost.com/covid-19-clinical-trials-ransomware/159877/). 06.10.2020).***

***

«Хакери систематично проводять атаки на японські компанії, залучені до розробки вакцини від коронавірусу починаючи з квітня. Головна підозра впала на Китай.

За цими кібернападами можуть стояти китайські зловмисники, вважають у американській CrowdStrike, пише Kyodo. Фахівці з'ясували, що хакери намагались отримати доступ до файлів, що містять інформацію про хід створення вакцин від COVID-19.

Як повідомлялось, у травні спецслужби РФ відкрили полювання за вакциною проти коронавірусу. У липні Британія, Канада та США звинуватили військових хакерів РФ у спробах вкрасти вакцину від COVID-19. Британія заявила, що Росії загрожує відповідальність через кібератаки на наукові центри, які розробляють вакцину проти коронавірусу.

Згодом США звинуватили Китай в кібератаках на розробників вакцини від COVID-19. Кібератак зазнали неурядові та правозахисні організації і в Штатах, і в самому Китаї, фармакологічні компанії, розробники медичних виробів». ***(У Японії скоєно кібератаки на розробників вакцин від COVID-19 // UA.NEWS (https://ua.news/ua/v-yaponyy-sovershyly-kyberataky-na-razrabotchykov-vaktsyn-ot-covid-19/). 19.10.2020).***

***

«У Чехії почалися випадки надсилання людям фальшивих повідомлень про результат тесту на коронавірус, які хакери використовують для "фішингу".

…про це повідомив Загальний університетський госпіталь у Празі.

У госпіталі дізналися про проблему від клієнтів, які заявили, що отримали такі повідомлення, хоча ще не здавали тест.

Зловмисники почали "бомбардувати" людей повідомленням в SMS та на електронну пошту про нібито результат їхнього тесту на коронавірус, сподіваючись на те, що якась частка адресатів дійсно здали тест і повірять обману.

У повідомлення додають лінк, за яким потрібно перейти, щоб нібито дізнатися результат. Якщо зробити це, на телефон або комп'ютер потрапляє шкідливе програмне забезпечення.

"Ця фальшива інформація шкодить людям, які тестувалися, і залякує тих, хто ще не здавав тест… Крім того, почастішали хакерські атаки на лікарні та інші медичні заклади. Ми вирішуємо цю проблему у співпраці з Національним офісом кібербезпеки", - зазначає госпіталь.

У лікарні нагадують, що результат тесту завжди приходить у стандартизованій формі, із зазначенням імені та результату, максимум за 48 годин після здачі тесту…». ***(У Чехії шахраї почали використовувати повідомлення про результат тесту для викрадення даних // Європейська правда (https://www.eurointegration.com.ua/news/2020/10/27/7115785/). 27.10.2020).***

***

«Компания Dr. Reddy's, подрядчик российской вакцины против COVID-19 «Спутиник V» и крупный производитель дженериков, была вынуждена закрыть заводы и изолировать свои центры обработки данных.

Согласно сообщениям, производитель вакцины COVID-19 Dr. Reddy's Laboratories закрыл свои заводы в Бразилии, Индии, России, Великобритании и США после кибератаки.

Индийская компания является подрядчиком по разработке российской вакцины против COVID-19 «Спутиник V», которая скоро войдет в фазу 2 испытаний на людях. 19 октября Генеральный контроль над наркотиками Индии (DCGI) дал компании добро.

В США это крупный производитель дженериков, в том числе терапевтических средств для желудочно-кишечного тракта, сердечно-сосудистой системы, лечения боли, онкологии, противоинфекционных препаратов, педиатрии и дерматологии.

The Economic Times сообщила, что помимо закрытия заводов производитель лекарств изолировал все услуги центра обработки данных, чтобы применить исправления. Со ссылкой на источники, ET заявил, что компания стала жертвой утечки данных.

«После обнаружения кибератаки мы изолировали все службы центра обработки данных, чтобы предпринять необходимые превентивные меры», - заявил

ИТ-директор Мукеш Рати в заявлении для СМИ в четверг вечером. «Мы ожидаем, что все услуги будут запущены в течение 24 часов, и мы не прогнозируем какого-либо серьезного воздействия на нашу деятельность из-за этого инцидента».

По данным BBC, производство на некоторых предприятиях доктора Редди в Индии было прервано, а в двух британских офисах оказались отключены телефонные линии. Компания не разглашает подробности атаки и не комментирует отключение объектов.

COVID-19 Шпионаж

Этот инцидент может быть связан или не связан с участием компании из Хайдарабада в разработке вакцины против COVID-19, но в целом шпионаж, связанный с медицинскими исследованиями пандемии, остается постоянной проблемой. По мнению исследователей, как частные, так и спонсируемые государством группы нацелены на фармацевтические препараты из-за экономических и влиятельных преимуществ, которые успешная вакцина предоставит странам.

В июле Министерство внутренней безопасности США предупредило, что связанная с Россией группа APT29 (также известная как CozyBear или Dukes) нацелена на исследовательские компании Великобритании, Канады и США. APT надеется украсть исследования вакцины COVID-19, проведенные академическими и фармацевтическими учреждениями, в вероятной попытке разработать лекарство от коронавируса, предупредило DHS.

Ранее во время пандемии Всемирная организация здравоохранения стала мишенью APT-группы DarkHotel, которая пыталась проникнуть в ее сети для кражи информации.

Между тем, Министерство юстиции недавно обвинило китайских хакеров, связанных с правительством, в шпионаже за Moderna, биотехнологической компанией из Массачусетса. Федеральное правительство поддерживает развитие исследований вакцин Moderna, инвестировав около 1 миллиарда долларов, и в настоящее время проводятся клинические испытания.

«Кибер-злоумышленники проявляют большой интерес к фармацевтической отрасли, поскольку усилия в области исследований и разработок сосредоточены на создании вакцины против COVID-19», - сказал Threatpost Крис Хейзелтон, директор по решениям безопасности компании Lookout. «Тот, кто первым выйдет на рынок с вакциной, будет иметь значительное конкурентное преимущество, поэтому в фармацевтической промышленности есть веские причины для кражи интеллектуальной собственности».

По сути, фармацевтические компании должны вкладывать ИТ-ресурсы в защиту своей уникальной среды, добавил он.

«Исследователи проводят значительное время вдали от столов, а это означает, что планшеты и смартфоны становятся основным устройством, используемым лаборантами, активно участвующими в разработке формул лекарств», - сказал Хейзелтон. «Фармацевтическая промышленность всегда была на переднем крае внедрения технологий. Они используют планшеты и смартфоны как неотъемлемую часть всего процесса разработки и распространения лекарств.

«Учитывая такое пристальное внимание к вакцине COVID-19, группы фармацевтической безопасности должны предположить, что в их инфраструктуре есть субъекты угроз», - добавил он». ***(Tara Seals. COVID-19 Vaccine-Maker Hit with Cyberattack, Data Breach // Threatpost (https://threatpost.com/covid-19-vaccine-cyberattack-data-breach/160495/). 23.10.2020).***

***

«Специалисты Group-IB представили доклад, посвященный главным тенденциям компьютерных преступлений в период пандемии COVID-19. Доклад был представлен в рамках международного форума Академии Управления МВД РФ «Стратегическое развитие системы МВД России: состояние, тенденции, перспективы».

Последствия пандемии коронавируса, перевод сотрудников на удаленный режим работы, сокращение персонала и финансовый кризис вызвали стремительный рост компьютерной преступности. По оценкам аналитиков Group-IB, в первую очередь, выросло число финансовых мошенничеств с использованием методов социальной инженерии. Так, за период с января по июнь 2020 года, по данным МВД, рост киберпреступности составил 91,7% по сравнению с аналогичным периодом прошлого года. При этом число «классических преступлений» снижалось: уличных разбоев стало меньше на 23,6%, грабежей — на 20,7%, краж — на 19,6%, угонов машин — на 28,7%.

Одной из главных тенденций в МВД называют развитие дистанционных способов совершения преступлений, при которых отсутствует физический контакт между злоумышленниками и их жертвами — преступления ушли из офлайна в онлайн. Например, если до 2014 года сбыт наркотиков производился преимущественно «из рук в руки», то в наши дни нарктorговцы стали чаще использовать исключительно электронные торговые площадки в даркнете, принимающие оплату в криптовалюте.

Практически 70% зарегистрированных преступлений, связанных с незаконным оборотом оружия в 2020 году тоже совершалось с использованием интернета — дистанционно и анонимно. То же самое касается, незаконного сбыта поддельных денег, ценных бумаг и документов.

На протяжении всего 2020 года аналитики Group-IB фиксировали рост числа финансовых мошенничеств с использованием социальной инженерии — вишинга, фишинга — жертвами которых становились, в основном, клиенты банков. Суммарно за девять месяцев 2020 года CERT-GIB заблокировал 14 802 фишинговых ресурса, нацеленных на хищение денег и персональной информации посетителей сайтов (логины, пароли от аккаунтов и интернет-банков, данные банковских карт). Это больше, чем за прошлый год, когда были заблокированы 14 093 таких веб-ресурсов.

В Академии Управления МВД отмечают, что наиболее распространенным механизмом дистанционного мошенничества является традиционный звонок от «службы безопасности банка» якобы по поводу несанкционированной транзакции или взлома личного кабинета. При этом телефонные мошенники активно использовали технологии, связанные с подменой номеров и SIP-телефонией. При

использовании анонимайзеров установить реальный IP-адрес злоумышленника весьма затруднительно.

Также в последнее время появилось много сервисов «по пробиву» клиентов банков, построенных на комбинировании методов OSINT и инсайдерского доступа к различным базам данных, что увеличило объем информации о потенциальных жертвах, доступной для злоумышленников, и привело к увеличению количества атак.

При этом сами схемы реализации мошенничества фактически не изменились. Основной мотив киберпреступников — прежний: кража денег или информации, которую можно продать, но они приобрели новую «упаковку», адаптированную под актуальную повестку. Это продажа фейковых цифровых пропусков, рассылка сообщений о штрафах за нарушение карантина, липовые сайты курьерских служб, мошеннические рассылки от имени сервиса видеоконференций Zoom.

«На протяжении всего 2020 года Group-IB наблюдала активный набор в преступные мошеннические сообщества. Порог входа существенно снизился: новых участников привлекают через Telegram-каналы и хакерские форумы с последующим обучением, и вступительными бонусами. В „серой зоне“ тоже быстро подстроились под требования рынка, так „билетная мафия“ переориентировала свои ресурсы на доставку продуктов питания и лекарств по завышенным ценам», — говорит Андрей Колмаков, руководитель департамента расследований инцидентов информационной безопасности Group-IB.

По словам эксперта, активно развивался и рынок криминальных услуг cybercrime-as-a-service, связанных со сдачей в аренду компьютерных сетей, зараженных малварью (ботнетов) и используемых, например, при организации DDoS-атак, рассылке фишинговых писем и предоставлении proxy-серверов. Так же как и предложения по взлому мессенджеров и соцсетей, эти услуги рекламируются в Telegram и на хакерских форумах.

Отчет гласит, что в период пандемии электронная почта по-прежнему оставалась одним из основных векторов атак.

«Злоумышленники адресно атаковали переведенных на удаленку сотрудников, заражая их компьютеры вредоносными программами, через которые затем получали доступ в корпоративную сеть. Чаще всего перехваченные вредоносные рассылки, замаскированные в том числе и под сообщения о COVID-19, несли на борту вложения с программами-шпионами или ссылки, ведущие на их скачивание, бэкдоры и загрузчики, которые впоследствии использовались для установки других вредоносных программ, в том числе банковских троянов или вирусов-шифровальщиков», — рассказывает Валерий Баулин, руководитель Лаборатории компьютерной криминалистики Group-IB.

Популярность последних — не случайна, пишут эксперты. В 2020 году подавляющее большинство преступных групп переключилось на работу с -шифровальщиками — злоумышленники поняли, что с их помощью можно заработать не меньше, чем в случае успешной атаки на банк, а техническое исполнение — значительно проще.

Текущий год дал жизнь еще большему количеству групп и партнерских программ, а также новым коллаборациям. Так операторы банковского трояна

QakBot присоединились к «охоте за крупной дичью» (Big Game Hunting — атаки на крупные компании с целью получения значительного выкупа), воспользовавшись помощью вымогателя ProLock, а еще недавно активно атаковавшая банки и отели группа FIN7 присоединилась к партнерской программе вымогателя REvil.

Размер выкупа при таких атаках так же значительно увеличился: операторы криптолокеров нередко требуют у жертв несколько миллионов долларов, а иногда — и несколько десятков миллионов». ***(Мария Нефёдова. Эксперты Group-IB рассказали о ключевых тенденциях киберпреступлений в период пандемии // Xakep (https://xakep.ru/2020/10/23/covid19-crimes/). 23.10.2020).***

***

Світові тенденції в галузі кібербезпеки

«Тенденція до неоіндустріалізації, впровадження концепції Індустрії 4.0, розвиток ІТ-технологій, екологічні проблеми – у найближчі 5–10 років змінять ландшафт найбільш потрібних професій. Про це йдеться в проекті Стратегії розвитку вищої освіти в Україні на 2021-2031 роки, який розміщений на сайті МОН для громадського обговорення.

«Ми прогнозуємо, що в майбутньому «чисті» гуманітарні спеціальності відійдуть на другий план, а технічні, інженерні, навпаки, будуть найбільш потрібними. Професії, пов'язані із забезпеченням здоров'я, навчанням, наданням індивідуальних послуг, творчістю залишаться актуальними, оскільки не можуть бути заміщені автоматизованими системами навіть із використанням штучного інтелекту. Водночас зростає потреба у фахівцях біологічного напрямку, особливо у сфері біоінженерії, біотехнологій, фармації тощо. Ці тенденції вимагають посилення природничо-наукової підготовки майбутніх фахівців разом із набуттям ними ІТ-навичок», – зазначив у своєму Telegram-каналі т.в.о. Міністра освіти і науки України Сергій Шкарлет.

За оцінками світових експертів, оприлюдненими у Forbes, BBC, Trade Schools Colleges, та експертів дослідницької групи «Digitale Transformation» Науково-дослідного інституту майбутніх трудових відносин (м. Бонн), найбільш потрібними будуть фахівці, які можуть проектувати, впроваджувати нову техніку і технології з урахуванням викликів майбутнього, а також професії, пов'язані із забезпеченням життя та здоров'я людини:

технології майбутнього – архітектор територій, фахівець з робототехніки, інженер-проектувальник різного профілю, фахівець з 3D-друку, розробник та диспетчер безпілотних апаратів, космогеолог; ІТ-технології та дані – проектувальник «розумного середовища» та «розумних будівель», програміст, аналітик даних, фахівець-аналітик з кібербезпеки, розробник технологій блокчейн, розробник віртуальної або доповненої реальності, фахівець із цифрового контенту, цифровий лінгвіст; екологізація виробництва та життя – екоаналітик у будівництві, фахівець з альтернативної (сонячної, вітрової тощо) енергетики, біоетик, ресайклінг-дизайнер, фахівці з «сіті-фермерства»; здоров'я людини – біогенетик, біоінженер, біоінформатик, біофармаколог, телехірург, ІТ-лікар, медична сестра,

фізіотерапевт, нейропсихолог…». ***(МОН прогнозує зміну ландшафту потрібних професій, – Сергій Шкарлет // Офіційно (https://oficiyno.com.ua/2020/10/09/mon-prognozue-zminu-landshaftu-potribnih-profesij-sergij-shkarlet-41674/). 09.10.2020).***

***

«Стимулирование передовых практик как в бизнесе, так и в повседневной жизни должно стать для страховщиков для инструментом построения безопасного глобального киберпространства. Такой вывод содержится в новом отчете Фонда Карнеги «Защита киберпространства».

По мнению авторов отчета, страховщики и перестраховщики могут делать привязку страхового покрытия и размера премий к передовой практике своих клиентов. В частности, речь идет о предоставлении более выгодных страховых программ для компаний, которые внедряют передовые технологии, а на всех этапах создания продукта используются защищенные кибернетические инструменты.

«Поскольку многие предприятия и страховые компании работают на транснациональном уровне, киберстрахование, вероятно, может продвигать передовые методы безопасности быстрее, шире и эффективнее, чем национальные правительства», — говорится в отчете.

Аналогичным образом должны действовать и инвесторы, «продвигая при этом свои собственные интересы и глобальное благо». ***(Страховщики имеют рычаги влияния на глобальную кибербезопасность // УкрСтрахование (https://www.ukrstrahovanie.com.ua/news/strahovshhiki-imeyut-rychagi-vliyaniya-na-globalnuyu-kiberbezopasnost). 06.10.2020).***

***

«За последние несколько лет концепция архитектуры «нулевого доверия» прошла ряд этапов эволюции. Из новой модной причуды она превратилась в банальность (во многом из-за потока маркетинга со стороны тех, кто хочет нажиться на тренде), в прошлом, и теперь, в конечном итоге, превратилась в то, что, вероятно, всегда должно было быть. вместе: надежный, практичный вариант безопасности с дискретными, наблюдаемыми преимуществами и недостатками, который можно включить в подход организации к обеспечению безопасности.

Нулевое доверие представляет собой модель безопасности, в которой все активы - даже управляемые конечные точки, которые предоставляет руководитель, в том числе локальные сети, настроенные администратором, - считаются враждебными, ненадежными и потенциально уже скомпрометированы злоумышленниками. Вместо устаревших моделей безопасности, которые отличают «доверенный» внутренний от ненадежного внешнего, нулевое доверие предполагает, что все сети и узлы одинаково ненадежны.

Как только этот фундаментальный сдвиг в предположениях будет сделан, руководитель может принимать различные решения о том, чему, кому и когда доверять, и разрешать допустимые методы проверки для подтверждения запроса или транзакции.

С точки зрения безопасности метод имеет свои преимущества и недостатки

Одним из преимуществ является то, что метод позволяет руководителю стратегически применять ресурсы безопасности там, где они нужны больше всего; и это увеличивает сопротивление движению атакующего (так как каждый ресурс нужно ломать заново, если будет установлен плацдарм).

Есть и минусы. Например, принудительное применение политик требуется для каждой системы и приложения, и более старые устаревшие компоненты, созданные с различными предположениями безопасности, могут не подходить, например что внутренняя сеть заслуживает доверия.

Один из наиболее потенциально проблемных недостатков связан с проверкой состояния безопасности, то есть в ситуациях, когда модель безопасности требует проверки более старыми, более ориентированными на наследие организациями. Эта динамика неудачна: те организации, которые, вероятно, сочтут модель наиболее убедительной, - это те же организации, которые, приняв ее, скорее всего, решат проблемы проверки.

Проверка и минимизация воздействия

Чтобы понять динамику, которая здесь описана, полезно подумать, каким будет следующий логический шаг после принятия нулевого доверия. В частности, если руководитель предполагает, что все конечные точки потенциально скомпрометированы, а все сети, вероятно, являются враждебными, естественным и логическим следствием этого предположения является минимизация того, куда могут попасть конфиденциальные данные.

Например, можно решить, что определенные среды недостаточно защищены для хранения, обработки или передачи конфиденциальных данных, кроме как через очень узко определенные каналы, такие как аутентифицированный доступ HTTPS к веб-приложению.

В случае интенсивного использования облачных сервисов вполне логично решить, что конфиденциальные данные могут храниться в облаке - при условии, конечно, механизмов контроля доступа, которые созданы специально для этой цели и имеют меры безопасности и оперативные персонал, который руководитель не может позволить развернуть или поддерживать только для собственного использования.

В качестве примера предположим, что есть гипотетическая более молодая организация из среднего бизнеса. Под словом «моложе» подразумевается, что, возможно, прошло всего несколько лет с момента основания организации. Скажем, эта организация является «родной для облака», то есть на 100% экстернализована для всех бизнес-приложений и полностью построена на использовании облака.

Для такой организации совершенно необходимо отсутствие доверия. Поскольку она 100% экстернализована, у нее нет центров обработки данных или внутренних серверов, и она поддерживает только самые минимальные локальные технологии. Эта организация может прямо потребовать, чтобы никакие конфиденциальные данные не могли «жить» на конечных точках или внутри их офисной сети. Вместо этого все такие данные должны находиться в подмножестве известных, определенных облачных сервисов, которые явно одобрены для этой цели.

Это означает, что организация может сосредоточить все свои ресурсы на укреплении облачной инфраструктуры, службах шлюзов, чтобы весь доступ (независимо от источника) был надежно защищен, и лишить приоритета таких вещей, как физическая безопасность, укрепление внутренней сети (при условии, что есть даже one), развертывание средств внутреннего мониторинга и т. д. Если для обеспечения безопасности использования облачных компонентов соблюдается тщательный и точный процесс, такой подход может помочь сосредоточиться на ограниченных ресурсах.

Однако ни одна организация не работает в идеальных условиях. Она работает с клиентами, руководит процессом продаж, деловыми партнерами и многими другими. Поскольку организация меньше, многие из ее клиентов могут быть более крупными организациями - потенциально клиентами с жесткими требованиями к защите внешних поставщиков услуг и проверке их безопасности. Возможно, у нее есть нормативное обязательство сделать это в зависимости от отрасли, в которой она работает. Теперь некоторые из таких клиентов могут быть полностью экстернализованы, но большинство не будет - у них будут устаревшие приложения, уникальные ограничения, специализированные требования и другие бизнес причины, по которым они не смогут полностью поддерживать внешнюю модель.

Какие результаты часто являются вполне понятными, но, тем не менее, контрпродуктивными, дискуссиями о перекрестных целях между организацией, проводящей оценку (потенциальный заказчик), и той, которая подвергается оценке (поставщик услуг). Например, поставщик услуг может очень разумно возразить, что меры контроля физической безопасности (если выбрать только один пример) выходят за рамки целей оценки. Они могут утверждать это на том основании, что единственные имеющие значение меры физической безопасности - это те, которые используются поставщиками облачных услуг, поскольку, в конце концов, это единственное место, где разрешено хранить данные.

С другой стороны, заказчик также может разумно беспокоиться об аспектах физической безопасности, которые действительно относятся к среде поставщика услуг. Например, доступ посетителей к объектам, где данные клиентов могут просматриваться на экране, даже если данные там не хранятся. Они могут представить себе сценарий, например, когда неавторизованный посетитель в офисе может "увидеть визуально" данные, когда они выводятся на экран легитимным пользователем.

Разговор, подобный приведенному выше, даже если он не вызывает споров, все же неоптимален для обеих сторон. С точки зрения поставщика услуг, это замедляется процесс продаж, что отнимает время у инженеров, которые в противном случае были бы сосредоточены на разработке продукта. Однако с точки зрения потенциального клиента это заставляет его нервничать по поводу потенциальных источников неучтенного риска - одновременно вызывая недовольство у внутренних деловых партнеров, стремящихся использовать услугу и желающих, чтобы проверка прошла быстро.

Принципиальные стратегии

Таким образом, возникает вопрос: как эффективно передать модель нулевого доверия, если мы хотим использовать его таким образом? Если мы подтверждаем

такой подход, как нам ответить на правильные вопросы, чтобы мы могли быстро прийти к определению и (в идеале) разрешить бизнес-использование сервиса? Оказывается, мы можем использовать несколько подходов. Никто из них не занимается ракетостроением, но для поддержки им требуется сочувствие и некоторая работа.

С точки зрения поставщика услуг следует помнить о трех полезных принципах: 1) быть готовым, 2) демонстрировать подтверждение ваших предположений и 3) подтверждать свои утверждения документацией.

Под «предстоящим» я подразумеваю готовность поделиться информацией, выходящей за рамки того, о чем мог бы спросить покупатель. Если руководитель предоставляет облачное SaaS, как в приведенном выше примере, это может означать, что он готов делиться информацией, выходящей за рамки определенного набора элементов, запрошенных клиентом. Это позволяет ему «обобщать» информацию даже с точки зрения использования стандартных результатов. Например, можно рассмотреть возможность участия в реестре CSA STAR, подготовить стандартные артефакты для сбора информации, такие как CSA CAIQ, SIG для стандартизированной контрольной оценки Shared Assessments или HITRUST Third Party Assessment Program в сфере здравоохранения.

Второй принцип, демонстрирующий валидацию, означает, что руководитель подтвердил предположения, которые вошли в егл модель безопасности. В приведенном выше примере это означает, что мы могли бы подтвердить предположение о том, что «данные не хранятся внутри», проверив его. Оценщик от заказчика с гораздо большей вероятностью поверит заявлению, если для его проверки используется такой элемент управления, как DLP.

Последний пункт наличия документации означает документирование модели, которая поддерживается на предприятии. Например, если можно предоставить архитектурный документ, описывающий конкретный подход: почему он применяется, анализ рисков, который выполнен заранее, средства контроля для проверки и т. д.

Со стороны оценщика на самом деле существует только один принцип - проявлять гибкость там, где это возможно. Если намерение и строгость элементов управления, которых ожидает руководитель, и поставщик услуг выполняет те же функции с тем же уровнем строгости, но другим способом, чем ожидалось, предоставляя поставщику услуг варианты (кроме требования приобретать и устанавливать элементы управления, которые им не нужны).

Стоит сказать, что ни один из этих советов не является истиной в последней инстанции. Но то, что очевидно, не означает, что все это делают. Сделав некоторую работу заранее и посмотрев сквозь призму эмпатии, можно упростить процесс оценки в ней». ***(Романов Роман. Применение модели "нулевого доверия" в оценке уровня кибербезопасности помогает предотвратить хакерские атаки // Internetua (https://internetua.com/Primenenie-modeli-nulevogo-doveria-v-ocenke-urovnia-kiberbezopasnosti-predpriyatiy).*** 05.10.2020).

***

«По данным последнего Всемирного экономического форума, в глобальном плане кибератаки снизили свой уровень угрозы для бизнеса относительно других рисков, но остались в высоком приоритете в Северной Америке и Европе.

Тремя наиболее значимыми угрозами для бизнеса в мире, по данным исследований, оказались безработица и распространение инфекционных заболеваний и финансовый кризис. Кибератаки в этом списке заняли четвёртое место.

В Северной Америке, исходя из результатов исследования, кибератаки заняли первое место среди угроз бизнесу. В Европе кибератаки заняли второе место, но первое в Великобритании.

Также было отмечено, что пандемия COVID-19 косвенно влияет на угрозу кибератак.

Всего в исследовании использовались ответы более 12000 владельцев бизнесов из 127 стран». ***(Всемирный экономический форум: кибератаки остаются главной угрозой для бизнеса на Западе // SecureNews (https://securenews.ru/world-economic-forum-cyberattacks-remain-top-business-threat-in-the-west/). 08.10.2020).***

***

Безопасность - это проблема для всех. Это всеобъемлющая идея, которую выдвинула команда Oxford Brookes University при реализации своей первой специальной стратегии информационной и кибербезопасности.

Для достижения успеха в распространении этого духа жизненно важно обеспечить участие влиятельных лиц в организации, особенно старших руководителей, и обеспечить их инвестиции.

Глава отдела управления информационной безопасностью Гарет Пэкхэм, который возглавляет стратегию, с самого начала дал понять, что:

«[Стратегия информационной безопасности] - это не просто технический операционный план, который только я и несколько других сотрудников ИТ-отдела когда-либо видели или слышали - она затрагивает всю организацию».

Мыслительный процесс и подход

Важно отметить, что несмотря на то, что трехлетняя стратегия была написана в конце 2019 года и одобрена до пандемии, предварительный обзор изоляции пришел к выводу, что она не требует обновления, чтобы учесть массовый переход к дистанционному обучению и работе. Гарет говорит:

«Любая стратегия должна быть достаточно гибкой, чтобы соответствовать драйверам бизнеса, целям организации и меняющейся операционной среде».

Это включает в себя учет текущих угроз. Частью этого является надежная, своевременная и отраслевая информация, - говорит Гарет, цитируя рекомендации Jisc и NCSC в качестве полезных ресурсов. Как член различных групп, включая платформу обмена информацией о кибербезопасности NCSC и форум по кибербезопасности University Alliance, Гарет также считает полезным обсуждение передового опыта с коллегами.

Первые шаги

В Oxford Brookes уже несколько лет работает специальная группа безопасности, которая помогла изменить то, что ранее было довольно частичным подходом, «и вовсе не целостным». Получение сертификата является частью плана. Команда сейчас работает над сертификацией Cyber Essentials, уже получив ISO 270001.

В качестве руководства по стратегии Гарет использовал структуру кибербезопасности Национального института стандартов и технологий США, которая предусматривает «выявление, защиту, обнаружение, реагирование и устранение последствий». В течение первого года основное внимание уделяется управлению - определению ролей и обязанностей, политик и процедур, а также соответствия. Два и три года будут посвящены предотвращению, обнаружению и реагированию, а после первой стратегии Гарет также стремится автоматизировать некоторые из этих функций.

Фундамент

«Было много задела», - говорит Гарет.

«Еще до того, как была написана стратегия, мы с моей командой работали над объединением практики безопасности между университетами, и я много общаюсь по вопросам безопасности и защиты данных.

«Я разговаривал со многими людьми в университете, не будучи паникером; Я не собирался рассказывать людям, что, если они не приведут свой дом в порядок, мы получим штраф в размере 20 миллионов фунтов стерлингов от Управления комиссара по информации, или мы будем взломаны и потеряем все наши данные - хотя оба эти Теоретически все возможно.

«Мое намерение состояло в том, чтобы побудить людей работать эффективно, но безопасно, и для этого мне нужно было завоевать и сохранить доверие сотрудников и студентов. Речь идет об изменении культуры, и это продолжается ".

Управление и ответственность

Эксперты по безопасности во всем секторе соглашаются, что значимая стратегия безопасности требует поддержки на уровне совета директоров; старшие руководители должны понимать риски и нести ответственность, как указали руководители службы безопасности в HE и FE, Мик Дженкинс из Университета Брунеля и Джонатан Висон из колледжа Милтон Кейнс.

В рамках процесса утверждения в Oxford Brookes Гарет представил свою стратегию высшему руководству, главе департаментов и совету управляющих.

«Это включало в себя описание рисков, связанных с безопасностью данных и кибератаками.

«Это показало, что мы серьезно относимся к безопасности, и помогло, когда мы представили инвестиционный план».

Принятие решений по безопасности в Oxford Brookes осуществляется с двух сторон. Существует технический совет, который собирается ежемесячно, и рабочая группа по управлению информацией, в которую входят старшие сотрудники, которые изучают все зарегистрированные инциденты информационной безопасности и нарушения защиты данных. Старшие сотрудники несут

ответственность за распространение информации о действиях по прояснению ситуации и профилактических мероприятиях.

Но ответственность на этом не заканчивается, как объясняет Гарет:

«Моя задача и функция моей команды - предоставлять людям специальные знания, инструменты и рекомендации, но я не несу ответственности за чужие данные, будь то исследовательская база данных или система записи студентов. Мы проводим оценку рисков и безопасность, и мы рассказываем ответственному лицу, как сделать это лучше, но, в конце концов, это их ответственность ».

Связь

Чтобы поделиться сообщениями безопасности, Гарет нацелен на определенные группы. «Если я смогу расположить к себе влиятельных лиц и заставить их играть в мяч, то другие последуют за мной.

«Одна из моих тактик - выявлять передовой опыт и хвалить его. Люди откликаются на это. Вероятность того, что что-то плохое, произойдет, если люди не будут чувствовать себя вовлеченными и заинтересованными. Чтобы помочь, мы помогаем людям быть бдительными в отношении фишинговых писем и устанавливать надежные пароли.

«Поскольку человеческая ошибка является фактором высокого риска киберпреступлений, необходимость в осведомленности о безопасности является важной частью обеспечения безопасности сектора. Вот почему у нас есть план связи как часть стратегии безопасности, и все 2800 сотрудников должны пройти 90-минутное обучение.

«Кроме того, мы проводим регулярные тренинги для менеджеров. Каждый раз я буду концентрироваться на разных вещах, включая программы-вымогатели, защиту от фишинга, защиту паролей и контроль доступа. Но на самом деле я использую любую возможность, чтобы рассказать разным кафедрам и факультетам по вопросам безопасности ».

Управляемые системы

По мере развития стратегии Гарет рассматривает платформы для автоматизации определенных функций безопасности и в настоящее время пилотирует сервис SIEM, управляемый Jisc, но при этом осознает необходимость достижения баланса между генерированием потенциально полезных данных и наличием достаточного количества аналитиков, чтобы извлечь из этого максимальную пользу.

«Мы будем искать управляемые или автоматизированные услуги в ряде областей, где у нас недостаточно внутренних ресурсов, таких как обнаружение угроз и реагирование на них, а также облачная безопасность. Однако мы хотим сохранить некоторые функции в качестве средства для роста технических знаний в нашей команде, что позволяет нашим людям развивать свои навыки.

«Управляемые услуги никогда не являются панацеей», Гарет заключает, потому что им требуются внутренние технические знания для настройки и кто-то, кто будет управлять контрактами.

«Это баланс. Ценность заключается в том, могут ли эти услуги повысить эффективность, давая нам лучший контроль, чем если бы мы полагались исключительно на расширенные ресурсы в нашей команде ». (‘Security is not a bolt-

on to the IT function' // Jisc (https://www.jisc.ac.uk/news/security-is-not-a-bolt-on-to-the-it-function-15-oct-2020). 15.10.2020).

В сентябре 2020 года Национальный центр кибербезопасности (NCSC) предупредил о всплеске атак программ-вымогателей на университеты, колледжи и школы, а Internet Watch Foundation (IWF) объявил об увеличении на 50% публичных сообщений о сексуальном насилии над детьми в Интернете в трех странах. месяцев после изоляции.

Поскольку люди проводят в Интернете больше времени, чем когда-либо прежде, для работы и отдыха, существует больший риск нанесения вреда в Интернете - как для отдельных лиц, так и для организаций. Что может быть лучше, чтобы по-новому взглянуть на способы сделать Интернет безопаснее для всех?

Повышенная опасность работы из дома

Директор IWF по связям с общественностью Эмма Харди увидела на 65% больше случаев сексуального насилия над детьми в Интернете по сравнению с 2019 годом и говорит:

«Одна из причин, по которой люди натыкаются на более неприятный контент, заключается в том, что они работают дома в недостаточно защищенных сетях».

Чтобы избежать этого, люди, которые работают из дома или у которых есть молодые члены семьи, могут проверить меры защиты, предоставляемые их интернет-провайдером (Интернет-провайдер). Дэвид Райт, директор Центра безопасного Интернета в Великобритании (UKSI), указывает на фильтрацию тестов как на простой и эффективный инструмент.

Следует также пересмотреть и усилить защиту сетей провайдеров образования. Надежная институциональная политика поддержки безопасности в Интернете поможет сотрудникам и студентам понять, как безопасно работать, чего от них ждут и что делать, если что-то пойдет не так. Между тем, цифровые решения, такие как веб-фильтрация и мониторинг, отсеивают вредоносный контент.

IWF также поддерживает список URL-адресов контента, который он пытается удалить, и список хэшей (цифровых отпечатков пальцев) сексуального насилия над детьми, которые можно использовать для идентификации и удаления экземпляров этого контента. Школы и колледжи должны убедиться, что в их решениях для веб-фильтрации включены и включены оба этих списка. Университеты должны серьезно подумать о специальном решении для веб-фильтрации, поскольку оно предлагает множество других преимуществ, но, как минимум, следует получать списки IWF и CTIRU и использовать их для блокировки незаконных материалов.

Безопасные методы работы

Теперь, когда увеличение объема онлайн-обучения, похоже, будет продолжаться в обозримом будущем, полностью ли готовы студенты и сотрудники? Возможно, нет, - говорит Райт.

«Ожидается, что образовательные организации смогут продолжать обучение в условиях локальных ограничений, но в некоторых случаях у учащихся нет подходящих устройств, на которых установлено подходящее программное

обеспечение, и они могут не знать о лучших и самых безопасных платформах для использования..

«Например, школы могут использовать Zoom, потому что он доступен, но это не подходит для учащихся младше 16 лет».

Учреждения должны внимательно следить за этим, а также проводить обучение сотрудников и студентов, чтобы помочь им оставаться в безопасности. Преподаватели должны знать, например, о рисках, связанных с использованием личных устройств и личных учетных записей для «чата». Их следует поощрять к установлению профессиональной дистанции, пониманию того, как и когда целесообразно использовать видеоконференцсвязь и потоковую передачу в реальном времени, и, что особенно важно, как ужесточить свои собственные настройки конфиденциальности.

UKSI предлагает полезные ресурсы для сотрудников, работающих из дома, а также информацию, которая поможет убедиться, что практика преподавания способствует безопасному удаленному обучению.

Проблемы почти одинаковы для студентов, многие из которых не будут так сообразительны, как мы, возможно, думаем о проблемах безопасности, связанных с социальными сетями и платформами онлайн-обучения.

По словам Райта, студенты являются особенно уязвимыми для вредоносных обмена интимных изображений онлайн (так называемые «порноместь») и UKSI видел потрясающие 100% -ное увеличение запросов о помощи с этим и «sextortion», так как национальная изоляция.

Эмма Бонд, профессор социотехнических исследований, директор по исследованиям и руководитель аспирантуры в Университете Саффолка, и Энди Фиппен, профессор цифровых прав в Борнмутском университете, создали Инструмент самопроверки по защите высшего образования в Интернете (pdf). Он содержит полезные ресурсы, посвященные всем аспектам правильного поведения в сети, а также информацию о том, где получить поддержку и помощь, когда они будут сочтены нужными.

Их совет сотрудникам университетов и колледжей - «проявлять инициативу». Они продолжают:

«Обсудите цифровую вежливость во время индукционного обучения. Предложите последовательное руководство по таким вещам, как использование камеры, и изложите четкие ожидания в отношении поведения и какие последствия будут для тех, кто запугивает или преследует в Интернете, и как студенты могут раскрыть насилие. Сделайте онлайн-безопасность и защиту дополнительными вопросами ».

Важнейшая онлайн-идентичность

Идентичность в Интернете имеет значение, от старших руководителей учреждения до учащихся в школе. Каждый должен защищать свою, чтобы не допустить кражи личных данных, мошенничества и шантажа, а также убедиться, что будущие работодатели производят хорошее впечатление, когда приходят на поиски.

Разумно проверить настройки конфиденциальности в социальных сетях и убедиться, что личные учетные записи настроены только для «друзей». Есть

инструменты, которые могут помочь в этом - SWGfL тестирует мой инструмент конфиденциальности, помогает с настройками конфиденциальности, а контрольные списки для социальных сетей - удобный способ не отставать от функций безопасности на различных платформах социальных сетей.

Отчет, отчет, отчет

Также важно незамедлительно сообщать о проблемах с защитой, будь то защита потенциальных клиентов внутри организации или, при необходимости, сторонним агентствам. Иногда это может показаться неловким или даже рискованным. Например, Эмма Харди и Дэвид Райт говорят, что люди, которые чаще всего сталкиваются с сексуальным насилием над детьми в Интернете, - это молодые люди в возрасте от 16 до 24 лет, но они также меньше всех сообщают об этом.

«Мы упростили возможность сообщать нам; это анонимно и безопасно », - говорит Харди.

«Как ни печально, когда вы находите подобные изображения, недостаточно просто щелкнуть по ним, потому что это не избавляет от злоупотреблений. Сообщение об этом занимает секунды, и это может помочь нам спасти ребенка ».

Есть много организаций, которые предоставляют помощь во всем, от удаления интимных изображений или экстремистского контента до борьбы с кражей в Интернете. Онлайн-руководство по безопасности Jisc содержит обширный список, как и Инструмент самопроверки по безопасности в сфере высшего образования (pdf) …» ***(Moving towards safer online experiences // Jisc (https://www.jisc.ac.uk/news/moving-towards-safer-online-experiences-12-oct-2020). 12.10.2020).***

***

«Результаты четвертого ежегодного исследования кибербезопасности в образовательном и исследовательском секторе, проводимого Jisc, продолжают демонстрировать растущие усилия по борьбе с киберпреступностью.

Есть положительные признаки того, что уровень знаний, технического контроля и обучения в университетах и колледжах растет из года в год, показывая, что провайдеры серьезно относятся к кибербезопасности.

В этом году, например, подавляющее большинство - 82% высшего образования (OH) респондентов и 87% лиц, получающих дополнительное образование (FE) респонденты - указывают, что кибербезопасность является приоритетом в их организации…

Однако важно противопоставить эти достижения постоянно меняющейся среде угроз. Киберпреступники гибки и быстро реагируют на использование социальных или экономических факторов.

Существует множество случаев фишингового мошенничества, использующего страх вокруг COVID-19, новички обычно становятся мишенью для мошенников, как недавно предупредило правительство, и сектор недавно пострадал от серии атак с использованием программ- вымогателей.

Угрозы и обучение

Опрос этого года, результаты которого были распространены среди членов Jisc, был опубликован в июне / июле 2020 года, когда сектор был заблокирован и до атак программ-вымогателей в конце лета. И все же программы-вымогатели, совершенно справедливо, по-прежнему представляют собой главную угрозу…

Как и в исследованиях 2018 и 2019 годов, фишинг и социальная инженерия являются главной проблемой, выявленной обоими ОН а также FE респондентов, при этом 72% ОН учреждений и 74% FE выбрав эту угрозу как самую высокую.

Программы-вымогатели / вредоносные программы и незащищенные уязвимости системы безопасности занимают второе и третье места в обоих случаях. ОН а также FE…

Среди перечисленных «других» угроз наиболее часто упоминались человеческие ошибки и случайные утечки данных со стороны сотрудников, что опять же отражает ответы от 2019 года. Это говорит о том, что внедрение средств контроля против фишинга наряду с обучением и повышением осведомленности среди сотрудников / студентов по-прежнему является ключевым приоритетом для организаций.

Обязательная подготовка персонала увеличилась как для FE а также ОНпровайдеров за четыре года, которые мы проводили опрос - с менее чем половины до более чем 80%. Колледжи лидируют в том, что касается обязательной подготовки по вопросам безопасности для учащихся: 30% настаивают на этом в этом году по сравнению с 8% университетов.

Сертификаты

Доля организаций, получивших сертификаты кибербезопасности, резко увеличилась. Только 21%ОН и 7% FEимели Cyber Essentials в 2017 году по сравнению с 69% и 49% соответственно в этом году; 8% отОН получили Cyber Essentials Plus в 2017 году по сравнению с 31% в 2020 году.

Нет FE организация сообщила о наличии Cyber Essentials Plus в 2017 году, в то время как 19% получили его в 2020 году, а еще 36% находятся на пути к нему.

Этот прогресс во многом обусловлен государственной политикой и потребностями в финансировании. Cyber Essentials уже является предпосылкой для организаций, надеющихся получить государственные контракты; Получение сертификата было ключевым действием в плане действий государственного сектора Шотландии по обеспечению киберустойчивости, и это также требование для тех, кто финансируется Агентством по финансированию образования и навыков в 2020/21 году, в то время как Cyber Essentials Plus будет требованием с 2021/22.

Экспертиза и сравнительный анализ

Большинство (86%) ОН организации сообщают о наличии специального персонала по кибербезопасности в 2020 году по сравнению с 69% в 2017 году, в то время как цифры по FE составляют 28% в этом году по сравнению с 3% в 2017 году…

Безопасность в колледжах, как правило, обеспечивается ИТ-персоналом, который носит несколько головных уборов, поэтому отрадно видеть рост числа поставщиков FES с выделенным персоналом по безопасности.

Почти все университеты (90%) используют сторонние сервисы для проверки своей защиты, причем почти три четверти используют те или иные формы тестирования на проникновение. При 68% эти инструменты менее распространены вFEорганизаций, хотя более половины (53%) сообщают об использовании тестирования на проникновение.

Последствия COVID-19

Опрос этого года был распространен в июне / июле 2020 года, когда сектор был заблокирован из-за пандемии. Помимо результатов опроса, регулярное общение моей команды с сотрудниками службы безопасности в колледжах и университетах показывает, что участники в значительной степени встали перед задачей поддержки быстрого перехода к работе в Интернете.

Однако респонденты заявили, что рабочая нагрузка на ИТ-персонал и персонал службы безопасности увеличилась, например, для расширения виртуальной частной сети (VPN) мощности и удаленного управления безопасностью устройств.

Хотя некоторые ИТ-проекты были отложены из-за закрытия кампуса или изменения приоритетов, оба FE и организации высшего образования сообщают, что проекты, связанные с безопасностью, включая внедрение многофакторной аутентификации, были выдвинуты или инициированы…

Поскольку кибербезопасность считается приоритетом, минимальный персонал был уволен, и потребовались дополнительные меры безопасности или мониторинг. Есть также упоминания о повышении осведомленности и обучении сотрудников и студентов.

Воздействие атак

Кибератаки могут быть катастрофическими событиями, которые могут привести к неделям сбоев и повлечь за собой большие расходы, не говоря уже о репутационном ущербе. Среди наиболее распространенных последствий, о которых сообщалось в исследовании, было то, что атаки мешали сотрудникам работать и требовали дополнительного времени сотрудников и дополнительных денег для восстановления.

Некоторые организации также сообщают, что атаки привели к инвестициям в дополнительные меры безопасности, но предотвращение всегда лучше лечения, и здесь нет места для самоуспокоенности.

Внедрение надежных технических средств контроля и процессов, безусловно, необходимо для защиты от угроз, но не является универсальным решением. Безопасность - это ответственность на уровне правления, и она должна быть встроена во все организации». ***(John Chapman. Cyber security in universities and colleges is improving, but there's no room for complacency // Jisc (https://www.jisc.ac.uk/blog/cyber-security-in-universities-and-colleges-is-improving-but-theres-no-room-for-complacency-20-oct-2020). 20.10.2020).***

***

«Минулого тижня користувачі Twitter на кілька годин залишилися без доступу до додатка і сайту після збою в роботі соцмережі.

Тисячі людей повідомляли про проблеми із сайтом і додатком технологічного гіганта для Android та iOS, через що новинні стрічки не завантажувалися, а користувачі не могли відправляти твіти.

17 вересня стався збій у роботі соціальних мереж Instagram і Facebook. Сторінки в Instagram не завантажувалися, а користувачі навіть не могли увійти у власні акаунти.

За даними ресурсу downdetector, регулярні збої в роботі інтернет-сервісів з мільярдними аудиторіями користувачів – не винятки, а норма.

Користувачі PayPal, YouTube, Telegram, GTA 5, Tinder, Gmail, Amazon, Twitch, Fortnite та багатьох інших відомих на весь світ інтернет-сервісів регулярно на години і навіть на дні втрачають доступ до своїх акаунтів.

Хтось втрачає можливість зайву годину розважитися в онлайн-грі, а хтось, якщо мова йде про PayPal, YouTube, Amazon, Google або Facebook, втрачає реальні гроші.

Чому відбуваються збої в роботі інтернет-компаній? Як це впливає на компанії і користувачів? Які загрози виникають з точки зору втрати даних? ЕП спробувала знайти відповіді на ці питання в описах найбільш масштабних за останній час збоїв соцмереж і месенджерів.

Кейс Twitter

319 млн активних користувачів. Оборот – 2,2 млрд дол. Дохід – 0,5 млрд дол.

Після 23:00 15 жовтня 2020 року на сайті DownDetector нараховувалося понад 10 тис повідомлень про проблеми з доступом до Twitter. Користувачі повідомляли про помилки, включаючи "Помилка твіту: щось не так. Будь ласка, спробуйте пізніше" і "Сервіс тимчасово перевантажений".

Спроби перевстановити додаток не давали результату – пароль для підтвердження входу в акаунт не надходив на мобільні пристрої користувачів.

У якийсь момент на головній сторінці Twitter було написано: "Щось технічно не так. Дякуємо, що помітили – ми збираємося виправити це, і скоро все повернеться в норму".

Пізніше Twitter опублікував офіційну заяву. У ній було сказано, що він працює над проблемою і не вважає, що відключення було викликане будь-яким порушенням безпеки.

"Twitter був недоступний для багатьох з вас, і ми працюємо над тим, щоб знову запустити його для всіх, – йшлося в заяві. – У нас були проблеми з нашими внутрішніми системами, і у нас немає ніяких доказів злому".

Між тим, двома місяцями раніше в Twitter відбувся найбільший в історії соцмережі злам. Біткоїн-шахраї зламали твітер-акаунти провідних світових діячів і компаній, включаючи Каньє Уеста, Барака Обаму, Білла Гейтса, Apple, Ілона Маска, Джо Байдена, Майкла Блумберга, Джеффа Безоса, Уоррена Баффета, Uber і Біньяміна Нетаньяху.

Усі облікові записи, які мали багато підписників у Twitter, були одночасно зламані. На кожному з них з'явилося повідомлення, у якому користувачам пропонувалося переказати 1 тис дол на біткоїн-адреси.

Користувачам обіцяли, що їхні гроші будуть подвоєні і згодом їх повернуть.

Загалом було зламано понад 50 авторитетних облікових записів. Обсяг коштів, надісланих користувачами хакерам, на першу годину ночі 16 липня перевищив 12 біткоїнів. За поточним курсом криптовалюти це понад 110 тис дол.

У відповідь на злом Twitter тимчасово заборонив усім перевіреним обліковим записам із синіми галочками завантажувати твіти, поки проводилося розслідування.

Кейс Facebook та Instagram

2,5 млрд активних користувачів. Оборот – 22,4 млрд дол. Дохід – 22,2 млрд дол.

Найбільший збій у своїй історії Facebook пережив 14 березня 2019 року. Сервіси Facebook, Instagram, WhatsApp "впали" по всьому світу більш ніж на 14 годин. Увесь цей час головні інформаційні платформи для багатьох людей виявилися недоступними.

"Нам відомо, що в деяких людей у даний час виникають проблеми з доступом до сімейства додатків Facebook", – сказано в заяві, яку Facebook оприлюднив у Twitter. – Ми працюємо, щоб вирішити цю проблему якомога швидше".

У відповідь на чутки, опубліковані в інших соціальних мережах, компанія заявила, що збої не були результатом DDoS-атаки, яка навантажує цільові служби надзвичайно великими обсягами трафіку.

Телеканал NBC News згодом повідомив, що причина була пов'язана з "перевантаженими" базами даних.

Після відновлення роботи Facebook у коментарі виданню Bloomberg компанія повідомила, що вивчає "можливість повернення коштів рекламодавцям". Інформація про обсяги втрат і кількість постраждалих рекламодавців не оприлюднювалася.

Як виявилося, навіть кілька годин збою було достатньо, щоб завдати матеріальної шкоди підприємцям по всьому світу. Збій зачепив і сервіс Facebook Workplace, який використовується бізнесом для внутрішнього спілкування.

Дизайнер з Буенос-Айреса Ребекка Брукер повідомила Бі-бі-сі, що перерва суттєво вплинула на роботу її фірми.

"Facebook для особистого використання – це добре, але що відбувається, коли ми покладаємося на такі великі компанії, як ця, у наданні бізнес-послуг? – питає вона. – Я намагаюся спілкуватися зі своєю командою в Нью-Йорку. Facebook Workplace – наш єдиний канал для спілкування, за винятком електронної пошти".

"Ви не можете покладатися лише на соцмережі для побудови бізнесу, – каже Аманда Абела, авторка Amazon-бестселера "Зробіть гроші своїм медом". – Приклад: Instagram і Facebook сьогодні не працюють. Якщо весь ваш бізнес працює на вашій сторінці IG, ви сьогодні втрачаєте гроші. Ось чому я навчаю своїх клієнтів різних методів маркетингу та продажів".

7 травня 2020 року Facebook "зламав" додатки для iOS від компаній DoorDash, Spotify, TikTok і Venmo. Причиною стала проблема з комплектом розробки програмного забезпечення (SDK) від Facebook, який вбудований у роботу багатьох мобільних додатків від великих і малих компаній.

Проблема демонструє масштаби платформи соціальної мережі і те, як навіть незначні негаразди можуть мати серйозні наслідки для індустрії мобільного програмного забезпечення.

Facebook SDK – це набір програмних інструментів для розробників, який допомагає використовувати такі функції, як вхід в обліковий запис і надання кнопок загального доступу до соціальної мережі. Проблема полягала в тому, що SDK очікував відповіді сервера в певному форматі, який сервери Facebook не надавали.

"Facebook підштовхує розробників до установки свого SDK. Ймовірно, Facebook потрібні докладні дані, які можна збирати про користувачів цього додатка", – пояснює Гільєрме Рембо.

За його словами, SDK пропонується як зручний інструмент для розробників та маркетингових команд, оскільки його також можна використовувати для відстеження конверсій реклами, що розміщується через Facebook.

Компанія публічно не заявляла про жодну фінансову компенсацію за збій.

Кейс WhatsApp

1,6 млрд активних користувачів. Оборот і дохід невідомі.

8 вересня користувачі месенджера WhatsApp почали повідомляти про втрату історії чату після відкриття смс, що містило дивні текстові символи. Відкриття таких повідомлень призводило до зависання месенджера.

Повідомлення з дивними символами передавалися і за допомогою файлу vCards – стандартного формату, призначеного для пересилання електронних візитних карток, який дозволяє користувачам легко додавати контакти до своєї адресної книги.

Як виявилося, проблема була викликана помилкою програмного забезпечення, яка заважає WhatsApp обробляти комбінацію символів у повідомленнях, що призводить до "нескінченного збою". У результаті деякі користувачі, які не резервували свої розмови, втратили всю історію чату назавжди.

Повідомлення з дивним поєднанням кодів та символів походили з Бразилії і шкодили користувачам, які працювали з WhatsApp через пристрої iOS та Android. У компанії швидко помітили проблему і випустили відповідне оновлення.

До цього WhatsApp довелося виправляти проблему, через яку номери телефонів деяких користувачів відображалися в результатах пошуку Google.

За словами дослідника Атула Джаярама, ця проблема торкнулася щонайменше 300 тис телефонних номерів, які з'явилися в Google під час пошуку "сайт: we.me". Google проіндексував номери, оскільки WhatsApp не спромігся вчасно відключити сканування номерів сканером пошукового гіганта.

Попри значні збої в роботі, не було знайдено жодної згадки про компенсацію збитків користувачам з боку WhatsApp.

Кейс Telegram

400 млн активних користувачів. Дохід – 0,68 млрд дол.

Регулярні збої трапляються і в роботі Telegram. За останній місяць користувачі двічі скаржилися, що не можуть підключитися до сервісу і надіслати повідомлення. Проте помилки в роботі сервісу, які б призводили до значних репутаційних втрат, у Telegram відбувалися нечасто.

Останній інцидент трапився у вересні 2019 року. Тоді в сервісі була виявлена помилка, яка дозволяла адресату відкривати фото і відеофайли, які відправник надіслав помилково і видалив за допомогою відповідної функції Telegram.

Цю проблему виявив дослідник у сфері інформаційної безпеки Дхирадж Мішра. За його словами, хоча Telegram видаляв повідомлення з пристрою адресата, усі відправлені фотографії або відео все одно зберігалися у його телефоні.

"Це прекрасно працює і в групах, – прокоментував він для TechCrunch. – Якщо у вас є група Telegram із 100 тис учасників, і ви помилково відправляєте повідомлення для ЗМІ і видаляєте його, воно буде видалене тільки з чату, але залишиться в сховищі мультимедіа для всіх 100 тис учасників".

Невідомо, чи постраждали користувачі Telegram від проблеми з конфіденційністю, але раніше TechCrunch повідомляв про кілька випадків, коли власникам віз відмовили у в'їзді в США через контент на їх телефонах, відправлений їм іншими людьми.

Після звернення до TechCrunch Telegram виправив уразливість. Мішра отримав 2 500 євро винагороди за виявлення і розкриття уразливості.

Чому відбуваються збої

За словами експертів, є три основні причини "падіння" соцмереж і сервісів світового рівня.

1. Збій у зв'язку з оновленням. Жодна соцмережа не живе в стабільному стані. Для збереження конкурентоспроможності вона змушена проводити оновлення. Іноді після цього щось може піти не за планом.

Високе навантаження на сервери не гарантує виявлення всіх варіантів збою. У соцмережі щодня заходять мільйони людей, які користуються різними сценаріями поведінки. Якийсь з них може породити збій.

2. Фізичне падіння ключових серверів. Існує сценарій, коли відбувається атака на мережу. Це найбільш складний варіант, за якого зловмисник намагається перевантажити сервери.

З великої кількості IP-адрес у мережу подаються запити, які її перевантажують. Якщо йдеться про великі соцмережі, то з такими атаками вона може боротися. Оскільки соцмережі базово розраховані на величезну кількість запитів, масштаб атаки має бути вкрай великим.

3. Втручання провайдера. Тут два варіанти: або через помилки в налаштуваннях може неправильно фільтруватися трафік, або порушення роботи мережі проводиться на вимогу держави. В історії є приклади обох варіантів.

30 серпня сервіси Google, Cloudflare, Amazon, Microsoft та інших компаній були недоступними по всьому світу з вини американського провайдера CenturyLink. Через неправильні налаштування мережевого обладнання сайти не працювали кілька годин, і трафік просів на 3,5%. Це один з найбільших збоїв у роботі мережі за всю історію.

Порушення роботи мережі на вимогу держави недавно сталося в Білорусі. У КНР, РФ, Ірані, Туреччині та інших країнах такі заходи відбуваються регулярно.

Наслідки для користувачів та бізнесу

Для звичайних користувачів порушення в роботі інтернет-сервісів проходять майже непомітно. Дані не пропадають, оскільки сервіси дублюють їх на кількох серверах, розташованих у різних місцях. Користувач може втратити одну-дві публікації.

У той же час люди, які роблять бізнес за допомогою Facebook, Instagram, Telegram чи Viber, отримують збитки. Коли сервіс недоступний, бізнес-користувач втрачає гроші через зупинку замовлень: косметики в Instagram, їжі через канал ресторану у Viber, уживаного авто через канал у Telegram, китайських інструментів у таргетованих оголошеннях Facebook.

У квітні 2018 року Роскомнадзор спробував заблокувати в РФ Telegram. Блокування торкнулося значної кількості онлайн-магазинів, сервісів і соцмереж. Наприклад, онлайн-школа з вивчення англійської мови SkyEng втратила 25 тис дол через зірвані уроки.

Об'єднує всі збої в роботі соцмереж та інтернет-сервісів те, що рядові користувачі не мають жодного шансу на отримання грошової компенсації за втрачені гроші, контент, час і вигоду. Угоди-оферти, які користувачі погоджують на етапі встановлення додатку та реєстрації акаунту, написані передусім в інтересах інтернет-сервісів». ***(Всеволод Некрасов. Глобальний збій: чому "падають" сайти соцмереж та інтернет-сервісів і як це шкодить користувачам // Економічна правда (https://www.epravda.com.ua/publications/2020/10/23/666546/). 23.10.2020).***

***

Сполучені Штати Америки

«Джон Макафі, який розбагатів на продажу програмного забезпечення для кібербезпеки і в останні роки став пропагандистом криптовалюти, був звинувачений Міністерством юстиції (DOJ) в ухиленні від сплати податків. Міністерство юстиції повідомило, що він був заарештований в Іспанії і очікує екстрадиції.

McAfee протягом багатьох років має спірний зв'язок з законом, хоча часом неясно, які порушення реальні, а які сфабриковані. Колишній кандидат у президенти США від Лібертаріанської партії в 2020 році, він стверджував, що кампанія була "у вигнанні" після того, як у січні 2019 року йому було пред'явлено звинувачення в "використанні криптографічних засобів [sic] в злочинних діях проти уряду США". У тому ж відео він сказав, що не платив податки вісім років. (Це буде мати значення пізніше.) Він також заявив, що ЦРУ "намагався нас забрати" у своєму твіті в липні 2019 року з фотографією, на якій він був на човні з пістолетом в руках, що було частиною пригоди, яка закінчилася його арештом і звільненням в Домініканській Республіці. Республіка…» ***(Творця антивірусу Джона Макафі заарештували в Іспанії, названо причину // Знай.ua (https://techno.znaj.ua/341996-tvorcya-antivirusu-dzhona-makafi-zaareshtuvali-v-ispaniji-nazvano-prichinu). 06.10.2020).***

***

«Спустя семнадцать лет после того, как октябрь стал Национальным месяцем осведомленности о кибербезопасности, американцы, несомненно,

гораздо лучше осведомлены о цифровых угрозах. Но в сети они как никогда небезопасны.

Ежегодная пиар-кампания Министерства внутренней безопасности, призывающая компании и частных лиц оставаться в безопасности в Интернете, продолжающаяся с 2003 года, может получить дополнительную поддержку в этом году всего за 32 дня до наиболее пристально наблюдаемых президентских выборов в США с точки зрения безопасности - и во время пандемии коронавируса. поскольку все, от школы до работы и покупок продуктов, перемещается в онлайн.

«Вначале на самом деле речь шла о том, чтобы убедить людей, что они должны заботиться об этом вопросе», - сказала Дженни Менна, бывшая сотрудница DHS, которая управляла грантом для финансирования программы «Месяц осведомленности» в первые годы ее существования, а сейчас является руководителем службы кибербезопасности в компании. Банк США. «Из-за того состояния, в котором мы находимся сейчас, вам больше не нужно доказывать это. Теперь это: «Хорошо, теперь, когда мы привлекли ваше внимание, вот что вам нужно сделать, чтобы быть в большей безопасности».

Американцев, которые почти два десятилетия назад плохо понимали, что такое кибербезопасность, сейчас засыпают новостями об опасностях кибератак на избирательные системы, а также о возможности дезинформации и других цифровых опасностях, скрывающихся в их приложениях и платформах социальных сетей. Коронавирус также вызвал беспрецедентную волну атак, направленных на больницы и направленных на обман людей, отчаявшихся в результате увольнений и медицинских счетов. В более широком смысле, американцы, вероятно, получили шквал уведомлений от компаний о краже их данных или взломе паролей.

Согласно оценкам фирмы McAfee, занимающейся кибербезопасностью, и аналитического центра Центра стратегических и международных исследований, ежегодные расходы на киберпреступность, которые были сравнительно незначительными в 2003 году, выросли до более чем 80 миллиардов долларов в год к 2013 году и примерно до 600 миллиардов долларов в год к 2018 году.. C onsumers сообщили потери более чем на $ 152 млн мошенничества коронавируса связанного с началом пандемии, в соответствии с Федеральной торговой комиссией.

Но, несмотря на все усилия, направленные на повышение осведомленности о кибербезопасности, многие компании по-прежнему не следуют основным методам, разработанным для ограничения угроз взлома.

И подавляющее большинство кибератак совершается с очень небольшими усилиями, заставляя людей нажимать на подозрительные ссылки и вложения, когда они должны знать лучше.

Эта линия тренда заставляет некоторых профессионалов в области кибербезопасности сомневаться, что типичная кавалькада рекламы на основе слоганов и онлайн-тренингов Национального месяца осведомленности о кибербезопасности по-прежнему является лучшим способом остановить волну разрушительных взломов.

«Это отличная идея по идее, и в прошлом она имела некоторый успех», - заявил в Twitter Тони Коул, технический директор компании по кибербезопасности

Attivo Networks. «Тем не менее, сейчас 2020 год, и попытка сделать людей более осведомленными во всем похожа на крик в песчаную бурю».

По мнению Кельвина Коулмана, рост числа хаков показывает острую необходимость месяца осведомленности.

Коулман - исполнительный директор Национального альянса кибербезопасности, некоммерческой организации, которая с момента своего основания проводит месяц осведомленности на гранты от DHS.

Он сравнил события месяца с кампанией Лесной службы США «Только вы можете предотвратить лесные пожары», которую популяризировал Smokey Bear. «Никогда не бывает слишком много осознанности», - сказал мне Коулман.

Мероприятия месяца включают в себя рекламный блиц и множество онлайн-мероприятий. NCSA также разбивает месяц на еженедельные темы, которые в этом году включают «если вы подключите его, защитите его» и «обезопасьте устройства дома и на работе», что является намеком на всплеск телеработы во время пандемии. В этом году он меняет название месяца на просто «Месяц осведомленности о кибербезопасности» и убирает слово «национальный», чтобы подчеркнуть, что проблема выходит за пределы национальных границ.

NCSA также сотрудничает с десятками компаний и других организаций, которые проводят собственные мероприятия, призванные повысить осторожность сотрудников в отношении цифровых угроз. Подразделение кибербезопасности Министерства внутренней безопасности, например, использует месяц, чтобы сделать последний рывок в обеспечении безопасности государственных и местных избирательных систем перед ноябрьским голосованием.

«Национальный месяц осведомленности о кибербезопасности - это […] возможность повысить осведомленность о важной роли, которую мы все играем в кибербезопасности», - сказал мне старший советник отдела по безопасности на выборах Мэтт Мастерсон. «Избирательное сообщество знает это не хуже всех и на световые годы опережает то, что было четыре года назад».

Но Коулман также признает, что многим людям все еще не хватает элементарных знаний в области кибербезопасности.

«Три основных направления - это продукты, процессы и люди», - сказал он. «С самого начала кампании мы много внимания уделяли продуктам и процессам. Я не думаю, что мы достаточно сосредоточились на людях, на изменении человеческого поведения ».

По словам Менна, в этом месяце все больше внимания уделялось внедрению конкретных правил кибербезопасности, таких как использование сложных паролей и оповещение ИТ-персонала компании о подозрительных электронных письмах. Она развивалась «от осознания того, что это то, о чем вы должны думать, к осознанию последних вещей, которые вам следует делать», - сказала она.

Многие профессионалы в области кибербезопасности описали кампанию как полезную, но неадекватную для гигантской задачи по повышению кибербезопасности.

«Осведомленность важна... Но мы слишком сильно зависим от осведомленности, потому что люди будут делать ошибки, и бесконечные ресурсы, применяемые для повышения осведомленности, не изменят этого», - сказал мне

Фил Райтингер, бывший высокопоставленный сотрудник отдела кибербезопасности DHS, который сейчас возглавляет Global Cyber Alliance.. «Вам нужны технологии и осведомленность в правильных мерах, а не ожидать того, чего не может дать осознание».

Бо Вудс, научный сотрудник аналитического центра Атлантического совета по кибербезопасности, призвал переориентировать месяц на пропаганду реформ, которые заставят компании производить более безопасные продукты и лучше защищать данные людей. Он сравнил это с принятием и соблюдением правил пожарной безопасности, а не просто с пропагандой пожарной безопасности.

«Осведомленность - это первый шаг на пути к полному решению проблем, вызванных сбоями в кибербезопасности. Возможно, пора сделать следующий шаг к активизации действий», - сказал он…

Ключи

Российская группа, вмешавшаяся в выборы 2016 года, выдает себя за правый новостной сайт, нацеленный на избирателей.

Отдел новостей для американских и европейских граждан (NAEBC) управляется людьми, связанными с связанной с Кремлем фермой троллей - Агентством интернет-исследований, и размещает материалы, направленные на очернение кандидата в президенты от Демократической партии Джо Байдена и движение Black Lives Matter, сообщает Джек Стаббс из агентства Reuters.

На фальшивом сайте были перепечатаны статьи консервативных СМИ. Настоящим американцам платили также за то, что они писали о политически чувствительных вопросах. Джек сообщает, что сеть фиктивных аккаунтов, выдавая себя за редакторов и репортеров, затем продвигала эти истории в социальных сетях.

Facebook и Twitter в сентябре разоблачили аналогичное фальшивое левое СМИ, которое, по их словам, также принадлежит людям, связанным с ИРА. Новое разоблачение подчеркивает, как Кремль дезинформирует обе стороны на выборах.

NAEBC описывает себя как «свободное и независимое» СМИ, базирующееся в Венгрии. Предупреждение на главной странице гласит: «Не дайте себя обмануть». После того как агентство Reuters связалось с сайтом по поводу его ссылок на IRA, аккаунты предполагаемых сотрудников в социальных сетях удалили ссылки на сайт и удалили предыдущие сообщения.

Твиттер удалил 130 аккаунтов, связанных с Ираном, которые пытались сорвать дискурс вокруг президентских дебатов во вторник.

Учетные записи были удалены на основе разведданных, предоставленных ФБР, говорится в сообщении компании. По словам Twitter, учетные записи имели низкую вовлеченность и не оказали существенного влияния…

ФБР и DHS предупредили, что Иран, Китай и Россия попытаются распространить дезинформацию, чтобы повлиять на выборы. На прошлой неделе Facebook удалил китайские аккаунты, нацеленные на Байдена и Трампа. У этих аккаунтов также была низкая вовлеченность.

Высокопоставленные представители АНБ и ЦРУ пытались помешать шефу Трампа опубликовать непроверенные утверждения кремлевской разведки о Хиллари Клинтон.

Должностные лица в собственном офисе директора национальной разведки Джона Рэтклиффа также заявили, что обмен информацией с Конгрессом может укрепить доверие к непроверенным заявлениям России Дастина Волца и Уоррена П. Стробла в отчете Wall Street Journal.

Анализ российской разведки, полученный шпионскими агентствами США, которым Рэтклифф поделился с Судебным комитетом Сената, уже был отклонен сенатским комитетом по разведке как не имеющий фактической основы. В нем утверждалось, что Клинтон одобрила план кампании на 2016 год, чтобы связать Трампа со взломом Москвой электронной почты демократов.

Рэтклифф признал в своем письме председателю судебной системы Сената Линдси О. Грэму (RS.C.), что разведывательное сообщество не могло подтвердить «точность этого утверждения или степень, в которой анализ российской разведки может отражать преувеличения или фальсификации».”

Решение Рэтклиффа поделиться непроверенными разведданными также озадачило бывшего директора ФБР Джеймса Б. Коми, который вчера дал показания перед Судебным комитетом Сената.

«Я действительно не знаю, что он делает, - сказал Коми.

Коми также защищал расследование бюро 2016 года о возможной координации между кампанией Трампа и Россией, сообщают Мэтт Запотоски, Девлин Барретт и Карун Демирджян.

Страховая компания Anthem заплатит почти 40 миллионов долларов, чтобы уладить расследование утечки данных в 2015 году.

Как сообщает Дания Надим из Reuters, расследование ФБР не обнаружило никаких доказательств того, что украденная информация привела к мошенничеству.

Официальные лица США заявили, что за нарушением стоит китайское правительство, и в 2019 году гражданину Китая были предъявлены обвинения в связи с этим.

Расследование ФБР не нашло никаких доказательств того, что украденная информация привела к мошенничеству. В рамках соглашения с генеральными прокурорами штата Anthem будет укреплять свои методы кибербезопасности.

Хеппенинги на холмах

В новом докладе Палаты представителей говорится, что Соединенные Штаты могут отставать от Китая, если они не изменят свой подход к технологиям и безопасности.

37-страничный отчет призывает к «значительному перераспределению ресурсов» и расширению сбора разведывательной информации о Китае, сообщает Карун Демирджян.

В отчете также осуждается то, что Вашингтон не готов к «мягким» угрозам, таким как новый коронавирус. В нем конкретно не упоминается реакция администрации Трампа на пандемию.

Обеспечение избирательного бюллетеня

Волнения на выборах подогревают предвыборную гонку среди государственных служащих избирательных органов.

Претенденты атакуют действующих республиканцев в Западной Вирджинии и штате Вашингтон по поводу использования ими новых избирательных технологий, сообщает Эрик Геллер из Politico. Демократы говорят, что технологии ставят под сомнение целостность рас в штатах.

Нападки Трампа на бюллетени, рассылаемые по почте, также дали боеприпасы демократам штата Вашингтон, которые говорят, что действующий госсекретарь Ким Вайман, республиканец, не сделал достаточно, чтобы опровергнуть нападки президента. Штат Вашингтон голосует почти полностью по почте…

Глобальное киберпространство

Госсекретарь Майк Помпео предупредил итальянское руководство об угрозе китайских технологий.

Помпео призвал министра иностранных дел Италии Луиджи ди Майо «внимательно рассмотреть риски для своей национальной безопасности и частной жизни своих граждан, которые представляют технологические компании, связанные с Партией китайского сообщества», - сообщает Анджело Аманте из Reuters.

Соединенные Штаты подталкивают западных союзников к запрету Huawei и других китайских компаний, которые они считают угрозой национальной безопасности в связи с развитием 5G.

Тем временем Huawei открыла центр кибербезопасности в Риме, чтобы убедить правительства, что ее технология не используется в качестве инструмента китайского шпионажа. «Мы откроем наши внутренности, мы готовы к вивисекции, чтобы отреагировать на все это политическое давление», - сказал на открытии глава итальянского подразделения Луиджи Де Веккис, сообщает Reuters.

По словам Де Веккиса, открытие центра в тот же день, когда Помпео прибыл в Италию, было случайностью…» ***(Joseph Marks. The Cybersecurity 202: Americans are as insecure as ever on the 17th annual Cybersecurity Awareness month // The Washington Post (https://www.washingtonpost.com/politics/2020/10/01/cybersecurity-202-americans-are-insecure-ever-17th-annual-cybersecurity-awareness-month/). 01.10.2020).***

***

«Команда з модернізації тактичної мережі армії США хоче інтегрувати носяться пристрої з новими бойовими окулярами з доповненою реальністю в якості засобу підвищення кібербезпеки.

Дональд Коултер, старший радник з науки та технологій мережевої крос-функціональної групи, заявив у понеділок на веб-семінарі, організованому C4ISRNET, що одним з пріоритетів команди на наступний рік є просування носяться технологій для аутентифікації користувачів.

Відповідно до поточних можливостей, користувачі проходять аутентифікацію з використанням паролів, загальних карт доступу або токенів для перевірки. Але цих можливостей недостатньо в операційному середовищі, сказав Коултер.

"Вони можуть бути зламані, пошкоджені [або] втрачені в умовах експлуатації", - сказав він. "Спроба ввести пароль в тактичних рукавичках за допомогою крихітної клавіатури, - не оптимальне рішення".

За допомогою носяться пристроїв особистість солдатів перевіряється з використанням біометричних даних, таких як частота серцевих скорочень, ХОДА, унікальні сигнатури шкіри і фізичне місце розташування. У носяться технологій двоякі переваги: вони роблять системи армії більш безпечними, але при цьому більш інтуїтивно зрозумілими для солдатів в польових умовах…» ***(Зброя солдатів армії США обзаведеться власними паролями // Знай.ua (https://techno.znaj.ua/346776-zbroya-soldativ-armiji-ssha-obzavedetsya-vlasnimi-parolyami). 27.10.2020).***

***

Російська Федерація та країни ЄАЕС

«Белорусские "киберпартизаны" готовят масштабную атаку на банковскую систему страны. Они призвали граждан снять наличные с банковских карт и отозвать депозиты со счетов госбанков.

Белорусские хакеры заявили, что они создали вредоносное программное обеспечение для банковских систем – троян. Он рассчитан на массовое внедрение в банкоматы. Об этом сообщили на телеграм-канале "Киберпартизаны".

"Киберпартизаны" заявили, что к вечеру 9 октября 2020 года угрозы для банковской системы нет.

Рекомендации: до конца рабочей недели выгрести всю валюту из обменников. Обналичить банковские карты. Отозвать депозиты со счетов государственных банков. Немедленно, – говорилось в сообщении.

Другие кибератаки в Беларуси

Белорусские хакеры 25 сентября 2020 года объявили об атаке на режим самопровозглашенного действующего президента Беларуси Александра Лукашенко. Они проинформировали, что "тотально будут атаковать" режим Лукашенко в конце сентября.

Также хакеры уже устраивали атаки на государственные сайты. На сайте МВД Беларуси объявили в розыск Александра Лукашенко и министра внутренних дел Юрия Караева. А впоследствии изъяли и опубликовали личные данные работников силовых структур». ***(Анастасия Мигидюк. Новая масштабная атака на банковскую систему Беларуси: "киберпартизаны" вернулись // Телеканал новостей «24» (https://techno.24tv.ua/ru/novaja-masshtabnaja-ataka-bankovskuju-sistemu-novosti-belarus_n1430273). 07.10.2020).***

***

«Финансирование федерального проекта «Информационная безопасность» нацпрограммы «Цифровая экономика» в 2022 и 2023 годах увеличится в восемь раз — до 16 млрд рублей. Это следует из проекта федерального бюджета на 2021-й и плановый период 2022–2023 годов, а также

новой версии паспорта федерального проекта («Известия» ознакомились с документами).

В период с 2021 по 2024 годы финансирование этого направления может составить 26,3 млрд рублей. В текущей версии паспорта на «Информационную безопасность» в ближайшие четыре года собирались выделить 7,6 млрд рублей.

Почти половину бюджета может забрать на себя создание и функционирование национального технологического центра внедрения методов современной криптографии. Это самое капиталоемкое мероприятие федпроекта. На него понадобится 11,5 млрд рублей госфинансирования.

Самая затратная часть может лечь на техническую реализацию федерального проекта, говорит руководитель отдела аналитики «СёрчИнформ» Алексей Парфентьев. К таким мероприятиям можно отнести проекты по фильтрации интернет-трафика, противодействию компьютерным атакам и созданию киберполигонов. Впрочем, в проект, по крайней мере в явном виде, не вошли меры, направленные на пресечение утечек и защиту персональных данных граждан, добавляет он». ***(Траты на информбезопасность в России могут увеличить в восемь раз // Известия (https://iz.ru/1068369/2020-10-02/traty-na-informbezopasnost-v-rossii-mogut-uvelichit-v-vosem-raz). 02.10.2020).***

***

«Отмечается, что на сайте разместили новости и фото, касающиеся встреч Тихановской с президентом Франции Эммануэлем Макроном, канцлером Германии Ангелой Меркель и другими политиками ЕС.

«Киберпартизаны» также разместили там ссылку на список граждан Белоруссии, которых арестовали во время или после выборов главы республики. Оппозиция не раз подчеркивала, что считает этих людей политическими заключенными, и требует их освобождения.

Кроме того, на сайте национального архива Белоруссии появился логотип «белорусских киберпартизан». Они атакуют государственные структуры страны уже не в первый раз. Хакеры начали действовать после выборов, в знак несогласия с их итогами…». ***(Киберпартизаны взломали сайт национального архива Белоруссии // SecurityLab.ru (https://www.securitylab.ru/news/512911.php). 11.10.2020).***

***

«Более 600 полицейских из всех регионов России пройдут подготовку в области кибербезопасности. Учебный курс организован Департаментом государственной службы и кадров МВД России совместно с Центральным банком России и организацией «Цифровая экономика» для сотрудников специализированных подразделений по противодействию ИТ-преступлениям, созданных в структуре министерства в 2020 году.

В разработке курса приняли участие профильные подразделения центрального аппарата МВД России, также к проведению занятий привлекаются эксперты Банка России, кредитно-финансовых организаций, заинтересованных

федеральных государственных органов власти, ведущих отечественных компаний в сфере информационной безопасности.

Обучение пройдет в дистанционном формате с 19 октября по 25 декабря. Занятия состоятся в форме лекций и практических тренингов при постоянной онлайн-коммуникации с аудиторией. Видеоконференции будут организованы в среднем 3 раза в неделю с возможностью дополнительного или повторного просмотра материала на выделенном интернет-ресурсе.

В рамках курса планируется рассмотреть вопросы нормативного и технологического обеспечения информационной безопасности в организациях кредитно-финансовой сферы, правовые и технические аспекты, связанные с использованием цифровых финансовых активов. Преподаватели и слушатели проанализируют проблемы хищения данных с применением методов социальной инженерии, фишинга, подмены номера и других цифровых атак на людей. Оценку получат инструменты интернет-разведки и компьютерной криминалистики, акцент будет сделан на практических аспектах расследования киберинцидентов, способах установления личностей мошенников и многом другом.

Необходимость совершенствования профессиональной подготовленности сотрудников Министерства внутренних дел обусловлена ростом преступности в сфере IT-технологий. С начала года в России зафиксировано 363 тысяч киберпреступлений, что на 77 % больше, чем за аналогичный период прошлого года. В каждом пятом регионе страны их число увеличилось в два и более раза.

Обучение проводится в рамках реализации федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации», а также комплекса мероприятий по переподготовке и повышению квалификации сотрудников МВД России, которые специализируются на противодействии преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий.

«Для подготовки данного мероприятия в рамках федпроекта «Информационная безопасность» была проведена огромная работа по привлечению компаний в сфере информационной безопасности – таких как InfoWatch, Лаборатория Касперского, Сбер, Ростелеком-Солар, ИнфоТеКС, Group-IB, Positive Technologies. Особо хочется отметить участие Банка России, который на безвозмездной основе предоставил технологическую площадку для возможности проведения обучения лучшим практикам в сфере информационной безопасности оперативным подразделениям правоохранительных органов», - комментирует Николай Зубарев, директор по направлению «Информационная безопасность» организации «Цифровая экономика». ***(Борцы с киберпреступностью пройдут спецподготовку // ООО "ИКС-МЕДИА (http://www.iksmedia.ru/news/5697334-Borcy-s-kiberprestupnostyu-projdut.html). 16.10.2020).***

***

«В четверг, 22 октября, на пленарном заседании дискуссионного клуба «Валдай» президент России Владимир Путин призвал добиваться бесперебойной и безопасной работы мирового киберпространства.

Как отметил глава государства, сейчас в мире формируется «практически бесконечное цифровое пространство, и люди с каждым годом осваивают его все быстрее». По его словам, вынужденные ограничения из-за пандемии COVID-19 стимулировали развитие дистанционных электронных технологий, и «коммуникация, в основе которой лежит интернет, превратилась во всеобщее достояние». В связи с этим необходимо сделать все возможное для обеспечения бесперебойной и безопасной работы киберпространства во всем мире.

По словам Путина, если США откажутся от сотрудничества с РФ в вопросе обеспечения международной кибербезопасности, Россия готова к диалогу со всеми заинтересованными партнерами. Как отметил глава государства, времена, когда все важнейшие международные вопросы решались между Москвой и Вашингтоном, давно прошли. Поэтому в настоящее время Россия активно продвигает двусторонние и многосторонние договоренности в сфере кибербезопасности. Вместе с тем, Путин выразил надежду, что следующий президент США и его администрация все-таки согласятся начать разговор по данному вопросу.

Касательно обеспечения бесперебойной и безопасной работы киберпространства президент предложил создать инструменты контроля за невмешательством во внутренние дела стран в киберпространстве. Глава государства отметил, что не предлагает ничего такого, что не соответствовало бы интересам партнеров.

«Если кто-то считает, что кто-то другой вмешивается в их дела, то давайте установим общие правила и выработаем инструменты верификации, контроля за тем, как мы исполняем наши договоренности», - отметил Владимир Путин.

Как заявил президент, Россия не вмешивается в киберпространства других стран, что доказано многочисленными исследованиями. Поэтому речи о «цифровом перемирии» межу Москвой и Вашингтоном быть не может, поскольку оно и так уже есть». ***(Путин предложил создать инструменты контроля за невмешательством в киберпространства стран // SecurityLab.ru (https://www.securitylab.ru/news/513315.php). 23.10.2020).***

***

Інші країни

«Информационная безопасность является таким же общественным благом, как чистая питьевая вода. Об этом в четверг, 1 октября, заявил помощник начальника Агентства по кибербезопасности Сингапура бригадный генерал Гаурав Киртхи (Gaurav Keerthi) на конференции Black Hat Asia.

По словам Киртхи, правительство Сингапура намерено обеспечить гражданам и компаниям безопасную информационную среду точно так же, как обеспечивает их другими общественными благами, такими как водопровод и канализация. Уже со следующей недели в Сингапуре начнется реализация схемы по улучшению кибергигиены путем добровольной оценки безопасности шлюзов широкополосного доступа, предоставляемых интернет-провайдерами своим пользователям.

Киртхи сравнил обеспечение информационной безопасности в наши дни с тем, как два столетия назад в Сингапуре относились к водопроводу и канализации. Как пояснил бригадный генерал, в 19-м веке добывание питьевой воды, утилизация отходов и гигиена были личной ответственностью каждого гражданина. В результате в стране начались эпидемии, и властям пришлось принимать меры. Решением проблемы стало проведение общественного водопровода и канализации.

По словам Киртхи, в настоящее время власти Сингапура ведут себя так же, как в 19-м веке, полагаясь в столь критическом вопросе, как кибергигиена, на граждан. Однако зависимость общества от цифровых технологий день ото дня становится все сильнее, поэтому правительство страны решило, что пришло время относиться к информационной безопасности как к общественному благу наподобие чистой воды.

Сингапурские власти предложили общенациональную схему идентификации граждан SingPass, в рамках которой пользователи «привязывается» к сервисам. Эта схема может также бесплатно использоваться организациями, в том числе банками, для идентификации клиентов. Такой подход освободит их от дополнительной финансовой нагрузки из-за разработки собственных решений для идентификации.

Кроме того, на следующей неделе правительство представит сервис «маркировки пользователей». Предполагается, что интернет-провайдеры должны будут предоставлять своим пользователям шлюзы широкополосного доступа, получившие оценку безопасности в четыре звезды. Таким образом власти намерены побудить вендоров к получению хороших оценок и инвестициям, которые сделают их продукты и, следовательно, Сингапур, более безопасными». ***(Власти Сингапура предложили относиться к ИБ как общественному благу // SecurityLab.ru (https://www.securitylab.ru/news/512644.php). 01.10.2020).***

***

Протидія зовнішній кібернетичній агресії

«Євросоюз запустив процедуру введення санкцій через кібератаку на німецький бундестаг, ймовірно зроблену з Росії в 2015 році. Посли 27 країн — членів ЄС в середу, 7 жовтня, домовилися ввести візові заборони щодо двох фізичних осіб та заблокувати їхні рахунки на території Євросоюзу…

Інформація щодо особистості і громадянства підданих санкціям осіб буде оприлюднена лише після вступу штрафних заходів в силу. За даними AFP, в списку санкцій присутня також одна організація. Остаточне рішення з приводу введення штрафних заходів повинні затвердити уряди країн — членів Євросоюзу.

Кібератака на німецький бундестаг в травні 2015 року паралізувала IT-інфраструктуру парламенту ФРН, бундестаг довелося повністю відключити від інтернету на кілька днів. Канцлер ФРН Ангела Меркель в травні 2020 року поклала відповідальність за те, що трапилося на Росію.

За повідомленнями ЗМІ, німецькі слідчі зробили висновок, що атака могла виходити від одного з агентів російського ГРУ. У зв’язку з цим Федеральна прокуратура ФРН 5 травня видала ордер на арешт громадянина Росії Дмитра

Бадіна. Москва категорично відкинула причетність до кібератаки на німецький бундестаг…». ***(Ілля Нежигай. ЄС узгодив санкції через кібератаки на німецький бундестаг // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1895961-yes-uzgodiv-sanktsiyi-cherez-kiberataki-na-nimetskiy-bundestag). 08.10.2020).***

***

«У соціальній мережі Twitter заблокували 1 589 акаунтів користувачів з Ірану, Саудівської Аравії, Куби й Таїланду за порушення політики компанії з маніпулювання платформою…

Заблоковані акаунти були пов'язані з інформаційними операціями, проведеними перерахованими країнами. Twitter дав детальну інформацію про ці облікові записи.

Крім цього в соцмережі внесли до своїх архівів п'ять акаунтів, пов'язаних з Росією, але закритих ще у вересні.

Облікові записи, що діють в Ірані, створювали агресію на політично чутливі теми, наприклад про расову та соціальної справедливості в США, русі Black Lives Matter і вбивстві Джорджа Флойда. Багато з цих облікових записів раніше були зламані зловмисниками, але Twitter повернув їх початковим власникам.

Заблоковано 33 аккаунта, пов'язаних з урядом Саудівської Аравії. Через них хакери видавали себе за ключових політичних фігур Катару і просували теми про політику Катару, які вигідні владі Саудівської Аравії.

Twitter також закрив 526 фейкові акаунти, якими управляли молодіжні групи, пов'язані з кубинським урядом, і ще 926 акаунтів, що імовірно знаходяться у віданні Королівської армії Таїланду (RTA).

Російські акаунти були пов'язані з фабрикою тролів.

Раніше Twitter видалив близько 178 000 облікових записів, пов'язаних з Китаєм, Росією і Туреччиною. Компанія додала в свій архів відомості про 32 242 з них…». ***(Андрей Лысенко. У Twitter заблокували 1 500 акаунтів з чотирьох країн // Дзеркало тижня. Україна (https://zn.ua/ukr/WORLD/u-twitter-zablokuvali-1-500-akauntiv-z-chotirokh-krajin.html#). 09.10.2020).***

***

«Міністерство внутрішньої безпеки (МВБ) США в доповіді "Оцінка національної загрози 2020" назвало Росію основною країною, що розповсюджує дезінформацію і створює загрозу кібербезпеці…

"Росія є, ймовірно, основним суб'єктом таємного впливу і постачальником дезінформації всередині країни", – йдеться в доповіді "Оцінка національної загрози 2020".

"Ми вважаємо, що головна мета Москви полягає в тому, щоб посилити своє світове становище і вплив шляхом ослаблення Америки – всередині країни і за кордоном – за допомогою зусиль із сіяння розбрату, відволікання уваги, формування громадських настроїв і підриву довіри до західних демократичних інститутів і процесів", – зазначають у міністерстві.

Згідно з доповіддю, “діяльність з іноземної експансії буде націлена на зовнішню і внутрішню політику США, міжнародні події, такі як COVID-19, а також демократичні процеси й інститути, включаючи президентські вибори 2020 року”.

Крім Росії, серед країн, які представляють кіберзагрозу США, названо Китай, Іран і Північну Корею». ***(У США вважають Росію найбільшою загрозою у сфері кібербезпеки // ТРК «ТВА» (https://tva.ua/2020/10/07/u-ssha-vvazhaiut-rosiiu-najbilshoiu-zahrozoiu-u-sferi-kiberbezpeky/). 07.10.2020).***

***

«Агентство по кибербезопасности и инфраструктурной безопасности в США (CISA) обнаружило хакерскую атаку на правительственные сети. Какую именно информацию могли получить хакеры после взлома, не сообщается. Об этом говорится на сайте агентства.

Атака проводилась на федеральном уровне, а также уровне территорий, резерваций и штатов. Предполагается, что атака связана с выборами, однако подтверждения этому пока что нет…». ***(В США хакеры атаковали правительственные сети // Journalist (https://journalist.today/v-ssha-hakery-atakovali-pravitelstvennye-seti/). 10.10.2020).***

***

«Російська військова розвідка планувала кібератаку на Олімпійські та Паралімпійські ігри 2020 (які планувалося провести цього літа в Токіо), щоб зірвати головну спортивну подію у світі.

Про це повідомляє Національний центр кібербезпеки Великої Британії, розкриваючи спільну операцію з американською розвідкою.

Російська кібердіяльність охоплювала організаторів Ігор, логістичні служби та спонсорів і велася до того, як Олімпіада була відкладена через коронавірус. Багато раніше приписувані росіянам кібератаки були спрямовані проти державних інститутів політичних супротивників Москви, але деяка кіберактивність була спрямована й на агентства, які проводять розслідування щодо допінгу в російському спорті.

Нові свідоцтва є першою ознакою того, що Росія була готова зайти так далеко, щоб зірвати літні Ігри, з яких всі російські учасники були виключені через постійні порушення допінгу, спонсоровані державою.

Велика Британія також стала першим урядом, який підтвердив деталі масштабів спроби Росії зірвати зимові Олімпійські і Паралімпійські ігри 2018 року в Пхенчхані, Південна Корея. Було заявлено з упевненістю в 95%, що спроба зриву зимових і літніх Олімпійських ігор був проведена віддалено підрозділом ГРУ.

У Пхенчхані, за даними Великої Британії, кіберпідрозділ ГРУ спробував замаскуватися під північнокорейських і китайських хакерів, коли націлився на церемонію відкриття зимових Ігор 2018 року, в результаті чого був зупинений вебсайт, щоб глядачі не могли розпечатати квитки, та відключився Wi-Fi на стадіоні.

У число основних цілей також входили телемовники, гірськолижний курорт, офіційні особи Олімпійських ігор, постачальники послуг і спонсори ігор в 2018 році, а це означає, що об'єкти атак були не тільки у Кореї. ГРУ також розвернуло шкідливе ПО для видалення даних в IT-системах зимових Ігор і націлилося на пристрої по всій Південній Кореї за допомогою VPN.

Велика Британія виходить з того, що розвідувальна робота перед літніми Олімпійськими іграми, включаючи цілеспрямований фішинг для збору ключових даних про облікові записи, створення підроблених вебсайтів і дослідження безпеки індивідуальних облікових записів, була розроблена для створення такої ж форми порушень, що зробить Ігри логістичним жахом для бізнесу, глядачів і спортсменів…». ***(Російські хакери готували кібератаку на Олімпіаду-2020 у Токіо // Champion.com.ua (https://champion.com.ua/others/2020/10/20/856018/rosiyski-hakeri-gotuvali-kiberataku-na-olimpiadu-2020-u-tokio). 20.10.2020).***

***

«Уряд США висунув офіційні обвинувачення офіцерам ГРУ Росії через причетність до організації міжнародних хакерських атак, у тому числі, проти України, а також поширення небезпечних вірусних програм, що спричинили мільярдні збитки.

Про це повідомило в понеділок американське впливове видання The Washington Post…

"Сполучені Штати в понеділок висунули кримінальне обвинувачення проти шести офіцерів російської розвідки у зв'язку з рядом найбільш шкідливих міжнародних кібератак, у тому числі, зриву роботи електромережі в Україні та запуску вірусу-вимагателя NotPetya, який заразив комп'ютери по всьому світу, завдавши збитків на мільярди доларів", - зазначається в повідомленні.

У звинувачувальному акті фігурують росіяни Юрій Андрієнко, Сергій Детистов, Павел Фролов, Артем Очиченко, Петро Пліскін, Анатолій Ковальов. Як уточнюється, всі вони є офіцерами в/ч 74455 Головного управління розвідки Генштабу РФ, яке "було причетне до зусиль щодо втручання у президентську кампанію 2016 року".

При цьому зазначається, що зловмисного впливу кібератак, організованих офіцерами ГРУ зазнали, в тому числі, міжнародні корпорації, організації, політичні кампанії, уряди, а також Зимові Олімпійські ігри 2018 року.

"Жодна країна не використовувала свої кіберможливості в якості зброї настільки згубно й безвідповідально, як Росія", - заявив під час оголошення обвинувального акту помічник генерального прокурора Джон Демерс.

Він підкреслив, що росіяни безглуздо завдавали побічних безпрецедентних збитків для досягнення невеликих тактичних переваг та задоволення злого умислу…». ***(США офіційно звинуватили офіцерів ГРУ Росії у хакерських атаках – WP // Эксперт-Центр (http://expert.org.ua/v-mire/2020/ssha-oficiyno-zvinuvatili-oficeriv-gru-rosiyi-u-hakerskih-atakah-wp). 19.10.2020).***

***

«Держсекретар США Майкл Помпео закликав всі країни приєднатися до притягнення до відповідальності шести росіян, які причетні до кіберзлочинів. Про це йдеться в поширеній у понеділок заяві Помпео. “Подібна кіберактивність говорить про повну зневагу до громадської безпеки і міжнародної стабільності”, — повідомив Помпео. Держсекретар США закликав Росію припинити “безвідповідальну поведінку”. “Ми також закликаємо всі країни, що зацікавлені в більшій стабільності в кіберпросторі, приєднатися до США з тим, щоб звинувачені сьогодні особи постали перед правосуддям”, — додав Помпео. Раніше судова влада США висунула обвинувачення проти шести росіян у зв’язку з хакерськими атаками проти компаній в США та у світі, зокрема за кібератаку на енергосистему України і учасників президентських виборів 2017 року у Франції». ***(Держсекретар США закликав країни приєднатися до переслідування кіберзлочинців з Росії // информационный портал "ua.today" (http://ua.today/news/world/derzhsekretar_ssha_zaklikav_krayini_priyednatisya_do_peresliduvannya_kiberzlochinciv_z_rosiyi). 20.10.2020).***

***

«У очільника Кремля Володимира Путіна виникли масштабні проблеми на міжнародній арені після того, як стало відомо, що Департамент юстиції США висунув офіційні звинувачення шести співробітникам ГРУ Російської Федерації, вважаючи їх винними у скоєнні низки глобальних кібератак. Варто звернути увагу на те, що усі шестеро є представниками військового підрозділу 74455 Генерального розвідувального управління РФ. Що також важливо розуміти, раніше Мін’юст Штатів вже висував звинувачення проти членів цього ж підрозділу, відомих як "Sandworm Team," за їхню роль у спробах офіційної Москви втрутитися у президентські вибори в США у 2016 році. Російських офіцерів не вважають причетними до втручання в американські вибори, але винуватцями низки інших кібератак. Окрім Sandworm Team, вони іноді діяли як "Telebots," "Voodoo Bear" та "Iron Viking", передає ONLINE.UA. Влада США переконана, що саме ці особи відповідальні за атаку на електромережі України у 2015 та 2016 роках. Окрім того, вони стояли за літньою кібератакою вірусу "NotPetya", який раніше вважався "вимагачем", однак насправді єдиною його ціллю було заблокувати роботу сотень установ і компаній. "Ця безвідповідальна поведінка вплинула і на критичну інфраструктуру, як транспорт та охорона здоров’я, і не лише в Україні, але й навіть у Західній Пенсильванії. Вважається, що лише для трьох пов’язаних із США жертв цієї атаки, з-поміж сотень інших, фінансові втрати склали близько мільярда доларів", — кажуть у Департаменті юстиції США. Не можна також не звернути увагу на те, що саме уих самих хакерів-співробітників ГРУ із "Sandworm Team" вважають винними у кібератаці на зимові Олімпійські ігри у Південній Кореї у 2018 році, а також — на сайти урядових структур та громадських організацій у Грузії в жовтні 2019 року. Що також важливо розуміти, докази для звинувачення готувала команда прокурорів разом із Федеральним бюро розслідування США, у співпраці з низкою компаній, серед яких Cisco’s Talos Intelligence Group, Facebook, Google і Twitter, а також правоохоронними структурами України, Грузії, Південної Кореї та Нової Зеландії». ***(Путін зіткнувся з новими серйозними проблемами***

через офіцерів ГРУ // ONLINE.UA(https://novyny.online.ua/putin-zitknuvsya-z-novimi-seryoznimi-problemami-cherez-ofitseriv-gru_n826195/). 20.10.2020).

***

«Міністр закордонних справ Норвегії Іне Еріксен Сёрейде звинуватила Росію в хакерській атаці на норвезький парламент - Стортинг, про яку стало відомо 24 серпня, повідомляє Deutsche Welle.

Про це йдеться в заяві, опублікованій на сайті зовнішньополітичного відомства у вівторок, 13 жовтня.

«Виходячи з наявної у уряду інформації, ми вважаємо, що Росія несе відповідальність за цю операцію», - наголошується в заяві.

Атака на поштові системи парламенту названа дуже серйозним інцидентом, що зачіпають найважливіший демократичний інститут Норвегії. «Зростаюче використання цифрових рішень означає, що загрози проти нас також перемістилися на цифрову арену», - заявили в МЗС.

Раніше керівник ІТ-відділу норвезького парламенту Маріана Андреассен повідомила, що Стортинг став жертвою кібератаки, спрямованої на внутрішню систему електронної пошти. Зазначалося, що з поштових скриньок деяких представників парламенту були викрадені великі обсяги даних…» ***(Юлия Абрамова. Норвегія звинуватила Росію в хакерській атаці на парламент // Дзеркало тижня. Україна (https://zn.ua/ukr/WORLD/norvehija-zvinuvatila-rosiju-v-khakerskij-atatsi-na-parlament.html). 14.10.2020).***

***

«Глава МЗС України Дмитро Кулеба закликав притягнути Росію до відповідальності за кібератаку на парламент Норвегії.

З такою заявою міністр виступив у середу ввечері 14 жовтня…

"Росія повинна понести відповідальність за кібератаки на парламент Норвегії", - написав Кулеба у своєму Twitter.

"Євроатлантична солідарність і взаємна підтримка мають ключове значення для протидії викликам гібридної війни", - підкреслив Кулеба.

Заява Кулеби надійшла наступного дня після того, як МЗС Норвегії звинуватило Росію у кібератаці на парламент країни.

Масштабний злам системи електронної пошти парламенту Норвегії відбувся 24 серпня». ***(Кулеба: Росія має відповісти за кібератаку на парламент Норвегії // Європейська правда (https://www.eurointegration.com.ua/news/2020/10/15/7115350/). 15.10.2020).***

***

«Дипломатическое представительство РФ в Соединённом Королевстве Великобритании и Северной Ирландии опубликовало комментарий на заявление официального Лондона.

По словам представителей российского посольства, новые обвинения в адрес нашей страны в кибератаках – это «неспровоцированные зловредные выпады» с целью «вбить клин» между Россией и другими государствами. В данном случае

речь идёт о Южной Корее и Японии, но такие методы уже применялись в отношении Украины и Грузии, заявили в дипломатическом представительстве.

«Эти "старания" разрушительны для российско-британских отношений и для международного престижа Великобритании», - говорится в сообщении.

Дипломаты считают, что британцы не хотят разбираться в инцидентах, а лишь стремятся очернить Россию. Такая активность вызвана, судя по всему, предстоящими в США выборами, отмечают в посольстве. Чем больше «козырей» они соберут, тем больше будет поводов обвинить РФ во вмешательстве в избирательный процесс.» ***(Российские дипломаты назвали обвинения в кибератаках «зловредными выпадами» Лондона // RuNews24.ru (https://runews24.ru/politics/20/10/2020/a787019e890b98d935495563b52d2bfc). 20.10.2020).***

***

«Группа анализа угроз Google проливает больше света на целевой фишинг учетных данных и вредоносные атаки на сотрудников президентской кампании Джо Байдена.

Хакеры рассылали сотрудникам президентской кампании Джо Байдена вредоносные электронные письма, которые выдавали себя за антивирусную компанию McAfee, и использовали ряд законных сервисов (например, Dropbox), чтобы избежать обнаружения. Электронные письма были попыткой украсть учетные данные сотрудников и заразить их вредоносным ПО.

Неудачные атаки передовых устойчивых групп угроз (APT) на кампанию Байдена были впервые обнаружены в июне вместе с кибератаками, нацеленными на кампанию Дональда Трампа. Однако подробности самих атак и использованной тактики были скудными до пятничного анализа Google Threat Analysis Group (TAG).

«В одном примере злоумышленники выдавали себя за McAfee», - заявили исследователи в пятницу. «Целям будет предложено установить легитимную версию антивирусного программного обеспечения McAfee с GitHub, в то время как вредоносное ПО будет автоматически установлено в систему».

По словам исследователей, в основе кампании лежали ссылки на электронную почту, по которым в конечном итоге загружалось вредоносное ПО, размещенное на GitHub. Вредоносное ПО представляло собой имплант на основе Python, использующий Dropbox для управления и контроля (C2), который после загрузки позволял злоумышленнику загружать и скачивать файлы и выполнять произвольные команды.

Исследователи отметили, что каждая вредоносная часть этой атаки была размещена на законных сервисах, поэтому защитникам было сложнее полагаться на сетевые сигналы для обнаружения.

Google приписал нападение на сотрудников кампании Байдена APT 31 (также известному как Zirconium). По имеющимся данным, этот злоумышленник связан с правительством Китая.

Согласно предыдущему исследованию Microsoft, помимо сотрудников кампании «Джо Байден на пост президента» APT 31 также нацелена на «видных

деятелей международного сообщества, ученых-международников из более чем 15 университетов».

ДТС группы угроз включают использование веб-маяков, которые привязаны к домену, контролируемому злоумышленником. Затем группа отправляет URL-адрес домена адресатам с помощью текста электронной почты (или вложения) и убеждает их щелкнуть ссылку с помощью социальной инженерии.

«Хотя сам домен может не содержать вредоносного контента, [это] позволяет Zirconium [APT 31] проверять, пытался ли пользователь получить доступ к сайту», - заявили в Microsoft. «Для субъектов национального государства это простой способ провести разведку целевых учетных записей, чтобы определить, действительна ли учетная запись или активен пользователь».

С другой стороны медали, личные учетные записи электронной почты сотрудников, связанных с кампанией «Дональд Дж. Трамп на пост президента», также стали мишенью для другой группы угроз под названием APT 35 (также известной как Phosphorus и Charming Kitten), о которой говорят исследователи. работает из Ирана. Связанная с Ираном хакерская группа, как известно, использует фишинг в качестве вектора атаки, и в феврале было обнаружено, что целью фишинговых атак с целью похищения информации об учетных записях электронной почты жертв был публичный деятель.

Однако исследователи отметили, что хорошей новостью является то, что повышенное внимание к угрозам, исходящим от APT, в контексте выборов в США. Со своей стороны Google заявила, что удалила 14 аккаунтов Google, связанных с депутатом украинского парламента Андреем Деркачем, вскоре после того, как Минфин США наложил санкции на Деркача за попытку повлиять на выборы в США.

«Правительственные агентства США предупреждали о различных субъектах угроз, и мы тесно сотрудничали с этими агентствами и другими участниками технологической индустрии, чтобы делиться информацией о потенциальных клиентах и информацией о том, что мы видим в экосистеме», - заявили исследователи Google…». ***(Lindsey O'Donnell. Biden Campaign Staffers Targeted in Cyberattack Leveraging Antivirus Lure, Dropbox Ploy // Threatpost (https://threatpost.com/biden-campaign-staffers-targeted-in-cyberattack-leveraging-anti-virus-lure-dropbox-ploy/160234/). 16.10.2020).***

***

«Вашингтон ввів санкції в п'ятницю щодо російського науково-дослідного інституту, пов'язаного з розробкою небезпечної комп'ютерної програми, здатної завдати катастрофічних збитків…

Міністерство фінансів США стверджує, що підтримуваний російським урядом Центральний науково-дослідний Інститут хімії та механіки відповідальний за "створення спеціалізованих інструментів, які дозволили атакувати" непізнаний нафтохімічний об'єкт на Близькому Сході в 2017 році.

Атака викликала стурбованість, тому що на відміну від типових цифрових вторгнень, спрямованих на крадіжку даних або утримання їх для викупу - вона була

спрямована на заподіяння фізичного збитку самому об'єкту шляхом відключення його системи безпеки.

Натан Брубейкер, аналітик компанії з кібербезпеки FireEye, яка виявила задіяне програмне забезпечення, сказав, що таке ПЗ є унікально небезпечним, тому що відключення систем безпеки на такому заводі може призвести до серйозних наслідків, таких як пожежа або вибух.

Мінфін також повідомив, що в минулому році зловмисники, що стоять за шкідливим ПЗ, як повідомлялося, сканували і промацували щонайменше 20 електричних мереж в Сполучених Штатах на предмет вразливостей.

"Ми ще раз підкреслюємо незаконність будь-яких односторонніх обмежень. Росія, на відміну від США, не проводить наступальних операцій в кіберпросторі", - заявив в соціальних мережах посол Росії в США Анатолій Антонов.

"Ми закликаємо Сполучені Штати відмовитися від порочної практики необґрунтованих звинувачень" – додав він». ***(США запровадили санкції проти російського інституту за розробку небезпечного ПЗ // Європейська правда (https://www.eurointegration.com.ua/news/2020/10/24/7115686/). 24.10.2020).***

***

«Міністерство внутрішньої безпеки й Агентство з кібербезпеки і безпеки інфраструктури попередили про виявлення за останні тижні десятків хакерських атак на системи органів влади США, а також на сервери, пов'язані з авіаційною промисловістю, йдеться в спільній заяві цих відомств.

Федеральні агентства США повідомили, що доказів того, що російські хакери безпосередньо вплинули на будь-які підрахунки голосів або інформацію про зареєстрованих виборців, немає. Хакери проникли в комп'ютерні мережі, «не роблячи подальших дій».

Однак вони могли «шукати доступу для отримання майбутніх варіантів зривів, впливу на політику та дії США або делегітимізації» державних чи місцевих органів влади, зазначають агентства.

У заяві не згадувалось, на кого або на що були націлені кібератаки, вказано лише, що кампанія проводилась проти «широкого кола цілей».

Як йдеться в повідомленні, хакери, які називають себе Berserk Bear, Energetic Bear, Dragonfly та іншими іменами, викрали дані щонайменше зі двох серверів.

Попередження надійшло менш ніж за два тижні до виборів президента США, запланованих на 3 листопада, і в той час, як влада США перебуває в стані підвищеної готовності через спроби інших країн поширити неправдиву інформацію або іншим чином втрутитися у вибори.

США заявили, що Росія, яка втручалася у вибори 2016 року через злам електронної пошти демократів і через кампанію в соціальних мережах, намагається знову вплинути на вибори цього року.

21 жовтня директор національної розвідки США Джон Ретклiф заявив, що Іран і Росія отримали інформацію про американських виборців та намагаються вплинути на громадську думку напередодні президентських виборів 3 листопада.

Влади Ірану й Росії відкинули звинувачення». ***(США заявили про атаки пов'язаних із Росією хакерів на системи органів влади // Радіо Свобода (https://www.radiosvoboda.org/a/news-rosia-hakery-ssha/30908681.html). 23.10.2020).***

***

«Міністерство внутрішньої безпеки й Агентство з кібербезпеки і безпеки інфраструктури попередили про виявлення за останні тижні десятків хакерських атак на системи органів влади США, а також на сервери, пов'язані з авіаційною промисловістю, йдеться в спільній заяві цих відомств.

Федеральні агентства США повідомили, що доказів того, що російські хакери безпосередньо вплинули на будь-які підрахунки голосів або інформацію про зареєстрованих виборців, немає. Хакери проникли в комп'ютерні мережі, «не роблячи подальших дій».

Однак вони могли «шукати доступу для отримання майбутніх варіантів зривів, впливу на політику та дії США або делегітимізації» державних чи місцевих органів влади, зазначають агентства.

У заяві не згадувалось, на кого або на що були націлені кібератаки, вказано лише, що кампанія проводилась проти «широкого кола цілей».

Як йдеться в повідомленні, хакери, які називають себе Berserk Bear, Energetic Bear, Dragonfly та іншими іменами, викрали дані щонайменше зі двох серверів.

Попередження надійшло менш ніж за два тижні до виборів президента США, запланованих на 3 листопада, і в той час, як влада США перебуває в стані підвищеної готовності через спроби інших країн поширити неправдиву інформацію або іншим чином втрутитися у вибори.

США заявили, що Росія, яка втручалася у вибори 2016 року через злам електронної пошти демократів і через кампанію в соціальних мережах, намагається знову вплинути на вибори цього року.

21 жовтня директор національної розвідки США Джон Реткліф заявив, що Іран і Росія отримали інформацію про американських виборців та намагаються вплинути на громадську думку напередодні президентських виборів 3 листопада.

Влади Ірану й Росії відкинули звинувачення». ***(США заявили про атаки пов'язаних із Росією хакерів на системи органів влади // Радіо Свобода (https://www.radiosvoboda.org/a/news-rosia-hakery-ssha/30908681.html). 23.10.2020).***

***

«Європейський Союз запроваджує санкції проти двох фізичних осіб та однієї організації, які відповідальні за кібератаки на німецький парламент і Організацію із заборони хімічної зброї.

Відповідне рішення оприлюднено на сайті ЄС…

Як зазначається, кібератаки на інформаційну систему парламенту Німеччини сталися у квітні та травні 2015 року.

Росіянами, проти яких вводяться санкції, є офіцери військової розвідки ГРУ РФ Ігор Костюков і Дмитро Бадін.

Невдовзі повідомлення про запровадження відповідних санкцій оприлюднило МЗС Великої Британії.

“Велика Британія заморозить рахунки і заборонить в’їзд на свою територію двом російським офіцерам ГРУ і введе санкції проти підрозділу ГРУ 26165 під кодовою назвою APT28 і Fancy Bear, які відповідальні за кібератаки на парламент Німеччини у 2015 році”, – заявили у відомстві…». ***(ЄС і Велика Британія вводять санкції проти РФ за кібератаки на Бундестаг // UATV (https://uatv.ua/yes-i-velyka-brytaniya-vvodyat-sanktsiyi-proty-rf-za-kiberataky-na-bundestag/). 22.10.2020)***

***

«Microsoft предупреждает, что APT Phosphorous начал успешные атаки на мировых лидеров, участвующих в Мюнхенской конференции по безопасности и саммите Think 20 (T20) в Саудовской Аравии.

Microsoft заявила, что иранский злоумышленник успешно скомпрометировал участников двух глобальных конференций, в том числе послов и старших экспертов по политике, в попытке украсть их учетные данные электронной почты.

К двум запланированным конференциям относятся Мюнхенская конференция по безопасности, намеченная на 19–21 февраля 2021 года, и саммит Think 20 (T20) в Саудовской Аравии, который состоится 31 октября - 1 ноября 2020 года. Обе конференции в этом году в большинстве своем являются виртуальными. являются давними и уважаемыми площадками для обсуждения, в частности, глобальной и региональной политики безопасности.

Microsoft связала атаку, нацеленную на более чем 100 участников конференции, с Phosphorus, который, по ее словам, действует из Ирана. Группа, также известная как APT 35, Charming Kitten и Ajax Security Team, как известно, использует фишинг в качестве вектора атаки.

«Мы полагаем, что Phosphorus участвует в этих атаках в целях сбора разведывательной информации», - написал Том Берт, корпоративный вице-президент по безопасности и доверию клиентов Microsoft, в своем сообщении, в котором излагаются сюжеты в среду. «В результате атак были скомпрометированы несколько жертв, в том числе бывшие послы и другие высокопоставленные эксперты по политике, которые помогают формировать глобальные программы и внешнюю политику в своих странах».

Берт сказал, что злоумышленники рассылали возможным участникам поддельные приглашения по электронной почте. По его словам, в этих электронных письмах используется почти идеальный английский, и они были отправлены бывшим правительственным чиновникам, экспертам по политике, ученым и лидерам неправительственных организаций. Они призваны помочь развеять страхи перед путешествиями во время пандемии Covid-19, предлагая удаленные сеансы.

Электронные письма приходят от поддельных организаторов конференций, использующих адреса электронной почты t20saudiarabia [@] outlook.sa, t20saudiarabia [@] gmail.com и munichconference [@] outlook.com

Если цель принимает приглашение, атакующему предлагается отправить свое изображение и биографию. Запрос злоумышленника вложен во вложенный защищенный паролем PDF-файл и представлен в виде короткой ссылки (внутри PDF-файла). Естественно, ссылка ведет на одну из нескольких известных страниц

сбора учетных данных, предназначенных для того, чтобы обманом заставить цели передать свои учетные данные электронной почты через поддельную страницу входа в учетную запись. Вредоносные домены включают de-ma [.] Online, g20saudi.000webhostapp [.] Com и ksat20.000webhostapp [.] Com.

Злоумышленники используют эти учетные данные для входа в почтовый ящик жертв, где они затем могут собирать дополнительную конфиденциальную информацию и запускать другие вредоносные атаки.

«В результате атак были скомпрометированы несколько жертв, в том числе бывшие послы и другие высокопоставленные эксперты по политике, которые помогают формировать глобальные программы и внешнюю политику в своих странах», - написал Берт.

Microsoft заявила, что работает с организаторами конференций, которые предупредили своих участников.

Threatpost обратился к обоим организаторам конференции за дополнительной информацией.

Между тем, Microsoft рекомендует участникам конференции оценивать подлинность получаемых ими электронных писем о крупных конференциях, убедившись, что адрес отправителя выглядит законным и что любые встроенные ссылки перенаправляют на официальный домен конференции.

«Как всегда, включение многофакторной аутентификации в корпоративных и личных учетных записях электронной почты успешно предотвратит большинство подобных атак по сбору учетных данных», - сказал Берт. «Всем, кто подозревает, что они могли быть жертвой этой кампании, мы также рекомендуем внимательно изучить правила пересылки электронной почты в учетных записях, чтобы выявить и удалить любые подозрительные правила, которые могли быть установлены во время успешного взлома».

Связанная с Ираном хакерская группа Phosphorus в этом году произвела фурор, нацеливая фишинговые атаки на сотрудников кампании Трампа и Байдена. В феврале группа обнаружила, что целью фишинговых атак являлось нападение на общественных деятелей, в ходе которых была украдена информация электронной почты жертв. Ранее в этом году Microsoft также взяла под свой контроль 99 веб-сайтов, используемых группой угроз для атак. В прошлом году Phosphorus также был обнаружен при попытке взлома аккаунтов, связанных с переизбранием президента Трампа в 2020 году. И совсем недавно было замечено, что сообщения WhatsApp и LinkedIn использовались для выдачи себя за журналистов». ***(Lindsey O'Donnell. Iran-linked APT Targets T20 Summit, Munich Security Conference Attendees // Threatpost (https://threatpost.com/microsoft-iranian-apt-t20-summit-munich-security-conference/160654/). 28.10.2020).***

***

«С приближением дня выборов местные органы власти должны быть готовы к атакам вредоносного ПО на избирательную инфраструктуру.

Банды программ-вымогателей официально вступили в борьбу на выборах 2020 года, сообщив об одном из первых нарушений сезона голосования в округе

Холл, штат Джорджия. Атака затронула базу данных округов с подписями избирателей, а также другие правительственные системы.

Хотя в округе заявили, что на процесс голосования не повлияла атака программы-вымогателя, этот инцидент является предупреждением другим муниципалитетам о блокировке своих систем, особенно в последние дни, предшествующие выборам.

Округ Холл находится примерно в часе езды к северу от Атланты и впервые сообщил о нападении 7 октября.

Атаки программ-вымогателей заключаются в том, что преступник внедряет вредоносное ПО в системы цели, которая затем захватывает данные организации и шифрует их до тех пор, пока не будет выплачен выкуп.

Атака программ-вымогателей округа Холл

21 октября газета Gainesville Times сообщила, что карта участков округа была отключена в результате атаки программы-вымогателя, в дополнение к базе данных подписей избирателей.

Только 22 октября округ объявил: «Атака не повлияла на процесс голосования граждан».

«Произошла атака программы-вымогателя с участием критически важных систем в правительственных сетях округа Холл, включая прерывание телефонных услуг», - говорится в пресс-релизе. «Как только это произошло, округ начал работу по расследованию причины, восстановлению работы и определению последствий инцидента».

Координатор регистрации округа Холл Кей Вимпье (Kay Wimpye) опубликовала документ о том, что некоторые системы уже работают, и если есть вопрос о подписи для голосования, сотрудники округа все еще могут вытащить карточки регистрации избирателей вручную. Но учитывая рекордное количество отправленных по почте бюллетеней, это может оказаться трудоемким процессом.

Вимпи сообщила Times, что ее офис разослал 27 573 открепительных удостоверения по состоянию на 21 октября, и 11 351 были отправлены обратно. Госсекретарь Джорджии сообщил, что к 21 октября 2016 года было возвращено 103 239 бюллетеней, отправленных по почте, по сравнению с 805 442 бюллетенями в тот же день в 2020 году, что свидетельствует о резком росте числа избирателей, выбравших голосование по почте в этом избирательном цикле.. Хотя подписи сейчас проверяются, по данным Times, подсчет бюллетеней не будет проведен до дня выборов.

Программы-вымогатели и государственный сектор

Атаки программ-вымогателей, приуроченные так близко к дню выборов, угрожают полностью разрушить и без того спорную конкуренцию.

Брэндон Хоффман, ИТ-директор компании Netenrich, назвал атаку на инфраструктуру голосования «неизбежной».

«Распространение программ-вымогателей практически не контролировалось, и очевидно, что именно этот тип вредоносного ПО будет поражать», - добавил он. «С другой стороны, с программами-вымогателями избирательная инфраструктура, вероятно, не была главной целью».

Но, предупреждает Хоффман, это может измениться.

«Тот факт, что это было успешным, подтверждает путь атаки», - сказал он. «Проверка пути атаки - ключевой шаг в любой последовательности атаки, и ее тестирование на небольших сценариях всегда имеет смысл. Если бы профессионалы в области безопасности, работающие с технологией голосования, еще не проявили особой бдительности, нельзя терять время на чрезмерную подготовку ».

Организации государственного сектора уже являются привлекательной мишенью для атак вредоносного ПО. Согласно недавнему отчету Mimecast о безопасности электронной почты в государственном секторе, более половины (52 процента) организаций государственного сектора подверглись атакам, и вредоносное ПО распространялось от скомпрометированного пользователя к коллегам.

В отчете добавлено, что 9% атакованных в результате простаивали более недели, больше всего в любой другой отрасли. А поскольку до выборов осталось чуть больше недели, это может означать катастрофу для своевременного подсчета голосов.

Мэтью Гардинер, стратег по кибербезопасности в Mimecast, сообщил Threatpost по электронной почте, что злоумышленники видят легкую зарплату в местных органах власти.

«Киберпреступники, ориентированные на программы-вымогатели, сосредоточены на деньгах, - сказал он. «Таким образом, они сосредотачиваются на поражении организаций, в которые относительно легко попасть и которые имеют возможность / готовность платить выкуп. В целом здесь высокие баллы получают города, муниципалитеты, поселки и школьные округа ».

После того, как выкуп уплачен, Гардинер сравнил его с «кровью в воде для акул», привлекающей больше хищников. Крайний срок выборов может привести к увеличению цены на данные или побудить цели платить быстрее, но, кроме того, Гардинер не рассматривает результаты выборов как особый мотиватор для киберпреступников.

Патчинг и обучение

По словам Дэниела Нормана, старшего аналитика по решениям в Information Security Forum, для обеспечения защиты систем в такое сложное время большое значение могут иметь две простые вещи: установка исправлений и обучение сотрудников.

«В дальнейшем конечные пользователи должны получить достаточную информацию о безопасности, просвещение и обучение по вопросам угроз, связанных с программами-вымогателями, особенно с механизмом их доставки», - сказал Норман в заявлении по электронной почте. «Как правило, успех программ-вымогателей зависит от того, исправила ли целевая организация свои устройства должным образом. Таким образом, установка обновлений и исправлений для всех систем является минимальным условием безопасности ».

Согласно отчету SonicWall о киберугрозах 2020 года, количество программ-вымогателей растет во всем мире благодаря пандемии, что на 109 процентов больше, чем в прошлом году.

Хэнк Шлесс, старший менеджер по решениям безопасности в Lookout, отметил, что работники, разбросанные по всему миру, использующие мобильные устройства, более уязвимы, чем когда-либо, перед уловками социальной инженерии при переключении между личными и профессиональными приложениями.

«Когда сотрудники по всему миру начали работать из дома, организации позволили своим сотрудникам оставаться продуктивными, используя мобильные устройства, и злоумышленники это знают», - сказал Шлесс.

«Организации, которые активно занимаются защитой мобильных устройств с помощью мобильной безопасности, находятся в авангарде инноваций и демонстрируют, что они адаптируются к сегодняшнему быстро меняющемуся ландшафту угроз», - добавил он.

Что касается округа Холл, то их пресс-секретарь Кэти Крамли отказалась предоставить Threatpost комментарий, помимо пресс-релиза, «в целях безопасности». В заявлении говорится, что округ «привлек сторонних специалистов по кибербезопасности для ускорения восстановления». ***(Becky Bracken. Georgia Election Data Hit in Ransomware Attack // Threatpost (https://threatpost.com/georgia-election-data-ransomware/160499/). 23.10.2020).***

***

«Агентство национальной безопасности США написало отчет об уроке, извлеченном из ситуации, когда иностранное государство воспользовалось его же бэкдором в межсетевых экранах Juniper. Однако, по иронии судьбы, АНБ так и не смогло найти этот отчет.

В среду, 28 октября, информагентство Reuters опубликовало статью о попытках сенатора США от штата Орегон Рона Уайдена выяснить, помещает ли АНБ до сих пор бэкдоры в технологические продукты американского производства. Сам Уайден является противником подобной практики, в особенности после случая с бэкдором в межсетевых экранах Juniper. По его мнению, использование бэкдоров в американских технологиях может иметь обратный эффект и подорвать национальную безопасность. Кроме того, такой подход делает продукты производства США менее привлекательными для покупателей. Тем не менее, расследование Уайдена, как члена сенатского комитета по разведке, было заблокировано ввиду отсутствия сотрудничества со стороны АНБ и представителей частного сектора.

В 2015 году компания Juniper обнаружила в операционной системе ScreenOS, на базе которой работают межсетевые экраны NetScreen, «неавторизованный код», присутствующий в ОС еще с 2008 года. Согласно ранее не публиковавшемуся отчету Juniper, направленному в Конгресс, «правительство неустановленного государства переделало механизм, изначально созданный АНБ».

Причина, по которой вредоносному коду удалось расшифровать VPN-соединение ScreenOS, - решение Juniper использовать в своих продуктах разработанный АНБ генератор псевдослучайных чисел Dual EC. Зачем ей это понадобилось, до сих пор неизвестно.

В 2018 году АНБ сообщило сотрудникам Уайдена о подготовке отчета об «извлеченном уроке» из сложившейся ситуации. Однако, по словам пресс-секретаря Уайдена Кита Чу (Keith Chu), в итоге агентство так и не смогло найти этот файл». ***(Американские шпионы увиливают от ответа на вопрос о бэкдорах // SecurityLab.ru (https://www.securitylab.ru/news/513514.php). 29.10.2020).***

***

«DHS CISA и ФБР сегодня поделились дополнительной информацией о том, как иранская хакерская группа, спонсируемая государством, смогла собрать информацию о регистрации избирателей с государственных веб-сайтов США, включая избирательные сайты.

Собранные данные позже были использованы поддельные электронные письма Proud Boys с запугиванием избирателей, нацеленные на избирателей-демократов, пытающихся убедить их проголосовать за президента Трампа.

«Дальнейшая оценка, проведенная CISA и ФБР, выявила, что нападения на сайты государственных выборов в США были преднамеренными попытками повлиять на президентские выборы в США 2020 года и вмешаться в них», - говорится в опубликованном сегодня совместном сообщении.

Согласно сообщению, попытки загрузить информацию о избирателях с избирательных сайтов имели место с 29 сентября по 17 октября 2020 года.

«Это включает попытки использования известных уязвимостей, обход каталога, внедрение языка структурированных запросов (SQL), загрузку веб-оболочки и использование уникальных недостатков на веб-сайтах», - поясняют ФБР и CISA.

В сообщении представлены технические подробности относительно подтверждения DNI Джона Рэтклиффа во время пресс-конференции о том, что поддерживаемые государством иранские хакеры собрали информацию о регистрации избирателей, которая использовалась в поддельных письмах с угрозами Proud Boys.

Избирательные участки проверены на уязвимости

Иранские акторы APT сначала использовали сканер уязвимостей Acunetix для обнаружения недостатков безопасности, затрагивающих целевые сайты, что позже позволило им использовать небезопасные серверы.

Их атаки позволили им успешно загрузить данные о регистрации избирателей по крайней мере для одного штата США, воспользовавшись неверной конфигурацией и уязвимостями избирательных участков.

Для этого они использовали скрипты, предназначенные для использования «инструмента cURL для итерации по записям избирателей», чтобы автоматически просматривать базы данных и загружать их с помощью

«После анализа журналов доступа к веб-серверу аналитики CISA в сотрудничестве с ФБР обнаружили экземпляры пользовательских агентов cURL и FDM, отправляющих запросы GET на веб-ресурс, связанный с данными регистрации избирателей», - говорится в сообщении.

«Подозреваемая активность по сценарию отправила несколько сотен тысяч запросов, повторяющих значения идентификации избирателя и получающих результаты с различным уровнем успеха».

Иранские хакеры использовали NordVPN

Как сообщило ФБР во вчерашнем экстренном предупреждении, многие из IP-адресов, используемых иранскими хакерами в поддельной почтовой кампании Proud Boys, принадлежат службе NordVPN и могут также соответствовать другим поставщикам VPN, включая CDN77, HQSERV и M247.

«Хотя это создает возможность для ложных срабатываний, любая деятельность, указанная ниже, вероятно, потребует дальнейшего расследования», - заявили в ФБР.

В ходе расследования ФБР также обнаружило доказательства, указывающие на то, что субъект APT исследовал следующую информацию во время своих попыток сканировать и использовать сайты государственных выборов:

YOURLS эксплойт

Обход брандмауэра веб-приложений ModSecurity

Обнаружение брандмауэров веб-приложений

Инструмент SQLmap

ФБР и CISA также предоставляют следующие общие меры по предотвращению атак в будущем:

Обновляйте приложения и системы и исправляйте их

Сканирование веб-приложений на предмет SQL-инъекций и других распространенных веб-уязвимостей

Развернуть брандмауэр веб-приложения

Разверните методы защиты от веб-оболочек

Используйте многофакторную аутентификацию для учетных записей администратора

Устранение критических рисков безопасности веб-приложений». ***(Sergiu Gatlan. FBI: How Iranian hackers stole voter info from state election sites // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-how-iranian-hackers-stole-voter-info-from-state-election-sites/). 30.10.2020).***

***

Створення та функціонування кібервійськ

«Операция проведена в рамках усилий по защите выборов президента США от внешнего вмешательства, сообщает газета Washington Post со ссылкой на источники.

По данным газеты, военные США запустили операцию по временному нарушению работы Trickbot, состоящего из "не менее 1 миллиона захваченных компьютеров", которыми управляют "русскоязычные преступники".

Четыре должностных лица сообщили изданию, что уже несколько недель назад в киберпространстве началась кампания по выведению из строя бот-сети

Trickbot. По данным военных, эта сеть состоит из миллиона зараженных компьютеров и контролируется русскоязычными злоумышленниками.

Кампания, которая разворачивается против сети Trickbot, не ставит цели ее полного отключения. По словам главы киберкомандования, такая тактика позволяет совершать "постоянное воздействие" на противника.

Операция проводится в рамках стратегии «постоянного конфликта» — попыток регулярно срывать действия иностранных кибер-противников для отвлечения их усилий.

По оценкам военных США Trickbot является одной из крупнейших бот-сетей в мире. Она используется для кражи финансовых данных и распространения вредоносного программного обеспечения…». ***(Киберкомандование США провело операцию против одного из крупнейших ботнетов Trickbot // SecurityLab.ru (https://www.securitylab.ru/news/512912.php). 11.10.2020).***

***

«Операция вредоносного ПО Trickbot находится на грани полного прекращения после усилий альянса кибербезопасности и хостинг-провайдеров, нацеленных на серверы управления и контроля ботнета.

Первоначальные действия по сбоям в работе, казалось, оставили ботнет без фазы, так как его операторы смогли восстановить инфраструктуру и сеть зараженных компьютеров.

Хотя битва еще не закончена, последний счет в борьбе с Trickbot ясно показывает, что работа коалиции, возглавляемой Microsoft Digital Crimes Unit (DCU), оказала серьезное влияние.

TrickBot ждет скоординированная операция по удалению

12 октября Microsoft и ее партнеры объявили, что сняли несколько Trickbot C2.

Это стало возможным после того, как Окружной суд Восточного округа штата Вирджиния удовлетворил запрос на удаление 19 IP-адресов в США, которые Trickbot использовал для управления зараженными компьютерами.

В партнерство входят ESET, Black Lotus Labs Lumen, NTT Ltd, корпоративный бизнес Broadcom Symantec, Центр обмена информацией и анализа финансовых услуг (FS-ISAC) и команда Microsoft Defender.

Сообщается, что до этого киберкомандование США пыталось вывести из строя ботнет в преддверии президентских выборов, отправив файл конфигурации на зараженные компьютеры, отключив их от управляющих серверов.

Партнеры с самого начала знали, что этот первый залп не приведет к остановке Trickbot, и описали это как продолжающееся вмешательство без гарантии полного уничтожения ботнета.

На прошлой неделе компания Intel 471, занимающаяся кибербезопасностью, увидела, что Trickbot продолжает заражать новые компьютеры, чему помогает его давний партнер Emotet, который также распространяет QBot…

Ожидался возврат

Исследователи из Lumen's Black Lotus Labs рассказали BleepingComputer, что администраторы Trickbot постоянно меняют IP-адреса C2 и зараженные хосты, что серьезно затрудняет попытки сбоя.

Они также используют разные серверы для связи с ботами и доставки плагинов, предназначенных для конкретных задач (кража паролей, кража трафика, распространение вредоносного ПО).

Intel 471 отмечает, что администраторы Trickbot на прошлой неделе обновили файл конфигурации сервера подключаемых модулей с 15 новыми IP-адресами. Они сохранили два старых адреса вместе с доменом сервера.onion, доступным через анонимную сеть Tor.

Шеррод ДеГриппо, старший директор по исследованию угроз в Proofpoint, сообщил BleepingComputer, что кампании Trickbot перешли на новые каналы C2. Она добавила, что первоначальные действия против ботнета не вызвали «прямого заметного изменения в нарушении вредоносной электронной почты с использованием Trickbot».

Столы превращаются

В сегодняшнем сообщении в блоге Microsoft предоставляет обновленную информацию о нарушении работы Trickbot, в которой говорится, что вместе со своими партнерами по всему миру они работали над отключением 94% критической инфраструктуры Trickbot…

Microsoft сообщает, что 18 октября 120 из 128 серверов Trickbot отключились по всему миру с момента начала операции.

Основная инфраструктура Trickbot включает устройства Интернета вещей (IoT) для управления ботнетом. Microsoft и ее партнеры определили семь из них, все в процессе вывода из строя.

Этот успех не означает, что борьба подходит к концу. Уникальная архитектура Trickbot требует постоянных действий против него, чтобы минимизировать шансы на воскрешение.

Эти усилия будут продолжаться как минимум до 3 ноября, дня президентских выборов в США, чему будут способствовать новые судебные постановления об отключении только что активированных серверов в стране…

Поскольку TrickBot размещает серверы управления и контроля на клиентских и бизнес-маршрутизаторах, Microsoft работает с поставщиками интернет-услуг (ISP), чтобы помочь исправить устройства, не прерывая законный трафик.

В настоящее время администраторы Trickbot заняты настройкой новой инфраструктуры, что требует времени и снижает частоту новых атак.

Microsoft заявляет, что им удалось идентифицировать новые серверы и использовать законные каналы, чтобы отключить их менее чем за три часа. В одном случае хостинг-провайдер отключил сервер Trickbot менее чем за шесть минут с момента получения уведомления о незаконной деятельности.

В образце вредоносного ПО Trickbot, распространенном 19 октября, Intel 471 выявила 16 новых серверов ботнета C2, разбросанных по всему миру, ни один из которых в настоящее время не отвечает на запросы от зараженных систем…

Intel 471 сообщает, что некоторые серверы Trickbot все еще активны в Бразилии, Колумбии, Индонезии и Кыргызстане. Более того, у администраторов

ботнета по-прежнему есть партнеры, желающие распространять их вредоносное ПО.

Даже если эти усилия не приведут к исчезновению Trickbot, ботнет может умереть сам по себе; но только потому, что злоумышленники переходят на BazarLoader, троян, который все чаще используется операторами Trickbot для нацеливания на крупные предприятия и развертывания вымогателя Ryuk в своих сетях…» ***(Ionut Ilascu. TrickBot malware under siege from all sides, and it's working // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/trickbot-malware-under-siege-from-all-sides-and-its-working/). 20.10.2020).***

***

«По словам исследователей кибербезопасности, хотя Microsoft успешно отключила серверы ботнета Trickbot в США, почти два десятка других работают на международном уровне, что может стать причиной хаоса на выборах.

Исследователи кибербезопасности поставили под сомнение эффективность мер, предпринятых Microsoft по разрушению ботнета, который, как они опасались, мог бы обрушиться на государственные и местные компьютерные системы, чтобы посеять недоверие к предстоящим президентским выборам.

Софтверный гигант заявил в понедельник, что компания выиграла суд в Вирджинии, получив контроль над серверами в США, контролирующими ботнет Trickbot, сеть компьютеров, тайно зараженных вредоносным ПО, которым можно управлять удаленно. Это позволило Microsoft лишить хакеров возможности работать с выборами чуть более чем через две недели на фоне опасений, что они распространят программы-вымогатели для блокировки систем отчетности в день выборов, подорвав доверие избирателей.

Однако, американская компания Intel 471 по анализу угроз обнаружила, что Trickbot продолжает работать через четыре дня после того, как Microsoft захватила американские серверы ботнета. Швейцарский сайт безопасности Feodo Tracker обнаружил, что 18 таких серверов все еще активны и рассылают вредоносные программы через спам, несмотря на усилия Microsoft.

«Они определенно помешали им, но действия Microsoft не повлияли на способность Trickbot делать то, что они делали раньше», - сказал исполнительный директор Intel 471 Марк Арена.

Microsoft стремится разрушить российский криминальный ботнет, который, может стать причиной хаоса на президентских выборах.

Microsoft отключила все командно-управляющие серверы Trickbot в США. Однако по состоянию на полдень четверга 11 серверов за пределами страны, которые работали до действий Microsoft, все еще были в сети, от Джакарты, Индонезия, до голландской провинции Утрехт и Боготы, Колумбия, согласно данным Intel 471.

Более того, операторы Trickbot подключили еще десяток серверов за пределами США, в таких городах, как Амстердам, Берлин и Москва, как выяснила Intel 471.

Фирмы по кибербезопасности называют попытки Microsoft разрушить ботнет для защиты от вмешательства в выборы неэффективными

«Плохие парни узнали», - сказал Арена. «Они распространили их по всему миру. Они создали устойчивость и создали резервные копии».

Microsoft возражает и заявляет, что продолжает вести борьбу по разрушению Trickbot.

«Мы считаем, что нам удалось серьезно ограничить возможности Trickbot. Наша работа по устранению сбоев продолжается в США и во всем мире, и отчеты третьих сторон не отражают текущее состояние», - заявил в своем заявлении вице-президент Microsoft по безопасности и доверию клиентов Том Берт.

Киберкомандование стремилось нарушить работу крупнейшего в мире ботнета, надеясь уменьшить его потенциальное влияние на выборы.

Microsoft всегда ожидала, что хакеры, работающие с Trickbot, вернутся, чтобы восстановить его работу.

«Мы активно отслеживаем эти усилия и предпринимаем дополнительные и важные шаги в направлении прекращения работы ботнета», - сказал Берт. Компания отказалась раскрыть, что это за шаги.

По заявлению Microsoft, ботнет, управляемый операторами Trickbot, включает не менее 1 миллиона зараженных компьютеров, хотя другие аналитики считают, что это число составляет около 3 миллионов устройств. Эти зараженные компьютеры могут использоваться для распространения программ-вымогателей, а также для рассылки вредоносного спама ничего не подозревающим получателям.

Атака программ-вымогателей на выборы 2020 года может нарушить работу баз данных для голосования по всем штатам.

Фактически, даже после действий Microsoft, Trickbot использовался для рассылки спама вредоносных программ в США в пятницу, сказал Роман Хюсси, исследователь безопасности в abuse.ch, некоммерческой группе, которая управляет Feodo Tracker. По словам Хюсси, до сих пор тактика Microsoft в лучшем случае нарушила работу Trickbot на несколько дней, хотя он признал, что дальнейшие действия могут вызвать дополнительные проблемы для ботнета. Но с таким количеством работающих командно-управляющих серверов и продолжающейся рассылкой спама жертв кампания Microsoft по подрыву «не выглядит очень многообещающей», - сказал Хюсси.

Хотя некоторая инфраструктура ботнета была выведена из строя, киберпреступники перебрались на новые серверы и нашли способы привлечь новых жертв, сказал Алекс Холден, исполнительный директор Hold Security из Милуоки. По его словам, за последние несколько дней ботнет заразил более 1000 новых компьютеров в США и за их пределами.

«К сожалению, - сказал он, - ряд командно-управляющих серверов все еще активен».

Захватив в начале этой недели контроль над серверами в США, которые отправляют инструкции ботнету, Берт в интервью заявил, что Trickbot, управляемый русскоязычными преступниками, представляет собой «теоретическую, но реальную» угрозу честности выборов. Microsoft опасалась, что операторы Trickbot могут запустить атаки программ-вымогателей, которые не

повлияют на фактические результаты выборов, а скорее ограничат способность избирательного участка сообщать результаты, например, подорвав доверие избирателей.

Не только Microsoft пыталась нарушить работу Trickbot. В последние недели киберкомандование США также начало кампанию против ботнета. А в четверг европейское политическое агентство Европол арестовало 20 человек, предположительно принадлежащих к международной сети, которая отмывала миллионы евро, украденные киберпреступниками с помощью вредоносных схем, а также помогала операторам Trickbot.

Таким образом, хотя эффективность попыток Microsoft нарушить работу Trickbot ограничена, «тройной удар» действий компании вместе с Cyber Command и Европолом снизит вероятность того, что хакеры будут использовать Trickbot для уничтожения программ-вымогателей, - сказал Гэри Уорнер, директор по исследованиям. в области компьютерной криминалистики в Университете Алабамы в Бирмингеме». ***(Романов Роман. Исследователи кибербезопасности заявляют о неэффективности мер, предпринятых Microsoft по уничтожению ботнета // Internetua (https://internetua.com/issledovateli-kiberbezopasnosti-zayavlyauat-o-neeffektivnosti-mer-predprinyatyh-microsoft-po-unicstojeniua-botneta). 17.10.2020).***

***

«…функционал спецназа, скорее всего, расширят, оснастив его беспилотными аппаратами и хакерами. Специалист добавил, что подразделения следует обучать с учетом изменяющейся ситуации на планете, где ведутся кибервойны, а также информационные и экономические противостояния.

Командование специальных операций ВС США (SOCOM), пишет Питер Сучиу, должно продолжить внедрение новых технологий, чтобы в случае военного конфликта не пришлось использовать непроверенную тактику и методы. К таким технологиям он отнес машинное обучение и искусственный интеллект.

- В нынешнем виде спецназ не отражает потребности современного общества. Этот факт должен заставить нас всех задуматься. Есть барьеры, которые оставляют необходимые нам таланты за пределами формирований, - заявил исполняющий обязанности помощника министра обороны по по специальным операциям и конфликтам низкой интенсивности Эзра Коэн». ***(Американский спецназ готовят к кибервойне с Россией и Китаем // SecurityLab.ru (https://www.securitylab.ru/news/512900.php). 10.10.2020).***

***

«Великобритания осуществила серию тайных кибератак на российских лидеров и их союзников, сообщил бывший член британского Кабинета министров лорд Марк Седвилл (Mark Sedwill). По его словам, Великобритания проэксплуатировала «уязвимости» Москвы, в том числе используя свои недавно заявленные кибернаступательные возможности.

Как сообщил Седвилл, целью атак было «назначить цену выше ожидаемой» в ответ на агрессивные действия России.

«Россия проводит операции в так называемом сером пространстве – зазоре между нормальными отношениями между государствами и вооруженным конфликтом, с применением кибератак, средств информационной войны и подрывных кампаний. Для нас очень важно уметь маневрировать в сером пространстве и делать это максимально эффективно. Мы не можем позволить себе отдать инициативу нашим противникам. Есть уязвимости, которые мы тоже можем проэксплуатировать. Просто мы не всегда говорим об этом», – сообщил Седвилл в эфире Times Radio.

В частности, Великобритания эксплуатировала уязвимости после отравления бывшего сотрудника ГРУ Сергея Скрипаля и его дочери Юлии нервно-паралитическим веществом в британском городе Солсбери в марте 2018 года. О возможности принятия мер в отношении РФ, в том числе кибератак, через неделю после отравления предупредила тогдашний премьер-министр Великобритании Тереза Мэй. Годом позднее на возможный кибердар по России намекнул министр иностранных дел Великобритании Джереми Хант на конференции по кибербезопасности НАТО». ***(Великобритания тайно атаковала российских лидеров // SecurityLab.ru (https://www.securitylab.ru/news/513369.php). 26.10.2020).***

***

Кіберзахист критичної інфраструктури

«Группа специалистов Оксфордского университета и Федерального управления по оборонным закупкам Швейцарии обнаружили, что системы предупреждения столкновения самолетов нового поколения так же уязвимы к спуфингу сигнала, как и их предшественники.

Специалисты провели экспертизу новых систем предупреждения столкновения самолетов Airborne Collision Avoidance System X (ACAS X), которая в ближайшие несколько лет будет реализована в коммерческих самолетах, и выявили, что злоумышленники могут заставить ее выдавать поддельные уведомления о столкновениях, вынуждающие пилотов увертываться от несуществующих препятствий.

По словам специалистов, в 44% случаев злоумышленник может успешно вызвать уведомление о столкновении, чреватое изменением высоты полета в среднем на 180 метров. Когда самолет находится на небольшой высоте, вероятность успеха кибератаки повышается до 79%.

Современные системы предупреждения столкновения самолетов представляют собой автоматизированные транспондерные системы, предназначенные для предотвращения столкновений в воздухе. Передатчики в самолетах посылают друг другу сигналы для определения местоположения и идентификационных данных во избежание чрезмерного сближения самолетов и возможного столкновения.

Система может выдавать информационные сообщения о движении, звуковые предупреждения, предписывающие пилотам проверять наличие ближайших

самолетов, а также приказы предпринимать определенные действия, такие как подъем или спуск, которым пилоты должны следовать.

Ранее в нынешнем году специалисты Политехнического университета Виргинии и Университета Пердью представили теоретическую атаку, позволяющую заставить систему предупреждения столкновения «увидеть» несуществующий самолет и выдать предупреждение. Как оказалось, системы нового поколения также уязвимы к этой атаке.

По словам специалистов, с помощью стандартного программно-определяемого радио, например, Hack RF, усилителя и антенны, способной передавать сигнал с мощностью 500 Вт в диапазоне 1030/1090 МГц, можно создать пользовательское устройство, отслеживающее самолеты путем перемещения антенны и передающее на их передатчики ложные данные о нахождении поблизости других самолетов.

«Последствия такой атаки могут быть очень серьезными. Хотя столкновение в воздухе маловероятно, эта атака вызывает сбой, который может повлиять на многие находящиеся поблизости самолеты», - заключили исследователи». ***(Эксперты научились обманывать новые системы предупреждения столкновения самолетов // SecurityLab.ru (https://www.securitylab.ru/news/512803.php). 07.10.2020).***

***

Захист персональних даних

«Европейский суд юстиции в Люксембурге постановил, что государства-члены Евросоюза не могут массово собирать мобильные и интернет-данные граждан… В решении говорится, что принуждение операторов широко и беспорядочно передавать или хранить данные о трафике или геолокации противоречит законодательству ЕС.

Однако Суд сделал оговорку: сбор возможен, если страна-член Евросоюза столкнулась «с серьёзной угрозой национальной безопасности». Впрочем, даже в таких ситуациях остаются правила, которые необходимо соблюдать. В подобных случаях хранение и передача данных должны быть ограничены во времени и проходить под надзором суда или независимой профильной структуры.

Решение является ответом на несколько дел, возбужденных по искам правозащитных организаций Privacy International и La Quadrature du Net. Суд ЕС в Люксембурге рассмотрел этот вопрос и принял соответствующее решение по запросу судов Франции, Бельгии и Великобритании.

La Quadrature du Net назвала это решение «долгожданным», хотя и не полностью удовлетворена им, поскольку право на неприкосновенность частной жизни, по её мнению, всё ещё остаётся в опасности, а существующие правовые нормы обязательно приведут к злоупотреблениям.

Privacy International же считает, что это судебное решение укрепляет верховенство права в ЕС, являясь напоминанием о том, что ни одно правительство

не должно быть выше Закона…». ***(Суд ЕС: правительства не могут массово собирать мобильные и интернет-данные граждан // РосКомСвобода (https://roskomsvoboda.org/64841/). 06.10.2020).***

***

«Частота, масштаб утечек данных и наносимый ими ущерб резко возросли в последние годы, причем большинство таких инцидентов происходит потому, что люди являются самым слабым звеном в цепи безопасности. Несоблюдение политики информационной безопасности (ISP) со стороны сотрудников — один из важных факторов риска.

Почему одни сотрудники организации с большей вероятностью соблюдают требования ISP, чем другие? Такими вопросом задались исследователи из Бингемптонского университета (штат Нью-Йорк). Результаты их анализа, опубликованные журналом Information Systems Research, указывают на существование субкультур внутри организации, которые влияют на степень ответственности служащих при соблюдении предписаний безопасности.

«В каждой организации есть культура, которая обычно устанавливается высшим руководством. Но внутри неё существуют субкультуры среди различных профессиональных групп, которые проходят разное обучение и отвечают за разные задачи», — рассказывает Сумантра Саркар (Sumantra Sarkar), доцент кафедры информационных систем управления в Школе менеджмента Бингемтонского университета.

Политики информационной безопасности, при выработке которых не учитывается специфика субкультур, подвергают организации повышенному риску утечки данных. Рекомендации по пересмотру подходов к формулированию и применению ISP авторы основывают на многолетних наблюдениях за тремя субкультурами, выявленными в больницах: за врачами, медсёстрами и персоналом поддержки.

«Врачи, которые постоянно имеют дело с неотложными ситуациями, чаще оставляли рабочую станцию разблокированной. Их больше беспокоила немедленная помощь пациенту, чем возможный риск утечки данных, — отмечает Саркар. — С другой стороны, сотрудники службы поддержки уходя, редко оставляли рабочие станции разблокированными, поскольку считали, что в случае утечки данных они с большей вероятностью будут наказаны или уволены».

Было также установлено, что большинство сотрудников осознают ценность соблюдения ISP и потенциальную опасность утечки данных. Однако устаревшие требования ISP могут ввергать персонал в конфликт приоритетов. Например, врачам может потребоваться смириться с возможностью утечки данных если они имеют дело с пациентом, которому требуется неотложная помощь

Саркар настаивает на необходимости поиска путей согласования ISP со всеми аспектами каждодневной работы разных сотрудников организации». ***(Политики безопасности нужно адаптировать к субкультурам внутри предприятий // Компьютерное Обозрение (https://ko.com.ua/politiki_bezopasnosti_nuzhno_adaptirovat_k_subkulturam_vnutri_predpriyatij_134807). 08.10.2020).***

***

«Операторы программы-вымогателя Netwalker опубликовали украденные данные K-Electric, крупнейшей частной энергетической компании Пакистана, после того, как выкуп не был уплачен.

7 сентября 2020 года компания K-Electric подверглась атаке программы-вымогателя Netwalker, которая нарушила работу сервисов онлайн-биллинга, но не поставила электроэнергию.

Вскоре после этого BleepingComputer получила доступ к странице оплаты выкупа Tor за атаку K-Electric, где операторы вымогателей потребовали выплату в размере 3 850 000 долларов. Злоумышленники также заявили, что освободят файлы, украденные во время атаки, если не будет уплачен выкуп.

В заявлении для BleepingComputer K-Electric отрицала факт кражи каких-либо данных у компании…

Netwalker публикует украденные данные

На этой неделе Netwalker опубликовал архив размером 8,5 ГБ с файлами, предположительно украденными у K-Electric во время сентябрьской атаки вымогателей.

Пакистанская компания по кибербезопасности Rewterz, которая изучила содержимое архива, сообщила BleepingComputer, что он содержит конфиденциальную информацию, такую как финансовые данные, информация о клиентах, технические отчеты, журналы обслуживания и многое другое.

Эти данные включают неаудированные отчеты о прибылях и убытках, технические схемы турбин и изображения отчетов клиентов, которые помечены как сделанные K-Electric.

Поскольку в ходе этой атаки раскрывается разнообразная информация, клиенты должны быть обеспокоены тем, что их личная информация могла быть раскрыта.

Для K-Electric также важно обеспечивать прозрачность раскрываемой информации, чтобы сотрудники и клиенты могли адекватно защитить себя.

BleepingComputer связалась с K-Electric для другого заявления, но не получила ответа». ***(Lawrence Abrams. Hackers leak files stolen in Pakistan's K-Electric ransomware attack // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/hackers-leak-files-stolen-in-pakistans-k-electric-ransomware-attack/). 01.10.2020).***

***

«Методика подсчета пользователей, открытая исследователем безопасности Карло Ди Дато, демонстрирует, как можно использовать Gravatar для массового сбора данных своих профилей веб-сканерами и ботами.

Gravatar - это онлайн-сервис аватаров, который позволяет пользователям устанавливать и использовать изображение профиля (аватар) на нескольких веб-сайтах, поддерживающих Gravatar.

Наиболее известные варианты использования Gravatar - это, пожалуй, веб-сайты WordPress, интегрированные с сервисом и GitHub.

Хотя данные, предоставленные пользователями Gravatar в их профилях, уже являются общедоступными, аспект услуги простого перечисления пользователей практически без ограничения скорости вызывает опасения в отношении массового сбора пользовательских данных.

Как получить доступ к профилю Gravatar (официально)

В нашей демонстрации этой ошибки мы будем использовать профиль "beau", упомянутый в документации Gravatar. Этот профиль принадлежит Бо Лебенсу, руководителю отдела разработки продуктов для WooCommerce в Automattic.

Согласно официальной документации Gravatar, структура URL-адреса профиля Gravatar состоит либо из имени пользователя, либо из хэша MD5 адреса электронной почты, связанного с этим профилем.

Это означает, что к профилю с именем пользователя beau можно получить доступ по адресу https://en.gravatar.com/beau или перейдя по адресу https://www.gravatar.com/205e460b479e2e5b48aec07710c08d50, который в конечном итоге перенаправит посетителя на общедоступную страницу пользователя. Страница Gravatar.

Это не проблема: в любом из этих случаев имя пользователя Beau Gravatar или параметры MD5 не могли быть легко предсказаны посетителем и должны были быть известны заранее.

Однако дополнительный метод доступа к данным пользователя, не раскрытый в документации, включает простое использование числового идентификатора, связанного с каждым профилем, для получения данных.

Скрытый маршрут URL-адреса позволяет перечислять пользователей

Итальянский исследователь безопасности Карло Ди Дато, обнаружив эту возможность, обратился к BleepingComputer на этой неделе после того, как не смог получить конкретные меры от Gravatar.

Как видно из приведенного выше примера профиля Бо, нажатие на ссылку «JSON» на странице приводит к тому, что http://en.gravatar.com/beau.json возвращает JSON-представление данных профиля.

Поле id в большом двоичном объекте JSON сразу привлекло внимание Ди Дато.

Скрытый маршрут API в службе позволяет любому получить данные JSON пользователя, просто используя поле «id» профиля.

«Я заметил интересное поле с именем «id» (это целое число). Следующим шагом было проверить, доступен ли мой профиль с помощью «id», - сказал исследователь BleepingComputer.

"Итак, я перешел на http://en.gravatar.com/ ID.json, и это сработало. Теперь, когда я знаю, что могу получить доступ к [данным пользователя JSON], используя целочисленное значение, следующим логическим шагом было проверить, могу ли я выполнить перечисление пользователей», - продолжил он.

Написав простой тестовый скрипт, который последовательно посещает URL-адреса профилей с идентификаторами от 1 до 5000 (как показано ниже), Ди Дато смог без проблем собрать данные JSON первых 5000 пользователей Gravatar.

http://en.gravatar.com/1.json
http://en.gravatar.com/2.json
http://en.gravatar.com/3.json
http://en.gravatar.com/4.json

«Если вы посмотрите файл JSON, вы найдете много интересной информации. Опасность такого рода проблем заключается в том, что злоумышленник может загрузить огромный объем данных и выполнить любую атаку социальной инженерии против законных пользователей, - сказал Ди Дато.

В наших тестах BleepingComputer мог подтвердить, что в определенных профилях пользователей было больше общедоступных данных, чем в других, например, адреса кошельков BitCoin, номера телефонов, местоположение и т. Д.

Пользователи, которые создают общедоступные профили на Gravatar, соглашаются сделать эти данные общедоступными, поэтому это не утечка данных или проблема конфиденциальности в этом отношении.

"Конечно, мистер Стивен знает, что после регистрации на Gravatar его данные станут общедоступными. Я почти уверен, что он не знает, так это то, что я смог получить эти данные, запрашивая Gravatar способом, который не должен быть возможно», - заявил Ди Дато.

Он продолжил: «Как Gravatar заявляет в своих руководствах, у меня должен быть адрес электронной почты мистера Стивена или его имя пользователя Gravatar для выполнения запроса. Без этой информации мне было бы почти невозможно получить данные мистера Стивена, верно?

Подобная проблема становится проблематичной, потому что любой веб-сканер или бот теперь может последовательно запрашивать практически всю базу данных Gravatar и очень легко собирать общедоступные пользовательские данные благодаря этой малоизвестной, но эффективной технике.

В прошлом преступники массово собирали данные профилей Facebook, используя его API, и продавали их в даркнете для получения прибыли.

BleepingComputer отправил Gravatar по электронной почте комментарий, но мы еще не получили от них ответа». ***(Ax Sharma. Online avatar service Gravatar allows mass collection of user info // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/online-avatar-service-gravatar-allows-mass-collection-of-user-info/). 03.10.2020).***

***

«Мошенники предлагают компенсацию, для получения которой необходимо перейти по ссылке. Таким образом жертва попадает на мошеннический сайт, после чего в распоряжении преступников оказываются деньги и данные банковской карты.

По словам специалистов, злоумышленники используют популярность сервиса Zoom в связи с переходом россиян на дистанционную работу. Аналитики установили, что письма были отправлены не с фейкового домена, а от официального сервиса.

«Все дело в том, что при регистрации Zoom предлагает пользователю заполнить профиль - указать «Имя» и «Фамилию», предоставляя возможность

вставить до 64-х символов в каждое поле. Мошенники используют эту возможность, вставляя фразу: «Вам положена компенсация в связи с COVID-19» и указывают ссылку на мошеннический сайт», – отметили в компании». ***(Group-IB выявила новую схему мошенничества с использованием сервиса Zoom // SecurityLab.ru (https://www.securitylab.ru/news/512793.php). 06.10.2020).***

***

«Власти Германии оштрафовали шведскую компанию H&M на 35 млн евро за утечку данных пользователей в результате внутреннего инцидента, имевшего место в центре обслуживания в Нюрнберге.

«Региональный регулятор в области защиты данных в Гамбурге наложил административный штраф в размере 35 млн евро. Группа H&M признает недостатки в работе своего сервисного центра и приняла решительные меры для их устранения», - приводит Reuters выдержку из финансового отчета компании за июнь-август 2020 года.

Как ранее сообщал SecurityLab, в начале текущего года Гамбургский комиссар по защите данных инициировал расследование в отношении H&M в связи с возможным нарушением им законодательства о защите данных. Как оказалось, сервисный центр компании собирал и хранили данные об условиях проживания сотрудников H&M. Кроме того, в рамках так называемых бесед «с возвращением» руководство опрашивало работников после их возвращения из отпусков или больничных, уточняя подробности о поездках и диагнозах.

Данная сумма является самым крупным штрафом, наложенным властями Германии за нарушение «Общего регламента по защите данных» (GDPR), закона Евросоюза о защите персональной информации, вступившего в силу в мае 2018 года. Крупнейший в Европе штраф (50 млн евро) за нарушение GDPR наложил французский регулятор на компанию Google в прошлом году». ***(Власти Германии оштрафовали H&M на 35 млн евро за нарушение GDPR // SecurityLab.ru (https://www.securitylab.ru/news/512688.php). 02.10.2020).***

***

«Поставщик облачных CRM-систем Blackbaud признался, что стал жертвой операторов вымогательского ПО, и информация о банковских счетах клиентов была похищена преступниками. Однако ранее руководители Blackbaud отрицали факт кибератаки.

Представители компании признали, что заражение программой-вымогателем в мае нынешнего года привело к тому, что злоумышленники получили доступ к финансовой информации клиентов.

«После 16 июля дальнейшее расследование показало, что киберпреступники могли получить доступ к некоторым незашифрованным полям, предназначенным для информации о банковском счете, номеров социального страхования, логинам пользователей и/или паролям. В большинстве случаев поля, предназначенные для конфиденциальной информации, были зашифрованы и недоступны», — сообщили представители компании.

Данные слова являются полной противоположностью предыдущим заявлениям, сделанным через два месяца после взлома.

«Киберпреступники не имели доступа к информации о кредитных картах, о банковских счетах или номерах социального страхования. Поскольку защита данных наших клиентов является нашим главным приоритетом, мы оплатили требование киберпреступника, подтвердив, что удаленная копия была уничтожена», — заявили представители Blackbaud после взлома.

Облачная CRM-система компании используется преимущественно благотворительными организациями и организациями дополнительного образования, которые стремятся собрать подробную информацию о текущих и потенциальных будущих инвесторах». ***(Провайдер облачных вычислений признал факт атаки вымогателей // SecurityLab.ru (https://www.securitylab.ru/news/512696.php). 02.10.2020).***

***

«Британская авиакомпания British Airways оштрафована на 20 млн фунтов стерлингов (25,8 млн долл.) в рамках дела об утечке персональных и финансовых данных более 400 тыс. ее пользователей в 2018 году.

Согласно заявлению Управления комиссара по информации Великобритании (Information Commissioner's Office), опубликованному в пятницу, расследование дела о кибератаке выявило, что "авиакомпания обрабатывала крупные объемы персональных данных, не имея в наличии адекватных мер защиты информации", пишет ЦТС, ссылаясь на Интерфакс-Украина.

Штраф стал крупнейшим в истории ICO, причем сумма штрафа должна была составить 183 млн фунтов, но регулятор снизил ее, приняв во внимание последствия пандемии коронавируса для British Airways.

"Неспособность компании принять необходимые меры была неприемлемой, и это отразилось на сотнях тысяч людей", - заявила директор ICO Элизабет Денхэм. "Когда организации принимают непродуманные решения, касающиеся персональных данных, это может реально влиять на жизни людей", - отметила она…». ***(British Airways оштрафовали на 20 млн фунтов в связи с утечкой персональных данных // ЦТС (https://cfts.org.ua/news/2020/10/19/british_airways_oshtrafovali_na_20_mln_funtov_v_svyazi_s_utechkoy_personalnykh_dannykh_61326). 19.10.2020).***

***

«В течение первых трех кварталов 2020 года Google направил своим пользователям более 33000 предупреждений, чтобы предупредить их о спонсируемых государством фишинговых атаках, направленных на их учетные записи.

«В этих случаях мы также поделились нашими выводами с кампаниями и Федеральным бюро расследований», - сказал Шейн Хантли, директор Google Threat Analysis Group (TAG).

Яркие напоминания, отправленные пользователям Google, подвергшимся атакам при поддержке правительства, отображались даже тогда, когда попытки взлома были заблокированы, чтобы информировать их об опасности.

Google также уведомляет администраторов G Suite пользователей, чтобы повысить осведомленность о риске, с которым сталкивается их корпоративная сеть, чтобы заранее предупредить их о потенциальной атаке…

Эти уведомления показываются до 0,1% всех пользователей Gmail по данным Google, который советует им принять некоторые меры для защиты своих учетных записей.

К ним относятся участие в Программе расширенной защиты, обновление программного обеспечения, включение двухэтапной аутентификации Gmail, а также использование Google Authenticator и / или физического ключа безопасности для двухэтапной аутентификации.

В целом, Google отправил 33015 предупреждений о фишинге при поддержке правительства в 2020 году, из них 11 856 предупреждений было отправлено в течение первого квартала 2020 года, 11023 - во втором квартале 2020 года и 10136 - в третьем квартале 2020 года.

В марте Google заявила, что в течение 2019 года она доставила около 40 000 предупреждений о спонсируемых государством попытках фишинга или взлома вредоносного ПО, что на 25% меньше, чем в 2018 году…

В прошлом месяце Microsoft также сообщила, что наблюдала поддерживаемые государством хакерские группы, действующие из России, Китая и Ирана, активно нацеленные на лиц и организации, участвовавшие в президентских выборах в США в 2020 году.

«Мы напрямую уведомили тех, кто был атакован или скомпрометирован, чтобы они могли принять меры для защиты», - заявила тогда Microsoft.

Одна из групп, стоящих за атакой, отслеживаемой Microsoft, APT31, поддерживаемая Китаем, также была обнаружена Google при нацеливании на «личные электронные письма сотрудников кампании с учетными фишинговыми письмами и электронные письма, содержащие ссылки для отслеживания»…

APT31 также размещал полезные нагрузки вредоносного ПО, которые использовали Dropbox для управления и контроля связи, а также доставлял поддельные установщики McAfee Total Protection на компьютеры жертв для развертывания вредоносных программ в фоновом режиме.

Северокорейские APT также были замечены Google при переключении целей на «исследователей COVID-19 и фармацевтические компании».

Отчеты Google и Microsoft подтверждают разведданные, предоставленные правительством США. о российских, иранских и китайских хакерских группах, пытающихся «скомпрометировать личные коммуникации американских политических кампаний, кандидатов и других политических целей».

Сегодня Google также сообщил, что в 2017 году субъект из национального государства нацелился на тысячи IP-адресов Google в ходе крупнейшей в истории DDoS-атаки со скоростью более 2,54 терабит в секунду». ***(Sergiu Gatlan. Google warned users of 33,000 state-sponsored attacks in 2020 // BleepingComputer.com***

(https://www.bleepingcomputer.com/news/security/google-warned-users-of-33-000-state-sponsored-attacks-in-2020/). 16.10.2020).

***

«Страны-участницы альянса Five Eyes (который объединяет спецслужбы Австралии, Канады, Новой Зеландии, США и Великобритании), а также Индия и Япония в очередной раз призвали технологические компании оставлять бэкдоры в своих продуктах, чтобы правоохранительные органы имели доступ к контенту в удобочитаемом и удобном формате.

В минувшие выходные члены альянса опубликовали официальное заявление, в котором призвали технологические компании создавать специальные решения, при помощи которых правоохранительные органы могли бы получать доступ к связи, защищенной сквозным шифрованием. Нужно сказать, что Five Eyes далеко не впервые пытается вынудить технологические компании внедрять бэкдоры в свой код. К примеру, с аналогичными призывами организация уже выступала в 2018 и 2019 годах.

На этот раз в Five Eyes заявили, что ИТ-компании сами загоняют себя в угол, оснащая продукты end-to-end шифрованием (E2EE). Ведь E2EE позволяет пользователям вести полностью защищенные разговоры (будь то чат, аудио или видео), не предоставляя ключ шифрования даже самим компаниями.

По мнению экспертов Five Eyes, все это мешает правоохранительным органам расследовать преступления, а сами компании оказываются неспособны обеспечить соблюдение своих же собственных пользовательских соглашений и не могут предоставить необходимые данные следователям. Заявление гласит, что в итоге шифрование ставит под угрозу безопасность «очень уязвимых членов нашего общества, таких как дети, подвергающиеся сексуальной эксплуатации».

«Мы призываем технологические компании сотрудничать с правительствами и предпринимать шаги, ведущие к разумным и технически осуществимым решениям», — пишут представители правительств семи стран.

В частности Five Eyes предлагает:

обеспечить безопасность общественности, заложив ее в системы при проектировании, что позволит компаниям эффективнее бороться с нелегальным контентом и деятельностью, не снижая при этом безопасности, а также будет способствовать расследованию и судебному преследованию правонарушений и защите уязвимых [категорий граждан];

предоставлять правоохранительным органам доступ к контенту в удобочитаемом и удобном формате, если разрешение выдано на законных основаниях, является необходимым и соразмерным, и будет применено в соответствии со строгими гарантиями и контролем.

Официальные лица заявили, что намерены работать с технологическими компаниями над разработкой решений, которые позволят пользователям продолжать применять безопасные зашифрованные коммуникации, но также позволят правоохранительным органам и технологическим компаниям бороться с преступной деятельностью.

При этом семь правительств призвали внедрить бэкдоры не только в зашифрованные мессенджеры, но также применять их в случаях «шифрования устройств, кастомных зашифрованных приложений и шифрования на интегрированных платформах». ***(Мария Нефёдова. Альянс Five Eyes, Индия и Япония призвали добавлять бэкдоры в ПО // Хакер (https://xakep.ru/2020/10/12/five-eyes-wants-backdoors/). 12.10.2020).***

***

«Выборка объемом 700 МБ, содержащая около 4 тыс. видеороликов и фотографий, доступна бесплатно.

Хакерская группировка выставила на продажу доступ к более чем 50 тыс. взломанных домашних камер видеонаблюдения, включая видеозаписи.

Как сообщило информагентство AsiaOne, группировка, насчитывающая более 1 тыс. участников по всему миру, использует платформу обмена сообщениями Discord для рекламы своих товаров.

Злоумышленники предлагают доступ к видеозаписям с камер за единовременную абонентскую плату в размере $150 и утверждают, что уже продали более 3 ТБ клипов. Выборка объемом 700 МБ, содержащая около 4 тыс. видеороликов и фотографий, доступна бесплатно.

Это не первый случай, когда пользователи домашних камер видеонаблюдения становятся жертвами утечек данных. Например, в декабре прошлого года учетные данные для авторизации тысяч владельцев камер Amazon Ring, а также 3672 электронных адреса, пароли, информация о часовых поясах и названия, присвоенные конкретным камерам Ring (например, «парадная дверь» или «кухня») были опубликованы в интернете». ***(Хакеры выставили на продажу доступ к видеозаписям с 50 тыс. домашних камер // SecurityLab.ru (https://www.securitylab.ru/news/513062.php). 14.10.2020).***

***

«Статистическая служба Евростат опубликовала результаты опроса жителей стран Европейского Союза о проблемах передачи персональных данных социальным или профессиональным интернет-сервисам.

Согласно опросу, каждый четвертый гражданин ЕС в возрасте от 16 до 74 лет в 2019 году избегал предоставления личной информации интернет-сервисам из соображений безопасности.

Среди стран-членов ЕС самый высокий показатель недоверия был зафиксирован во Франции (40%), за которой следуют Нидерланды (39%), Финляндия (37%), Словакия и Швеция (36%).

С другой стороны, самыми доверчивыми пользователями оказались жители Восточной Европы. Персональные данные при общении с социальными и профессиональными интернет-сервисам скрывали лишь 6% респондентов в Литве, 8% — в Болгарии и Венгрии и 9% — в Хорватии и Румынии». ***(Каждый четвертый европеец боится предоставлять данные интернет-сервисам // SecurityLab.ru (https://www.securitylab.ru/news/513071.php). 14.10.2020).***

***

«Умные» часы Xplora 4 от китайской компании Qihoo 360 Technology Co., предназначенные для детей, могут скрытно делать фотографии и записывать аудио при активации путем зашифрованного SMS-сообщения. Как сообщили эксперты из ИБ-компании Mnemonic, бэкдор представляет собой не уязвимость, а преднамеренно скрытый функционал.

«Бэкдор сам по себе не является уязвимостью. Это набор намеренно разработанных функций, которые включают удаленную съемку фотографий, отправку данных о местоположении и прослушивание телефонных разговоров через встроенный микрофон. Бэкдор активируется путем отправки SMS-команд на устройство», — сообщили специалисты.

Согласно Mnemonic, Xplora 4 содержит пакет под названием «Persistent Connection Service», который запускается во время процесса загрузки Android и перебирает установленные приложения для создания списка «намерений» (команд для вызова функций в других приложениях).

При соответствующем намерении Android входящее зашифрованное SMS-сообщение, полученное приложением Qihoo SMS, может быть направлено через диспетчер команд в службе постоянного подключения для запуска команды приложения, такой как удаленной снимок памяти.

Для использования этого бэкдора необходимо знать номер телефона целевого устройства и его заводской ключ шифрования. По словам исследователей, эта информация известная компаниям Qihoo и Xplora, однако злоумышленник с физическим доступом к устройству может похитить данные с помощью специальных инструментов.

Как утверждают представители компании, проблема связана с неиспользованным кодом из прототипа, который в настоящее время исправлен. Когда разрабатывались «умные» часы, родители предоставили отзывы и пожелания иметь возможность связаться со своими детьми в чрезвычайной ситуации и получать изображения местоположения в случае похищения. Xplora включила данные функции в прототипе, но решила не реализовывать их в коммерческой версии из соображений конфиденциальности». ***(Детские смарт-часы Xplora 4 могут тайно следить за пользователями // SecurityLab.ru (https://www.securitylab.ru/news/512977.php). 13.10.2020).***

***

«Здається, уже не залишилося жодної людини, яка б не знала про те, що великі корпорації на регулярній основі збирають різноманітні дані про користувачів, щоб рекомендувати їм персоналізований контент і, звичайно ж, релевантну рекламу. Фахівці із компанії Clario, яка спеціалізується на кібербезпеці, вирішили нарешті оприлюднити рейтинг мобільних додатків, які збирають найбільше особистої інформації про своїх користувачів. Що важливо розуміти, експерти враховували не дані cookie, які використовуються додатками і сайтами для надання цільової реклами, а реальну інформацію, яку розробники знають або хочуть знати про користувачів, передає ONLINE.UA. За словами аналітиків, додатки збирають таку дані про користувача, як вік, стать, ім’я,

сексуальну орієнтація, релігійні уподобання, домашню адресу, улюблені місця, хобі, посаду на роботі, зарплата і навіть фізичні дані на зразок ваги, зросту та інформації про здоров'я. Згідно з останніми даними, найбільше даних про користувачів збирає Facebook. Соціальна мережа, яку створив Марк Цукерберг, збирає 70,59% персональних даних. Як стверджують експерти, наразі виняток – фізіологічні показники, фінансові та деякі інші дані. На другій щаблині опинився Instagram з 58,82%, а на третій сходинці – популярний сервіс знайомств Tinder з 55,88%. Що цікаво, з усіх сервісів Google у рейтинг потрапили тільки "Карти" з 20,59%. Навіть Ikea і Netflix знають про користувачів більше – 23,53% і 26,47% відповідно. Аналітики дивуються, оскільки саме браузер Google Chrome "славиться" своїми невгамовними апетитами щодо користувацької інформації – він збирає дані навіть у режимі "Інкогніто". Що важливо розуміти, навіть коли ви вручну вимкнете відслідковування у налаштуваннях, Google Chrome не перестане стежити за вами». ***(Нарешті опублікований рейтинг додатків, які найчастіше слідкують за користувачами // ONLINE.UA (https://novyny.online.ua/nareshti-opublikovaniy-reyting-dodatkiv-yaki-naychastishe-slidkuyut-za-koristuvachami_n826428/). 28.10.2020).***

***

«Пароль від профілю Трампа – «maga2020!», тобто скорочення передвиборчої фрази чинного президента «Make America Great Again!»

Нідерландський фахівець з кібербезпеки Віктор Геверс зламав акаунт у Twitter президента США Дональда Трампа, підібравши пароль з п'ятого разу. Про це повідомляє de Volkskrant.

За словами хакера, пароль від профілю Трампа – «maga2020!», тобто скорочення передвиборчої фрази чинного президента «Make America Great Again!».

Геверс також сказав, що в акаунті Трампа навіть не було двофакторної аутентифікації.

Хакер не став нічого писати в акаунті президента, зробивши тільки скріншоти як доказ того, що він дійсно отримав до нього доступ.

Хакер написав до адміністрації соцмережі, в ЦРУ, ФБР, Агентство з кібербезпеки США і ряд інших відомств, а також відправив лист у Білий дім, порадивши Трампу краще захистити свій акаунт…». ***(Хакер із п'ятої спроби зламав Twitter Трампа // Українські медійні системи (https://glavcom.ua/news/haker-iz-pyatoji-sprobi-zlamav-twitter-trampa-713332.html). 23.10.2020).***

***

«Крупная психотерапевтическая клиника в Финляндии находится в тяжелом стрессе после того, как злоумышленник запросил выкуп за базу данных клиентов с конфиденциальной информацией, украденной в результате утечки данных, которая, вероятно, произошла почти два года назад.

Тысячи историй болезни могут оказаться под угрозой, поскольку частная клиника является общенациональной практикой с более чем дюжиной отделений, а другие учреждения заключают контракты на ее услуги.

Утечка записей и вымогательство жертв

Центр психотерапии Вастаамо объявил об инциденте в прошлую среду, заявив, что вымогатель впервые связался с тремя его сотрудниками в сентябре и попросил 40 биткойнов (в настоящее время более $ 500 000), чтобы не разглашать украденные данные пациентов.

Злоумышленник пригрозил опубликовать данные о пациентах, пытаясь заставить клинику заплатить выкуп, и сдержал свое слово. По словам местного источника, после публичного уведомления на сайте анонимной сети Tor произошло утечка не менее 300 историй болезни.

Дело обострилось еще больше, когда вымогатель начал связываться с жертвами по электронной почте и просил 240 долларов в биткойнах (200 евро) за удаление их записей.

Сообщения имеют тему «Информация об автоответчике» и содержат личную информацию получателя.

Злоумышленнику, возможно, было предложено сделать это после того, как нескольким лицам, обнаружившим место утечки, предложили заплатить за удаление их информации из украденной базы данных. По сообщению Ilta Sanomat, для них шантажист установил цену в 0,05 биткойна (около 650 долларов).

В той же газете говорится, что злоумышленник «пишет на очень хорошем английском» и полагается на почтовые службы, ориентированные на конфиденциальность. Первоначально они использовали Tutanota, затем перешли на Protonmail и Cock.li, последний позволял регистрацию и использование через Tor и аналогичные службы конфиденциальности.

На пресс-конференции в воскресенье Национальное бюро расследований Финляндии подтвердило, что количество утечек данных о пациентах исчисляется десятками тысяч. Лаура Халминен из Helsingin Sanomat смогла подтвердить, что шантажист слил не менее 2000 историй болезни.

Согласно ее отчету, вымогатель на короткое время загрузил файл размером 10 ГБ с информацией о пациентах Vastaamo, включая имена, номера социального страхования, почтовые и электронные адреса, номера телефонов и заметки терапевтов о посещениях пациентов.

Нарушение до приобретения скрыто

Вастаамо публиковал обновления об инциденте почти ежедневно с момента первого публичного раскрытия информации. Перед этим клиника проинформировала Финский центр кибербезопасности, Валвиру, и комиссара по защите данных.

Этичные хакеры в Финляндии также помогают властям, предоставляя полиции любые цифровые хлебные крошки, которые они находят у вымогателей, такие как сообщения, скриншоты сайтов и метаданные.

Технические аспекты взлома расследуются компанией по кибербезопасности Nixu, которая обнаружила, что инцидент, вероятно, произошел в ноябре 2018 года.

«На основании расследований представляется вероятным, что утечка данных, которая привела к краже клиентской базы данных, произошла в ноябре 2018 года» - Вастаамо

Это означает, что конфиденциальная информация клиентов, зарегистрированных после взлома, не включается в утечки, поясняет Вастаамо в своих уведомлениях.

Однако это было не единственное вторжение. В середине марта 2019 года произошло еще одно нарушение, и генеральный директор знал об этом, но решил сохранить это в секрете от Совета директоров частной клиники, властей и затронутых лиц.

После этого разоблачения совет директоров Vastaamo освободил Вилле Тапио от должности генерального директора компании.

На данном этапе расследования не ясно, украли ли хакеры базу данных клиентов, но есть вероятность, что злоумышленник просмотрел или скопировал информацию.

В результате мартовского нарушения были предприняты шаги по устранению проблем, связанных с защитой информации о клиентах, особенно с учетом того, что в мае компания PTK Midco должна была приобрести Vastaamo.

В рамках процесса приобретения в апреле-мае 2019 года был проведен внешний аудит кибербезопасности. Проблем не выявлено.

Согласно обновлениям Vastaamo, расследование Nixu пока подтверждает, что инфраструктура клиники не имела критических уязвимостей безопасности и не подвергалась кибератакам после марта 2019 года.

PTK Midcon, принадлежащая частной инвестиционной компании Intera Partner, является основным акционером Vastaamo и в понедельник начала судебный процесс по поводу процесса приобретения в мае 2019 года.

Vastaamo предлагает жертвам утечки данных поддержку по телефону, советуя, что делать в случае утечки их личной информации в Интернете». ***(Ionut Ilascu. Finnish psychotherapy clinic discloses data breach, victims extorted // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/finnish-psychotherapy-clinic-discloses-data-breach-victims-extorted/). 27.10.2020).***

***

«Иммиграционная юридическая фирма Fragomen, Del Rey, Bernsen & Loewy, LLP выявила утечку данных, в результате которой были раскрыты личные данные нынешних и бывших сотрудников Google.

Fragomen - одна из крупнейших юридических фирм США, занимающихся иммиграционным правом, с более чем 582 адвокатами в 47 местах по всему миру.

Нарушение данных раскрывает формы занятости в США

В «Уведомлении о взломе данных», отправленном сотрудникам Google, пострадавшим от взлома, Fragomen заявляет, что они несут ответственность за предоставление Google услуг по проверке занятости I-9.

Согласно уведомлению, юридическая фирма недавно узнала, что их сеть была взломана, и хакер получил доступ к файлу, содержащему личную информацию Googler.

«Недавно нам стало известно о подозрительной активности в нашей компьютерной сети. Пока наше расследование продолжается, мы обнаружили, что неавторизованная третья сторона получила доступ к одному файлу, содержащему

личную информацию, относящуюся к службам проверки занятости I-9. Этот файл содержал личную информацию для определенное количество сотрудников Google (и бывших сотрудников Google), включая вас», - говорится в уведомлении об утечке данных.

Форму I-9 должна быть заполнена всеми сотрудниками США, чтобы объявить их гражданство и право на работу в Соединенных Штатах.

Эта форма содержит информацию, которая может включать полное имя сотрудника, почтовый адрес, дату рождения, адрес электронной почты, номер телефона, номер социального страхования, номера паспортов и другие иммиграционные идентификаторы.

Поскольку эта информация является очень конфиденциальной и может быть использована злоумышленниками для кражи личных данных или других злонамеренных действий, все затронутые сотрудники Google должны внимательно следить за попытками целевого фишинга или мошеннической деятельности в своих кредитных отчетах.

Fragomen предлагает один год бесплатного кредитного мониторинга всем пострадавшим сотрудникам Google.

BleepingComputer связался с Google и Fragomen с вопросами о количестве пострадавших и о том, как произошла атака, но не получил ответа». ***(Lawrence Abrams. Google employees personal info exposed in law firm data breach // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/google-employees-personal-info-exposed-in-law-firm-data-breach/). 26.10.2020).***

***

«Microsoft улучшила обнаружение спрея паролей в Azure Active Directory (Azure AD), удвоив количество взломанных учетных записей, которые она обнаруживает с помощью новой системы машинного обучения (ML).

«Это новое обнаружение машинного обучения дает 100-процентное увеличение запоминаемости, что означает, что оно обнаруживает вдвое больше скомпрометированных учетных записей, чем предыдущий алгоритм», - сказал Алекс Вайнерт, директор по безопасности идентификационной информации Microsoft.

«Он делает это, сохраняя при этом поразительную точность предыдущего алгоритма в 98 процентов - это означает, что если этот алгоритм говорит, что учетная запись попала под спрей паролей, это почти наверняка так».

Машинное обучение используется для повышения эффективности обнаружения

Microsoft создала эвристический движок, ориентированный на обнаружение атак с использованием спрея паролей, который помог компании обнаруживать и предупреждать клиентов о сотнях тысяч атак каждый месяц (350 000 в апреле 2018).

Этот механизм обнаружения предоставляет клиентам Azure AD доступ к уведомлениям функции защиты личных данных (через лицензию Azure AD Premium P2) при обнаружении атаки с использованием паролей.

Теперь компания улучшила механизм обнаружения компрометации учетных данных для клиентов Azure AD Identity Protection с помощью новой системы машинного обучения, которая использует известные шаблоны атак и дополнительные данные для повышения эффективности обнаружения атак.

Данные, используемые новым режимом машинного обучения, используемым для повышения возможностей обнаружения компрометации учетных данных, включают, помимо прочего, различные сигналы отклонения поведения учетной записи, такие как незнакомые свойства входа и репутация IP.

«Это новое обнаружение спрея паролей - отличный пример того, как мы используем информацию, полученную в системах идентификации Microsoft, для постоянного расширения и улучшения нашей защиты, которую вы можете использовать для автоматизации процессов в условном доступе Azure AD, в Azure Sentinel или через API для все, что вы можете себе представить », - добавил Вайнерт.

Встроенная защита паролем Azure AD

Злоумышленники запускают атаки с распылителем паролей через большие бот-сети, пытаясь подобрать учетные записи одной или нескольких организаций, сопоставляя имена пользователей с коротким списком общих (обычно слабых) паролей, что позволяет им скрыть неудачные попытки с использованием разных IP-адресов.

Это также позволяет им преодолевать автоматические средства защиты, предназначенные для блокировки нескольких неудачных попыток входа в систему, таких как блокировка вредоносных IP-адресов и блокировка пароля.

Защита паролей Azure AD была запущена в апреле 2019 года (общедоступная предварительная версия с сентября 2019 года), чтобы снизить риски, связанные с атаками со спреем паролей, поскольку пользователи не могут выбирать легко угадываемые пароли, что резко снижает вероятность успеха таких атак примерно до 1%, говорит Вайнерт.

«Каждый цвет отслеживает свой хэш пароля для попыток входа в систему с неправильными паролями в Azure Active Directory (Azure AD). Просматривая миллионы клиентов, мы можем увидеть образец атаки с использованием распыления пароля», - пояснил Вайнерт.

«Обычно график был бы плоским и равномерно рассредоточенным, как вы видите на левой стороне. Огромный рост одного хеш-кода, сбойного во многих учетных записях, указывает на попытку применения одного пароля к сотням тысяч имен пользователей от многих клиентов - атака с использованием спрея пароля в прогресс."

Чтобы начать работу с защитой паролей Azure AD, вам необходимо войти на портал Azure как глобальный администратор, перейти в Azure Active Directory> Методы аутентификации, где вы можете управлять защитой паролем.

Клиенты с доступом к Azure AD Identity Protection могут получить доступ к новым отчетам об обнаружении рисков на портале и с помощью API-интерфейсов для Identity Protection». ***(Sergiu Gatlan. Microsoft upgrades password spray attack detection capabilities // Bleeping Computer®***

(https://www.bleepingcomputer.com/news/security/microsoft-upgrades-password-spray-attack-detection-capabilities/). 26.10.2020).

***

«Массовая утечка данных, от которой пострадала служба Nitro PDF, затронула многие известные организации, включая Google, Apple, Microsoft, Chase и Citibank.

Приложение Nitro, которое, как утверждают, используют более 10 тысяч бизнес-клиентов и 1,8 миллиона лицензированных пользователей, используется для создания, редактирования и подписания PDF-файлов и цифровых документов.

В рамках своего предложения услуг Nitro предлагает облачную службу, используемую клиентами для обмена документами с коллегами или другими организациями, участвующими в процессе создания документов.

Программное обеспечение Nitro страдает от утечки данных

21 октября Nitro Software выпустила уведомление для Австралийской фондовой биржи, в котором говорилось, что они пострадали от «инцидента безопасности, не оказавшего серьезного воздействия», но никакие данные клиентов не пострадали…

Оказывается, в этой истории может быть больше, чем было заявлено изначально.

Кибербезопасность разведка фирма Cyble сказала BleepingComputer, что угроза актер продает пользовательские и документы баз данных, а также 1 Тб документов, что они утверждают, что украдены из облачного сервиса Nitro Software.

Эти данные сейчас продаются на частном аукционе со стартовой ценой в 80 000 долларов.

Cyble заявляет, что таблица базы данных user_credential содержит 70 миллионов записей пользователей, содержащих адреса электронной почты, полные имена, хешированные пароли bcrypt, заголовки, названия компаний, IP-адреса и другие данные, связанные с системой.

BleepingComputer смог определить подлинность украденной базы данных пользователей, подтвердив известные адреса электронной почты учетных записей Nitro, которые присутствовали в базе данных.

База данных документов содержит название файла, информацию о том, был ли он создан, подписан, какой учетной записи принадлежит документ и является ли он общедоступным…

Если злоумышленники украдут документы, как они утверждают, это может быть одним из самых серьезных нарушений корпоративных данных, которые мы видели за последнее время.

Поскольку Nitro обычно используется предприятиями для цифровой подписи конфиденциальных финансовых, юридических и маркетинговых документов, он может допускать утечку информации, которая может существенно повлиять на бизнес компании.

BleepingComputer не смог подтвердить, были ли документы украдены в результате этой атаки.

Для тех, кто обеспокоен тем, что их учетная запись Nitro является частью этого взлома, Cyble добавил данные в свою службу AmIBreached.com. Пользователи могут отправить свой адрес электронной почты и проверить, был ли он обнаружен в украденной базе данных с помощью этой службы.

Обновление 27.10.20: Nitro отправил BleepingComputer обновленное заявление о том, что «домены электронной почты в этих журналах не являются «клиентами» или «учетными записями» Nitro. К сожалению, это не кажется точным, поскольку база данных пользователей, которую видит BleepingComputer, действительно содержит столбец хешированного пароля bcrypt.

Nitro продолжает расследование изолированного инцидента безопасности, связанного с ограниченным доступом к базе данных Nitro со стороны неавторизованной третьей стороны. База данных инцидентов не содержит никаких пользовательских или клиентских документов, которые хранятся в отдельной базе данных в другом месте.

База данных инцидентов в основном используется для регистрации сервисов, связанных с популярными бесплатными онлайн-сервисами конвертации документов Nitro.

Для использования бесплатных сервисов конвертации документов Nitro не требуется, чтобы пользователи создавали учетную запись или становились клиентом Nitro. Пользователи должны указать адрес электронной почты - преобразованные файлы доставляются на указанный адрес электронной почты, а общие домены электронной почты часто вводятся и будут отображаться в этих журналах.

Для ясности, домены электронной почты в этих журналах не являются «клиентами» или «учетными записями» Nitro, и журналы не содержат никаких документов.

В настоящее время нет установленных доказательств того, что какие-либо конфиденциальные или финансовые данные, касающиеся клиентов, были скомпрометированы. Нет никакого влияния на Nitro Pro или Nitro Analytics.

Окружающая среда Nitro была полностью защищена сразу после обнаружения инцидента. Хотя база данных инцидентов не содержит конфиденциальной или финансовой информации, а пароли надежно зашифрованы, мы общаемся с клиентами и в качестве меры предосторожности реализовали сброс пароля». ***(Lawrence Abrams. Massive Nitro data breach impacts Microsoft, Google, Apple, more // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/massive-nitro-data-breach-impacts-microsoft-google-apple-more/). 26.10.2020).***

***

«Популярные чат-приложения, в том числе LINE, Slack, DM в Twitter и другие, также могут пропускать данные о местоположении и делиться личной информацией со сторонними серверами.

Как выяснили исследователи, превью ссылок в популярных приложениях для чата на iOS и Android - это проблема безопасности и конфиденциальности. В зоне риска находятся Facebook Messenger, LINE, Slack, Twitter Direct Messages, Zoom и

многие другие. Согласно анализу, в случае Instagram и LinkedIn с помощью этой функции даже можно выполнять удаленный код на серверах компаний.

Предварительный просмотр ссылок является стандартным в большинстве приложений для чата и может быть очень полезным. Когда пользователь отправляет ссылку, он отображает краткую сводку и изображение для предварительного просмотра прямо в чате, поэтому другим пользователям не нужно щелкать ссылку, чтобы увидеть, на что она указывает.

К сожалению, есть и обратная сторона. По словам независимых исследователей Талала Хаджа Бакри и Томми Мыска, эта функция может вызывать утечку IP-адресов, раскрывать ссылки, отправляемые в чатах со сквозным шифрованием, и была обнаружена «незаметно загружая гигабайты данных в фоновом режиме».

По словам исследователей, проблемы связаны с тем, как создаются превью. Это можно сделать тремя способами: отправитель может его сгенерировать; приемник может его генерировать; или сервер может его сгенерировать. Последние два проблематичны, причем больше всего беспокоит версия, созданная сервером.

«Как приложение узнает, что показывать в сводке?» Бакры и Мыск объяснили. «Он должен каким-то образом автоматически открывать ссылку, чтобы узнать, что внутри. Но безопасно ли это? Что делать, если ссылка содержит вредоносное ПО? Или что, если ссылка ведет к очень большому файлу, который вы не хотите, чтобы приложение загружало и использовало ваши данные ».

Ссылки, созданные отправителем

Если отправитель создает предварительный просмотр, приложение загрузит содержимое ссылки, создаст сводку и изображение предварительного просмотра веб-сайта, и оно отправит это как вложение вместе со ссылкой.

«Когда приложение на принимающей стороне получает сообщение, оно будет показывать предварительный просмотр, полученный от отправителя, без необходимости открывать ссылку», - пояснили исследователи в публикации на этой неделе. «Таким образом, получатель будет защищен от риска, если ссылка злонамеренная».

Они отметили, что iMessage, Signal (если в настройках включен предварительный просмотр ссылок), Viber и WhatsApp следуют этому передовому подходу. Но когда дело доходит до Viber, есть нюанс.

«Если вы отправите ссылку на большой файл, ваш телефон автоматически попытается загрузить весь файл, даже если он имеет размер в несколько гигабайт», - отметили исследователи.

Они добавили: «Также стоит упомянуть, что даже несмотря на то, что чаты Viber зашифрованы из конца в конец, нажатие на ссылку заставит приложение перенаправить эту ссылку на серверы Viber в целях защиты от мошенничества и персонализированной рекламы».

Ссылки, созданные получателем

Когда получатель создает предварительный просмотр, это означает, что приложение автоматически откроет любую ссылку, отправленную на него, без вмешательства пользователя.

«Этот плохой», - сказали исследователи, отметив, что процесс может привести к утечке данных о местоположении.

«Давайте кратко объясним, что происходит, когда приложение открывает ссылку», - написали они. «Во-первых, приложение должно подключиться к серверу, на который ведет ссылка, и спросить у него, что находится в ссылке. Это называется запросом GET. Чтобы сервер знал, куда отправить данные, приложение включает IP-адрес вашего телефона в запрос GET ».

Они добавили: «Если вы используете приложение, которое следует этому подходу, все, что нужно сделать злоумышленнику, - это отправить вам ссылку на свой собственный сервер, где он сможет записать ваш IP-адрес. Ваше приложение с радостью откроет ссылку, даже если вы не нажмете на нее, и теперь злоумышленник будет знать, где вы находитесь [вплоть до городского квартала] ».

Вторая проблема заключается в том, что ссылка потенциально может указывать на большой видео- или архивный файл.

«Приложение с ошибками может попытаться загрузить весь файл, даже если он имеет размер в гигабайты, что приведет к расходу заряда аккумулятора и тарифного плана вашего телефона», - предупреждают исследователи.

Ссылки, созданные сервером

Наконец, в третьем подходе приложение отправляет ссылку на внешний сервер и просит его создать предварительный просмотр, а затем сервер отправит предварительный просмотр обратно как отправителю, так и получателю.

Хотя это позволяет избежать проблемы утечки IP-адреса, обнаруженной в сценарии генерации получателя, по словам исследователей, он потенциально предоставляет информацию третьим сторонам и может позволить выполнение кода, если ссылка указывает на вредоносный веб-сайт с помощью JavaScript.

Что касается раскрытия данных, серверу необходимо будет сделать копию (или, по крайней мере, частичную копию) того, что находится по ссылке, для создания предварительного просмотра.

«Допустим, вы отправляете кому-то частную ссылку Dropbox и не хотите, чтобы кто-то еще видел, что в ней содержится», - пишут исследователи. «Возникает вопрос… загружают ли серверы файлы целиком или только небольшую часть для предварительного просмотра? Если они загружают файлы целиком, хранятся ли копии на серверах, и если да, то как долго? И надежно ли хранятся эти копии, или люди, управляющие серверами, могут получить к ним доступ?»

Этот подход используется в нескольких приложениях для предварительного просмотра ссылок. Но при тестировании они сильно различаются по количеству данных, загруженных серверами, по словам исследователей:

Discord: загружает до 15 МБ любых файлов.

Facebook Messenger: загружает целые файлы, будь то изображение или видео, даже файлы размером в гигабайты.

Google Hangouts: загружает до 20 МБ любого файла.

Instagram: точно так же, как Facebook Messenger, но не ограничивается файлами любого типа. Серверы загрузят все, что угодно, независимо от размера.

LINE: загружает до 20 МБ любого файла.

LinkedIn: загружает до 50 МБ любого файла.

Slack: загружает до 50 МБ любого файла.

Twitter: загрузка до 25 МБ любого файла.

Масштаб: загрузка до 30 МБ любого файла.

«Хотя большинство серверов приложений, которые мы тестировали, устанавливают ограничение на объем загружаемых данных, даже ограничение в 15 МБ по-прежнему охватывает большинство файлов, которые обычно передаются по ссылке (большинство изображений и документов не превышают несколько МБ. размером)», - отметили исследователи. «Так что, если на этих серверах будут храниться копии, это станет кошмаром конфиденциальности, если когда-либо произойдет утечка данных на этих серверах».

По словам Бакри и Мыска, эта проблема вызывает особую озабоченность у пользователей LINE, потому что LINE утверждает, что имеет сквозное шифрование, при котором только отправитель и получатель могут читать сообщения.

«Когда приложение LINE открывает зашифрованное сообщение и находит ссылку, оно отправляет эту ссылку на сервер LINE для создания предварительного просмотра», - утверждают исследователи. «Мы считаем, что это противоречит цели сквозного шифрования, поскольку серверы LINE знают все о ссылках, которые отправляются через приложение, и о том, кто и кому какие ссылки передает. В принципе, если вы создаете приложение с сквозным шифрованием, пожалуйста, не следуйте подходу [сгенерированному сервером]».

После того, как исследователи отправили отчет группе безопасности LINE, компания обновила свой FAQ, включив в него информацию о том, что они используют внешние серверы для предварительного просмотра ссылок, а также информацию о том, как их отключить.

Facebook Messenger и его родственное приложение Instagram Direct Messages - единственные в тестировании, которые не ограничивают объем данных, загружаемых для создания предварительного просмотра ссылки. Facebook ответил на опасения исследователей, заявив, что считает, что функция работает должным образом, но не подтвердил, как долго он хранит данные. Twitter дал такой же ответ.

«Как мы объяснили исследователю несколько недель назад, это не уязвимости системы безопасности», - сказал Threatpost представитель компании facebook. «Описанное поведение - это то, как мы показываем предварительный просмотр ссылки в Messenger или как люди могут делиться ссылкой в Instagram, и мы не храним эти данные. Это соответствует нашей политике в отношении данных и условиям обслуживания».

Тем временем Slack подтвердил, что кэширует предварительные просмотры ссылок только на 30 минут, что также объясняется в его документации.

Zoom сообщил исследователям, что он изучает проблему и обсуждает способы обеспечения конфиденциальности пользователей.

Исследователи также связались с Discord, Google Hangouts и LinkedIn, чтобы сообщить о своих выводах, но заявили, что не получили ответа от этих двоих.

Проблемы с удаленным выполнением кода

Что касается проблемы выполнения кода, исследователи опубликовали видео с доказательством того, как хакеры могут запускать любой код JavaScript на серверах Instagram. А в случае с LinkedIn Messages серверы также были уязвимы для запуска кода JavaScript, что позволило им обойти ограничение на загрузку в 50 МБ в тесте.

«Нельзя доверять коду, который можно найти во всех случайных ссылках, которыми делятся в чатах», - объяснили Бакри и Мыск. «Однако мы нашли как минимум два основных приложения, которые сделали это: Instagram и LinkedIn. Мы проверили это, отправив ссылку на веб-сайт на нашем сервере, который содержал код JavaScript, который просто выполнял обратный вызов на наш сервер. Мы смогли подтвердить, что на этих серверах у нас было не менее 20 секунд времени выполнения. Может показаться, что это не так уж много, и наш код на самом деле не сделал ничего плохого, но хакеры могут проявить изобретательность».

Когда мы связались с ним через DM в Twitter, Майск сообщил Threatpost: «В ходе нашего тестирования злоумышленник может запустить любой код JavaScript на этих серверах. Хотя может быть не сразу очевидно, как это может нанести реальный вред, запуск кода JavaScript оставляет дверь открытой для команды преданных злоумышленников. Самая простая атака - это что-то вроде добычи криптовалюты на этих серверах и использования их ресурсов».

Ни одна из компаний не ответила на опасения исследователей. Но представитель Facebook сообщил Threatpost, что эта функция работает, как задумано, и что это не уязвимость системы безопасности. Этот человек добавил, что способ представления функциональности не учитывает стандартные меры безопасности, которые Instagram ввел для защиты от рисков выполнения кода, и что, когда о проблеме было сообщено, он «не обнаружил риска RCE».

Что касается LinkedIn, представитель Threatpost сообщил Threatpost по электронной почте: «Чтобы обеспечить безопасность наших участников, мы используем среду песочницы для оценки риска безопасности передаваемых ссылок. Эти среды эфемерны и имеют строгий контроль доступа, предназначенный для обнаружения выполнения вредоносного кода. С этой целью мы выполняем JavaScript в содержимом URL-адреса для полноты оценки. Мы также не кэшируем содержимое этих URL-адресов. Все эти шаги предприняты для проверки содержания ссылки на безопасность».

Но Мыск заметил, что такой защиты может быть недостаточно.

«Средства защиты на стороне сервера, такие как запуск кода JavaScript в среде песочницы, эффективны в предотвращении большинства атак, но более сложные атаки могут позволить злоумышленнику покинуть песочницу и выполнить код за пределами защищенной среды, что потенциально может позволить злоумышленнику украсть данные. и секретные ключи », - сказал он Threatpost. «Мы видели много успешных попыток выйти из песочницы JavaScript в таких приложениях, как Chrome, и эти серверы предварительного просмотра ссылок ничем не отличаются».

В поисках безопасности

Проблема с предварительным просмотром ссылок - это еще одна проблема, когда речь идет о безопасности приложений для совместной работы, которые стали неотъемлемой частью реальности работы из дома, вызванной пандемией COVID-19.

Хорошей новостью является то, что некоторые приложения вообще не отображают превью, например Signal (если в настройках отключена опция предварительного просмотра ссылок), Threema, TikTok и WeChat.

«Это самый безопасный способ обработки ссылок, поскольку приложение ничего не сделает со ссылкой, если вы специально не нажмете на нее», - отметили исследователи.

Однако они также предупредили, что предварительный просмотр ссылок является широко распространенным явлением: «Существует множество приложений для электронной почты, бизнес-приложений, приложений для знакомств, игр со встроенным чатом и других видов приложений, которые могут неправильно генерировать предварительный просмотр ссылок и могут быть уязвимыми. к некоторым из проблем, которые мы рассмотрели». ***(Tara Seals. Researchers: LinkedIn, Instagram Vulnerable to Preview-Link RCE Security Woes // Threatpost (https://threatpost.com/linkedin-instagram-preview-link-rce-security/160600/). 27.10.2020).***

***

«На этой неделе Amazon уведомила клиентов и правоохранительные органы об инциденте с инсайдерской угрозой.

Amazon уволила сотрудника, который поделился именами клиентов и адресами электронной почты с третьей стороной.

Представитель Amazon сообщил Threatpost, что у него есть системы для ограничения и контроля доступа к информации, а также процессы для выявления и расследования подозрительного поведения. Эти системы уведомили Amazon о «подозрительном поведении». После расследования инцидента компания уволила сотрудника, направила его в правоохранительные органы и сотрудничает с правоохранительными органами в их уголовном преследовании.

«Никакой другой информации, связанной с вашей учетной записью, не разглашается», - говорится в примечании, опубликованном в Twitter несколькими клиентами Amazon. «Это не результат того, что вы сделали, и вам не нужно предпринимать никаких действий. Приносим извинения за этот инцидент ».

Amazon не прокомментировал запрос Threatpost о том, сколько клиентов было затронуто, и какова была роль сотрудника Amazon.

«Для предприятий критически важно осознавать, что угрозы от законных пользователей всегда были более неуловимыми и их труднее обнаружить или предотвратить, чем традиционные внешние угрозы», - сказал Орион Кассетто, директор по маркетингу продуктов Exabeam, в заявлении по электронной почте. «Хотя степень утечки в настоящее время неизвестна, ряд клиентов Amazon были уведомлены о том, что их адреса электронной почты были переданы третьей стороне сотрудником, что привело к их увольнению. Организации должны быть вооружены инструментами для предотвращения атак изнутри своих стен»…».

(Lindsey O'Donnell. Amazon Fires Employee Who Leaked Customer Names, Emails // Threatpost (https://threatpost.com/amazon-fires-employee-customer-data/160610/). 27.10.2020).

***

«Клиенты Made in Oregon, местного ритейлера, стали жертвами мошенничества после утечки платёжных данных.

Как заявили представители компании, злоумышленники получили доступ к сайту в период между февралём и августом 2020 года.

На прошлой неделе вендор разослал письма с информацией об утечке 7,800 клиентам, которые совершили покупки в этот период. По информации ритейлера, могли быть скомпрометированы такие данные клиентов, как их имена, адреса проживания и доставки, электроные почты и данные кредитных карт.

Представители вендора считают, что реальное число пострадавших от утечки очень небольшое, но ритейлер решил предупредить всех клиентов, так как данные любого из них могут быть скомпрометированы.

Об инциденте сообщили в правоохранительные органы, было запущено расследование. Потенциально пострадавшим клиентам предложили услугу мониторинга средств на год». ***(Ритейлер из Орегона пострадал от серьёзной утечки данных // SecureNews (https://securenews.ru/oregon-retailer-suffers-from-severe-data-breach/). 23.10.2020).***

***

Кібербезпека Інтернету речей

«Специалисты международного разработчика антивирусного программного обеспечения, эксперта в области киберзащиты – компании ESET в рамках Месяца кибербезопасности, стартовавшего в Украине в октябре, подготовили 5 основных правил безопасного пользования смарт-устройствами и защиты интернета вещей (IoT).

«Сегодня устройства интернета вещей стали неотъемлемой частью жизни каждого, упрощая выполнение повседневных дел. Использование голосового помощника помогает записать заметку или поставить напоминание о встрече, подключение смартфона к камерам видеонаблюдения и смарт-звонкам обеспечивает удобное управление системой дома, а смарт-телевизоры позволяют насладиться просмотром любимых фильмов. С ростом популярности смарт-устройств увеличивается интерес к ним со стороны киберпреступников, которые постоянно ищут новые способы атак пользователей», - сообщила компания ESET.

Защищайте Wi-Fi роутер

В первую очередь, согласно данным ESET, для безопасности интернет-соединения следует обеспечить надежную защиту роутера, который является основным устройством интернета вещей. Большинство пользователей после установки роутера оставляют настройки по умолчанию, что является достаточно

распространенной ошибкой. Это может представлять большую угрозу безопасности подключенных устройств. Поэтому следует немедленно сменить пароли для подключения к роутеру и для доступа к его настройкам.

«При смене пароля выберите вариант WPA2 (или WPA 3 на более новых роутерах, если все ваши устройства могут подключаться к нему). Кроме этого, не забывайте обновлять встроенное программное обеспечение до последней версии, хотя многие из роутеров делают это автоматически, однако время от времени следует проверять актуальность версий», - отмечают в компании.

Шифруйте веб-трафик

Эксперты по кибербезопасности добавляют, что еще одним способом повышения безопасности онлайн и защиты интернета вещей является шифрование веб-трафика. Самый простой метод — создать виртуальную частную сеть (VPN), которая будет работать как зашифрованный туннель для веб-трафика. Это позволит не только защитить персональные данные от посторонних лиц, но и в случае необходимости — получить доступ к ним из любой точки мира.

Позаботьтесь о безопасности смартфона

Мобильные устройства обладают функционалом компьютеров и используются не только для звонков, но и для фотосъемки, хранения файлов, получения и отправки электронной почты. Поскольку большинство этих задач предусматривает доступ к личным данным и подключение к интернету, смартфон должен быть надежно защищен.

Как сообщают специалисты ESET, для большинства смартфонов доступны решения по безопасности, которые помогают предотвратить проникновение угроз на устройство. Однако, для дополнительной защиты следует зашифровать все конфиденциальные данные на смартфоне. Таким образом, в случае получения доступа к устройству, киберпреступники не смогут прочитать личные данные пользователя.

Защищайте смарт-телевизор

Сегодня трудно найти телевизор, который не обладает смарт-функциями. Соответственно такие устройства, как отмечают в компании ESET, тоже могут быть скомпрометированы киберпреступниками. В частности, злоумышленники могут использовать уязвимости для удаленного управления телевизором или инфицировать устройство вредоносным программным обеспечением.

«Чтобы защитить смарт-телевизор, сначала следует правильно настроить его. Прежде всего необходимо определить параметры конфиденциальности для данных, которые может собирать провайдер, а также включить функцию родительского контроля для защиты детей от нежелательного контента. Кроме того, важно проверить наличие обновлений встроенного программного обеспечения, и, конечно, загрузить решение по безопасности для защиты смарт-телевизора», - подытожили специалисты ESET.

Обновляйте устройства

Регулярное обновление устройств — базовое правило кибербезопасности. По информации ESET, любые исправления безопасности и обновления следует применять сразу после их выхода, иначе пользователь рискует стать жертвой атак киберпреступников.

…по данным ESET, в Украине ежедневно фиксируется около 300 тыс. новых киберугроз для информационной безопасности. При этом, найти хакеров-злоумышленников крайне сложно, компаниям остается лишь проводить ежеминутные мониторинги на предмет выявления киберугроз с целью их дальнейшего блокирования…». ***(Надежда Бурбела. Специалисты по кибербезопасности дали советы, как усилить защиту интернета вещей // UNIAN.NET (https://www.unian.net/science/kiberbezopasnost-sovety-kak-usilit-zashchitu-interneta-veshchey-novosti-11172053.html). 06.10.2020).***

***

«Хакери можуть використати домашні прилади для вимагання викупу, DDoS атак та витоку даних.

Хакери можуть отримати доступ до будь-яких кухонних приладів - розумних холодильників, кавоварок тощо з метою отримати викуп або шантажувати власника приладу. Це журналісти видання Wired продемонстрували на прикладі кавоварки, яка видавала дивні звуки і вимагала викупу.

Експерт провів аналітик компанії Avast, яка займається розробкою антивірус, Мартін Хрон. Він відремонтував одну зі старих кавомашин, щоб спробувати її хакнути. Як виявилось, існує чимало способів це зробити.

Наприклад, досліднику вдалось за допомогою віддалено включили кавоварку, щоб вона одночасно молола кавові зерна і вимагала викуп. Зупинити це можна було лише виключивши кавоварку з електромережі.

«Мій експеримент показав, що інтернет речей може бути небезпечним. При цьому мені не довелось нічого налаштовувати. Продавці техніки зазвичай не думають про це», - заявив Хрон.

Під час експерименту прилад з легкістю приєднався до домашнього інтернету Хрона, при цьому не вимагав ніякого шифрування. Це ще більше спростило б задачу хакерам, які хотіли б зламати кавоварку.

Дослідник відмічає, що повідомлення з метою викупу - це найпростіше, що може використати потенційний зловмисник. За бажанням, він може запрограмувати кавоварку на будь-які дії. Хрон відмічає, що кавоварка має дуже обмежені можливості, а є домашні електронні прилади, які дають хакерам більше можливостей взлому.

«Зазвичай холодильник служить 17 років, але мало хто користується ним такий час. Це сприяє появі великої кількості покинутих приладів, які можуть стати зброєю в руках хакерів. Вони можуть використати їх для порушень мережі, витоку даних та DDoS-атак», - відмічає дослідник…». ***(Кавоварка, що вимагає викуп. Чим можуть бути небезпечні домашні прилади // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/25633/2020-10-02-kavovarka-shcho-vimagae-vikup-chim-mozhut-buti-nebezpechni-domashni-priladi/). 02.10.2020).***

***

«Согласно недавно представленному Microsoft отчету Digital Defense Report, злоумышленники стали все активнее использовать методы, которые затрудняют их обнаружение и выбирают своими целями даже самые защищенные организации.

За год компания заблокировала более 13 млрд вредоносных и подозрительных писем, из которых более 1 млрд включали URL-адреса, активирующие запуск фишинг-атак, нацеленных на получение учетных данных.

С октября 2019 г. по июль нынешнего года наиболее частой причиной реагирования на инциденты командами ИБ стали программы-вымогатели.

В числе самых распространенных техник атак, нацеленных на государственные организации, стали разведка, сбор учетных данных, использование вредоносного ПО и эксплойты виртуальных частных сетей.

Также из отчета следует, что продолжается активный рост количества угроз в области Интернета вещей. В первой половине текущего года общий объем подобных атак увеличился примерно на 35% по сравнению со второй половиной 2019 г.

Криминальные группировки продолжают экспериментировать с фишинговыми приманками, видами атак и различными способами сокрытия своей деятельности. Киберпреступники продолжают использовать такие человеческие черты, как любопытство, тревожность и потребность в информации. Соответственно, злоумышленники использовали новости, связанные с пандемией, для привлечения внимания широкого круга пользователей.

Около 70% всех киберинцидентов пришлось на данный вид мошенничества. Чтобы обманом заставить людей поделиться своими учетными данными, злоумышленники также отправляли электронные письма, имитирующие рассылку крупных компаний. Согласно данным телеметрии Office 365, основными брендами, под которые маскировали свои письма злоумышленники, стали Microsoft, UPS, Amazon, Apple и Zoom.

Модели атак показывают, что киберпреступники анализируют и тщательно выбирают время осуществления атаки, например, в праздничные дни, когда организации сложнее оперативно отреагировать на вторжение. Также они изучают потребности бизнеса, выбирая время, когда объекту атаки будет проще выплатить выкуп, чем оплатить простои, например, в течение биллинговых циклов в здравоохранении, финансах или юриспруденции.

Злоумышленники воспользовались пандемией, чтобы сократить время пребывания в системе жертвы – в некоторых случаях киберпреступники прошли путь от первоначального входа в систему до компрометации всей сети менее чем за 45 минут.

Удаленная работа бросает новые вызовы безопасности. Традиционные политики защиты периметра организации стало намного сложнее применять в более широкой сети, которая включает домашние и другие частные сети. По мере того, как организации продолжают перемещать приложения в облако,

киберпреступники стали чаще использовать DDoS-атаки, чтобы нарушить доступ пользователей и скрыть более опасные атаки на ресурсы организации.

Человеческий фактор остается основополагающим. В недавнем опросе, проведенном Microsoft, 73% директоров по ИБ указали, что их организация столкнулась с утечкой данных, а также конфиденциальных данных за последние 12 месяцев, и что они планируют потратить больше средств на технологии управления рисками инсайдерских атак в связи с пандемией COVID-19.

В первой половине текущего года также отмечен рост атак, направленных на компрометацию корпоративных учетных записей. В рамках этого метода используются систематическое угадывание, списки паролей, выгруженные учетные данные из предыдущих взломов и др. Учитывая частоту угадывания, фишинга, кражи с помощью вредоносного ПО или повторного использования паролей, очень важно, чтобы пользователи связывали пароли со вторым фактором надежной аутентификации. Для организаций включение многофакторной аутентификации (MFA) является необходимостью. Наши данные показывают, что включение многофакторной аутентификации предотвращает 99% всех атак, нацеленных на кражу учетных данных.

Учитывая резкое увеличение количества атак за последний год, важно предпринять шаги по установлению новых правил поведения в киберпространстве. Частные или государственные организации должны инвестировать в специалистов и технологии, а простые пользователи должны уделять внимание основным правилам кибергигиены, таким как регулярная установка обновлений для обеспечения безопасности, применение комплексных политик резервного копирования и использование многофакторной аутентификации.

Со своей стороны, Microsoft использует сочетание технологий, операционной деятельности и правовых механизмов для предотвращения и сдерживания злонамеренных действий. В качестве технической меры компания инвестирует в технологии интеллектуальной кластеризации Microsoft 365, чтобы дать возможность операционным центрам ИБ (SOC) обрабатывать информацию о более сложных инцидентах». ***(Александр Мацько. За год 73% CISO столкнулись с утечкой данных // Компьютерное Обозрение (https://ko.com.ua/za_proshedshij_god_73_ciso_stolknulas_s_utechkoj_dannyh_134822). 09.10.2020).***

***

«ИТ-системы компании Swatch подверглись «развивающейся» атаке, что, скорее всего, означает заражение шифровальщиком-вымогателем. Аналогичные атаки за последние несколько недель постигли сразу несколько крупных компаний во всем мире.

Атака в развитии

Компания Swatch, знаменитый швейцарский производитель часов, сообщила об отключении своих ИТ-систем после того как обнаружила несколько дней назад кибератаку на свои сети. Отключение систем было вызвано необходимостью остановить развитие атаки.

«Swatch Group подтверждает обнаружение явных признаков развивающейся кибератаки на некоторые из своих ИТ-систем в выходные. В целях безопасности группа компаний немедленно приняла меры к отключению части своих систем в профилактических целях, что сказалось на некоторых операциях, — говорится в заявлении организации. — Были проведены незамедлительные оценка и анализ природы атаки и предприняты надлежащие меры, а также внесены необходимые исправления».

В Swatch также заявили, что ситуация «вернется к норме, как только возможно», и что против предполагаемых инициаторов атаки будет подана жалоба в правоохранительные органы.

Не первые и не последние

Пресс-служба корпорации не уточнила, какого рода атака имела место, но логично предположить, что речь идет о заражении шифровальщиком. Компания является достаточно привлекательной мишенью для вымогателей. Обороты Swatch в 2019 г. составили $9,6 млрд, штат работников корпорации — 36 тыс. человек.

«Компании таких размеров привлекают особый интерес злоумышленников, надеющихся поживиться крупным выкупом, — говорит Анастасия Мельникова, эксперт по информационной безопасности компании SEC Consult Services. — Крупные компании рискуют вдвойне, поскольку операторы шифровальщиков теперь не только шифруют данные, но и крадут их, требуя деньги в двойном размере. Серия атак последних недель, по-видимому, объясняется расширением “партнерских программ” у наиболее крупных преступных группировок — все большее их количество работают по модели RaaS (шифровальщик как услуга)»… ***(Роман Георгиев. Часовой гигант Swatch отключил ИТ-системы из-за хакерской атаки // CNews (https://www.cnews.ru/news/top/2020-10-01_hakeryvymogateli_atakovali). 01.10.2020).***

***

«Tyler Technologies заплатила выкуп за ключ дешифрования для восстановления файлов, зашифрованных в результате недавней атаки программы-вымогателя.

Tyler Technologies заявляет, что это крупнейшая компания-производитель программного обеспечения в Северной Америке, работающая в государственном секторе, с доходом более 1,2 миллиарда долларов на 2020 год и 5 500 сотрудниками.

Забастовка вымогателей RansomExx

23 сентября Tyler Technologies подверглась кибератаке со стороны операторов вымогателя RansomExx, которые также стояли за недавними атаками на Konica Minolta и IPG Photonics.

В ответ на атаку Tyler Technologies немедленно отключила части своей сети, чтобы сдержать распространение программы-вымогателя и ограничить уязвимость своих клиентов.

«Сегодня рано утром мы узнали, что неавторизованный злоумышленник нарушил доступ к некоторым из наших внутренних систем. После обнаружения и из мер предосторожности мы закрыли точки доступа к внешним системам и

немедленно начали исследование и устранение проблемы. ИТ-директор Tyler Technologies Мэтт Биери написал клиентам электронные письма.

Атака вызвала серьезный сбой в работе Tyler Technologies, она была локализована и не распространилась на их клиентов.

Источники в государственном секторе сообщили BleepingComputer, что атака программы-вымогателя серьезно повлияла на Tyler Technologies и что компания ожидала, что для полного восстановления операций потребуется тридцать дней.

Платный выкуп за дешифратор

Источник сообщил BleepingComputer, что компания Tyler Technologies оплатила выкуп RansomExx за восстановление зашифрованных данных.

Однако неизвестно, сколько было заплачено за получение ключа дешифрования.

Когда программа-вымогатель зашифровывала файлы Tyler Technologies, они добавляли расширение, подобное «.tylertech911-f1e1a2ac».

Чтобы доказать, что дешифратор действовал, BleepingComputer смог расшифровать зашифрованные файлы [1, 2], загруженные в VirusTotal во время атаки вымогателя.

После расшифровки файл Arin.txt содержал список диапазонов IP-адресов, используемых компанией.

Также известно, что RansomExx крадет данные перед шифрованием устройств в сети. Затем операторы вымогателей угрожают раскрыть эти украденные данные, если жертва не заплатит выкуп.

Поскольку многие школьные округа, судебные системы, местные и государственные органы власти в Соединенных Штатах являются клиентами Tyler Technologies, риски публичной утечки конфиденциальной информации и исходного кода вызывают обеспокоенность.

Это беспокойство могло стать движущей силой при принятии решения о выплате выкупа.

Когда его спросили о дешифраторе, Tyler Technologies не оспорила выплату выкупа, но сказала BleepingComputer, что в настоящее время они не могут раскрывать какую-либо дополнительную информацию…» ***(Lawrence Abrams. Tyler Technologies paid ransomware gang for decryption key // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/tyler-technologies-paid-ransomware-gang-for-decryption-key/). 10.10.2020).***

***

«Министерство внутренней безопасности США сообщило, что неизвестные злоумышленники нацелились на сеть переписи населения США в прошлом году в своем первом отчете об оценке угроз для населения (HTA), опубликованном ранее на этой неделе.

Бюро переписи населения США является крупнейшим в США федеральным правительственным статистическим ведомством, ответственным за сбор статистических данных об экономике США и населения.

Затем эти данные используются федеральным правительством для выделения более 675 миллиардов долларов из федеральных фондов органам власти племен, местным властям и властям штата каждый год.

Атаки включали попытки несанкционированного доступа

DHS заявляет, что как государственные, так и негосударственные злоумышленники, вероятно, попытаются скомпрометировать или нарушить инфраструктуру, которую США используют для поддержки президентских выборов в США 2020 года, а также переписи населения США 2020 года.

В частности, DHS упоминает в отчете несколько случаев, когда неизвестные злоумышленники пытались получить доступ к системам в сети переписи населения США.

«Неизвестные актеры кибера занимались подозрительными связями с общественностью обращенных сетью переписи населения США, по меньшей мере, в прошлом году, в том числе проведения сканирования уязвимостей и попыток несанкционированного доступа,» отчет DHS HTA показывает [PDF].

«Кибератаки, направленная на перепись в США, может включать попытки получить незаконный доступ к массиву данных, собранных переписью; изменить регистрационные данные переписи; поставить под угрозу цепочку поставок инфраструктуры переписи или провести атаки типа «отказ в обслуживании».

Это не первый раз, когда переписи населения США становятся мишенью для злоумышленников, о чем свидетельствует отчет Reuters о взломах и DDoS-атаках во время тестирования систем переписи населения в 2018 году, когда российские IP-адреса были задействованы как минимум в одном из инцидентов.

«Он попал в сеть», - сказал Рейтер источник. «Он попал туда, где публика не должна идти».

К счастью, согласно источникам безопасности, ни один из инцидентов не привел к краже данных или повреждению систем.

«Мы работаем с ведущими экспертами из государственного и частного секторов, чтобы обеспечить безопасность и производительность наших систем, чтобы было легко и безопасно реагировать», - говорится в сообщении переписи.

Государственные субъекты угроз продолжат атаки

«Федеральные, государственные, местные, племенные и территориальные правительства, а также частный сектор столкнутся с множеством кибер-угроз, предназначенных для доступа к конфиденциальной информации, кражи денег и принуждения к выплате выкупа», - говорится в отчете HTA.

Среди этих злоумышленников DHS заявляет, что хакеры, связанные с государством, при поддержке Китая, России, Ирана и Северной Кореи, будут продолжать попытки атак, призванных поставить под угрозу или нарушить критически важную инфраструктуру выборов 2020 года, а также попытаться повлиять на мнения и мнения американских избирателей. предпочтения.

В то время как Россия, Китай и Иран также сосредоточат свои атаки на кибершпионаже, согласно DHS, «кибер-возможности Северной Кореи, хотя и являются сложными, вероятно, останутся ограниченными преступным получением доходов».

HTA DHS 2020 включает информацию об угрозах (разведывательную и оперативную) от нескольких агентств DHS, включая Иммиграционную и таможенную службу (ICE), Береговую охрану США и Службу таможенно-пограничной охраны США (CBP).

Этот первый в своем роде годовой отчет HTA предназначен для информирования партнеров из государственного и частного секторов, а также широкой общественности об угрозах, нацеленных на США.

Об этом докладе было объявлено в сентябре 2019 года, когда DHS опубликовало Стратегические рамки противодействия терроризму и целенаправленному насилию». ***(Sergiu Gatlan. DHS: Unknown hackers targeted the US Census Bureau network // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/dhs-unknown-hackers-targeted-the-us-census-bureau-network/). 09.10.2020).***

***

«Исследователи вредоносных программ, отслеживающие угрозы программ-вымогателей, заметили резкое увеличение количества таких атак за последние месяцы по сравнению с первыми шестью месяцами 2020 года.

Согласно недавно опубликованным данным Check Point и группы реагирования на инциденты IBM Security X-Force, в верхней части списка находятся семейства вымогателей Maze, Ryuk и REvil (Sodinokibi).

Обе компании наблюдали всплеск инцидентов с программами-вымогателями на глобальном уровне в период с июня по сентябрь, причем одни угрозы были более активными, чем другие.

Сектор здравоохранения под ударом

Данные Check Point, относящиеся к третьему кварталу года, показывают, что Maze и Ryuk были самыми распространенными семействами вымогателей, причем последние атаковали в среднем 20 компаний в неделю.

Согласно сегодняшнему отчету Check Point, Ryuk увеличил свою деятельность в июле и сосредоточился в основном на медицинских организациях, которые уже находятся в тяжелом стрессе от пандемии и не могут позволить себе отключение своих систем.

Компания заявляет, что количество атак программ-вымогателей увеличилось на 50% на глобальном уровне в третьем квартале 2020 года и что Ryuk и Maze были наиболее распространенными угрозами. В США количество таких атак в третьем квартале увеличилось почти вдвое, благодаря чему они вошли в пятерку наиболее пострадавших стран в третьем квартале:

США (рост 98,1%)

Индия (рост на 39,2%)

Шри-Ланка (рост на 436%)

Россия (рост на 57,9%)

Турция (рост на 32,5%)

Основываясь на данных, полученных в ходе мероприятий по реагированию на инциденты, IBM отмечает, что угрозы программ-вымогателей «взорвались в

июне 2020 года», когда они имели дело с третью всех подобных событий, зарегистрированных до сентября.

В конце сентября компания сообщила, что на Maze приходится 12% всех атак с использованием программ-вымогателей, расследованных в этом году командой X-Force Incident Response.

Однако наиболее распространенной разновидностью программ-вымогателей, с которыми столкнулась целевая группа IBM, была Sodinokibi (REvil), которая наблюдалась в 29% инцидентов, расследованных ими в 2020 году.

Согласно анализу IBM, REvil заявляет о более чем 140 жертвах в сфере оптовых, производственных и профессиональных услуг, большинство из которых из США. По оценкам компании, 36% из них заплатили требование выкупа.

IBM считает, что с запросами на сумму от 1500 до 42 миллионов долларов прибыль группы вымогателей REvil в этом году составила не менее 81 миллиона долларов.

Третьим по распространенности программ-вымогателем, обнаруженным IBM в 2020 году, является EKANS (Snake), на долю которого приходится 6% инцидентов, которые могут уничтожить процессы, связанные с операциями системы промышленного управления (ICS).

Атаки программ-вымогателей были настолько прибыльными для киберпреступников, что у этой угрозы почти нет шансов исчезнуть в ближайшее время, особенно с развитой тактикой (кража данных и их утечка или продажа в темной сети), разработанной для принудительного выкупа.

Непрерывное резервное копирование данных, хранящееся в автономном режиме, по-прежнему является хорошей практикой, которая может обеспечить более быстрое восстановление после такой атаки, так как своевременное применение обновлений безопасности и ограничение или отключение удаленного доступа к внутренней сети компании». ***(Ionut Ilascu. Ransomware threat surge, Ryuk attacks about 20 orgs per week // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/ransomware-threat-surge-ryuk-attacks-about-20-orgs-per-week/). 06.10.2020).***

***

«Неизвестная хакерская группа внедрила вредоносный код в законную службу отчетов об ошибках Windows (WER), чтобы избежать обнаружения в рамках бесфайловой атаки вредоносного ПО, обнаруженной исследователями Malwarebytes в прошлом месяце.

Использование службы WER в атаках с целью уклонения от защиты - не новая тактика, но, как заявили исследователи Malwarebytes Threat Intelligence Team Хоссейн Джази и Жером Сегура, эта кампания, скорее всего, является работой еще неизвестной группы кибершпионажа.

«Злоумышленники взломали веб-сайт, на котором размещены его полезные данные, и использовали структуру CactusTorch для проведения бесфайловой атаки с применением нескольких методов антианализа», - поясняется в отчете, заранее предоставленном BleepingComputer.

Целевой фишинг, используемый для сброса полезной нагрузки

Впервые атака была обнаружена 17 сентября после того, как исследователи обнаружили фишинговые письма, содержащие вредоносный документ, заключенный в ZIP-архив.

Первоначальная вредоносная нагрузка попадала на компьютеры целей посредством целевого фишинга с использованием электронных писем, в которых в качестве приманки использовалось требование компенсации работнику.

После открытия документ будет выполнять шелл-код с помощью вредоносного макроса, идентифицированного как модуль CactusTorch VBA, который загружает полезные данные.NET прямо в память теперь зараженного устройства Windows.

На следующем этапе этот двоичный файл выполняется из памяти компьютера, не оставляя следов на жестком диске, путем внедрения встроенного шеллкода в WerFault.exe, процесс Windows службы WER.

Тот же метод внедрения процесса используется другими вредоносными программами для обхода обнаружения, включая программы- вымогатели Cerber и NetWire RAT.

Недавно созданный поток службы отчетов об ошибках Windows, в который был внедрен вредоносный код, будет проходить несколько антианалитических проверок, чтобы узнать, отлаживается ли он, работает ли он на виртуальной машине или в среде песочницы, - все признаки проверки исследователем вредоносных программ.

Если все проверки пройдены и загруженное вредоносное ПО кажется достаточно безопасным, чтобы перейти к следующему шагу, оно расшифрует и загрузит окончательный шелл-код во вновь созданном потоке WER, который будет выполнен в новом потоке.

Последняя полезная нагрузка вредоносного ПО, размещенная в сети asia-kotoba [.] В виде фальшивого значка, затем будет загружена и введена в новый процесс.

К сожалению, Malwarebytes не смог проанализировать эту окончательную полезную нагрузку, поскольку URL-адрес хоста был недоступен в то время, когда исследователи анализировали атаку.

Возможные отпечатки APT32

Хотя исследователи Malwarebytes не смогли с достаточной уверенностью приписать атаку какой-либо хакерской группе, некоторые из индикаторов компрометации и использованной тактики указывают на поддерживаемую Вьетнамом группу кибершпионажа APT32 (также отслеживаемую как OceanLotus и SeaLotus).

Одним из них является тот факт, что APT32 известен тем, что использует модуль CactusTorch VBA для отбрасывания вариантов Denis Rat в своих атаках.

К сожалению, Malwarebytes не удалось получить копию окончательной полезной нагрузки после расследования этой атаки, чтобы установить прямое соединение.

Другой намек, который потенциально может связать эту атаку с вьетнамской хакерской группой, - это домен (yourrighttocompensation [.] Com),

зарегистрированный в Хошимине, Вьетнам, который использовался для размещения и доставки фишингового документа и вредоносных полезных данных.

APT32 ранее был нацелен на «иностранные компании, инвестирующие в производство, потребительские товары, консалтинг и гостиничный сектор Вьетнама», рассылая вредоносные вложения через целевые фишинговые электронные письма, согласно данным фирмы FireEye, занимающейся кибербезопасностью.

Также известно, что они стоят за целенаправленными атаками на исследовательские институты со всего мира, СМИ и правозащитные организации, а также на китайские морские строительные фирмы. [1, 2, 3, 4, 5, 6, 7] ***(Sergiu Gatlan. Hackers abuse Windows error service in fileless malware attack // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/hackers-abuse-windows-error-service-in-fileless-malware-attack/). 06.10.2020).***

***

«Район государственных школ Спрингфилда в Массачусетсе стал жертвой атаки с использованием программ-вымогателей, в результате которой школы были закрыты на время расследования кибератаки.

Спрингфилд - третий по величине школьный округ в Массачусетсе с более чем 25 000 учеников, 4500 служащими и более чем шестидесяти школами. Из-за пандемии COVID-19 в школьном округе была открыта модель дистанционного обучения с запланированным переходом на гибридное обучение к концу октября.

Сегодня округ объявил в Facebook, Twitter и с звонками родителям, что школы закрыты из-за «проблем» с их сетью.

Вскоре после первых уведомлений родителям и ученикам сообщили, что в районе произошла кибератака и что школьные устройства должны быть отключены…

Позже кибератака была подтверждена мэром Домеником Дж. Сарно и суперинтендантом Дэниелом Уорвиком, которые объявили о приостановке дистанционного обучения…

Ровно месяц назад, 8 сентября, школьный округ Хартфорд в Коннектикуте подвергся атаке программы-вымогателя, из-за которой был отложен первый школьный день.

По мнению Хартфорда, кибератака задержала открытие школы всего на один день.

Эта задержка может быть больше для Springfield, в зависимости от количества устройств, зашифрованных атакой программы-вымогателя, и времени, необходимого для их восстановления.

BleepingComputer связалась с мэрией Спрингфилда по поводу атаки, но пока не получила ответа». ***(Lawrence Abrams. Massachusetts school district shut down by ransomware attack // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/massachusetts-school-district-shut-down-by-ransomware-attack/). 08.10.2020).***

***

«Вымогатели начали использовать новую тактику для вымогательства у своих жертв: DDoS-атака на веб-сайт жертвы, пока она не вернутся за стол переговоров.

Распределенная атака типа «отказ в обслуживании» (DDoS) - это когда злоумышленник наводняет веб-сайт или сетевое соединение большим объемом запросов, чтобы сделать службу недоступной.

После того, как переговоры зашли в тупик в связи с недавней атакой программы-вымогателя, филиал программы-вымогателя SunCrypt совершил DDoS-атаку на сайт жертвы.

Когда жертва снова вошла на сайт оплаты Tor программы-вымогателя, ее приветствовало сообщение о том, что SunCrypt несет ответственность за DDoS и продолжит атаку, если переговоры не будут продолжены.

«В настоящий момент ваш веб-сайт не работает из-за усилий наших специалистов. Пожалуйста, отправьте нам сообщение как можно скорее, или будут предприняты дальнейшие действия», - предупредил жертву оператор программы-вымогателя SunCrypt.

Когда жертва спросила, почему они закрывают свой веб-сайт, операторы вымогателей заявили, что это было сделано для принуждения к переговорам.

«Мы были в [sic] процессе переговоров, и вы не явились, поэтому были предприняты дальнейшие действия», - заявили участники угрозы.

После того, как жертва снова начала переговоры о выкупе, оператор программы-вымогателя согласился, чтобы «техник» отключил DDoS-атаку.

Команда MalwareHunterTeam, которая поделилась чатом с BleepingComputer, рассказала нам, что эта тактика в конечном итоге привела к тому, что жертва заплатила выкуп.

Эта тактика оказалась особенно эффективной против этой жертвы, поскольку это была небольшая организация, которая уже сильно пострадала от атаки вымогателя.

Комбинируя кражу данных, угрозу утечки данных, отсутствие доступа к зашифрованным файлам, а теперь и DDoS-атаку, жертва могла полностью прекратить свою работу.

Это еще один пример того, как банды вымогателей обновляют свою тактику, чтобы усилить давление на своих жертв, чтобы они чувствовали, что у них нет другого выбора, кроме как заплатить выкуп». ***(Lawrence Abrams. Ransomware gangs add DDoS attacks to their extortion arsenal // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/ransomware-gangs-add-ddos-attacks-to-their-extortion-arsenal/). 01.10.2020).***

***

«Всплеск фишинговых и вредоносных веб-сайтов, нацеленных на обман клиентов Amazon.com, призван сделать Prime Day полем для хакеров.

Киберпреступники подключаются к ежегодной кампании Amazon для подписчиков Prime Day, где исследователи предупреждают о недавнем всплеске фишинговых и вредоносных веб-сайтов, которые мошенническим образом используют бренд Amazon.

Согласно отчету Bolster Research, опубликованному в четверг, с августа наблюдался всплеск количества новых ежемесячных фишинговых и мошеннических сайтов, созданных с использованием бренда Amazon, что стало самым значительным после пандемии COVID-19, вынудившей людей закрыться в помещении в марте.

«По мере того, как покупатели готовятся к двухдневным выгодным сделкам, киберпреступники готовятся охотиться на неосторожных, используя тех, кто теряет бдительность, чтобы скупить сделки», - пишут исследователи.

Prime Day на самом деле происходит в течение двух дней - в этом году мероприятие приходится на 13–14 октября. Клиенты Amazon Prime получают специальные скидки и скидки на лучшие бренды в ознаменование крупнейшего торгового события года на сайте гиганта онлайн-торговли.

Amazon в прошлом году принесли более $ 7 млрд в продажах в течение 36-часового мероприятия, которые могли бы пойти еще больше в этом году из - за «снижения несетевых розничных и непосредственной близости от праздников,» отметил исследователи. Действительно, обязательные заказы на домохозяйство во всем мире, которые начались с пандемии COVID-19 в марте, значительно стимулировали бизнес Amazon, и эта тенденция не имеет никаких признаков ослабления.

Исследователи проанализировали сотни миллионов веб-страниц, чтобы отследить количество новых фишинговых и мошеннических сайтов с использованием бренда и логотипов Amazon. Его исследования показывают, что злоумышленники используют преимущества как функций Amazon, так и поведения потребителей, чтобы заманить онлайн-покупателей на мошеннические сайты, которые могут украсть их учетные данные, финансовую информацию и другие конфиденциальные данные.

Одна из новых кампаний нацелена на «возврат» или «отмену заказов», связанных с Prime Day, с использованием мошеннического сайта www.amazoncustomersupport [.] Net, который имитирует законный сайт Amazon. Однако более пристальное изучение сайта показывает, что он явно предназначен для обмана потребителей, отметили исследователи.

Одним из явных доказательств является использование телефонного номера, поскольку «Amazon не поощряет обслуживание клиентов по телефону и прилагает большие усилия, чтобы найти поддержку по телефону на реальном сайте Amazon», - пишут исследователи.

Форма на сайте также запрашивает информацию о банке или кредитной карте от клиентов - явное намерение украсть эту информацию, поскольку Amazon всегда предлагает возврат средств на исходную форму оплаты или подарочные карты. Кроме того, сайт также не запрашивает пароль клиента, который всегда требуется Amazon для покупок и возврата.

На сайте также появляются другие более мелкие проблемы, на которые можно не обращать внимания, такие как неработающие ссылки, прикрепленные к логотипу Amazon Prime и кнопка «Начать». Исследователи отметили, что это также ключи к мошенничеству, на которые покупатели должны обращать внимание при совершении покупок в Prime Day.

Другой вредоносный сайт, недавно обнаруженный исследователями, использует врожденную любовь большинства потребителей к бесплатным подаркам. Сайт www.fr-suivre [.] Vip продвигает программу лояльности Amazon и предлагает бесплатный iPhone 11 Pro, если люди ответят на несколько вопросов. После ответов на эти вопросы люди попадают в простую игру, в которой они выигрывают, после чего их просят ввести данные кредитной карты, чтобы сайт мог взимать с них 1 доллар за получение iPhone.

На сайте даже есть снимок экрана, на котором «бесплатный iPhone подтверждается многими другими людьми, которые уже получили свои телефоны», - пишут исследователи. «Несмотря на восторженные отзывы, телефон за 999 долларов так и не поступит, и покупатель начинает видеть странные платежи по указанному номеру кредитной карты», - предупредили они.

К счастью, для клиентов Amazon Prime, которые планируют воспользоваться этим событием в этом году - или для тех, кто совершает покупки на Amazon в наши дни - избежать онлайн-мошенничества, по словам исследователей, не так уж сложно. Всем покупателям следует начинать прямо с источника - Amazon.com - и уделять пристальное внимание своему опыту, чтобы убедиться, что ничего необычного не происходит.

«Покупатели должны знать о киберпреступниках, готовых воспользоваться ситуацией», - отмечают исследователи. «При должном усердии и внимании к деталям покупатели смогут заключить эти сделки, не подвергаясь мошенничеству».

Amazon также может предпринять еще больше мер безопасности для защиты клиентов, поскольку ее бизнес продолжает процветать, а киберпреступность неизбежно следует этому примеру, заметил Кевин Бисли, ИТ-директор VAI, поставщика программного обеспечения для управления предприятием.

«Чтобы минимизировать риск утечки данных или проблем с безопасностью, розничные продавцы, такие как Amazon, должны установить дополнительную многофакторную аутентификацию для логинов и политик для защиты паролей и тех, кто имеет доступ к данным», - сказал он в электронном письме Threatpost.

По словам Бизли, интернет-магазины по всему миру также должны уйти в преддверии напряженного курортного сезона, сделав свою платформу «средой, ориентированной на безопасность».

Это может быть сделано «путем установки дополнительных уровней инфраструктуры безопасности между операционной системой и аппаратной платформой, а также непрерывного тестирования безопасности и автоматизации сканирования аппаратных и программных систем для поиска уязвимостей и исправления потенциальных проблем по мере их возникновения», - сказал он Threatpost». ***(Elizabeth Montalbano. Amazon Prime Day Spurs Spike in Phishing, Fraud Attacks // Threatpost (https://threatpost.com/amazon-prime-day-spurs-spike-in-phishing-fraud-attacks/159960/). 08.10.2020).***

***

«Несколько хакерских групп из Армении атаковали банки Азербайджана. Как утверждается, одной из групп удалось взломать банковские базы данных и "слить" персональные данные около 520 тысяч клиентов. Также

хакерам удалось получить доступ к информации о денежных переводах в банковской системе Азербайджана.

Как сообщает "Kapital Bank", от имени банка, руководящих лиц или сотрудников банка отправляются поддельные сообщения и электронные письма о том, что сервера банков подверглись нападению армянских хакеров и в связи с этим якобы нужно немедленно снять депозиты.

"Мы просим клиентов не придавать значения информации такого содержания, а также другим таким необоснованным и не указывающим источник сообщениям, и ссылаться только на официальные новости, размещенные банком в СМИ или на сайте" - сообщили в пресс службе банка.

Ранее армянские хакеры взломали базу данных военно-морского флота Азербайджана, в ответ хакеры из Азербайджана взломали ряд государственных сайтов Армении.

7 октября эксперты из Cisco Talos сообщили о вредоносной кампании, в рамках которой хакеры тайно взломали IT-сети правительства Азербайджана и получили доступ к дипломатическим паспортам некоторых официальных лиц». ***(Армянские хакеры атаковали банки Азербайджана // SecurityLab.ru (https://www.securitylab.ru/news/512910.php). 11.10.2020).***

***

«Инфраструктура одной из крупнейших в мире компаний по разработке программного обеспечения Software AG пострадала от атаки с использованием программы-вымогателя Clop.

Инцидент произошел 3 октября нынешнего года, когда операторы Clop проникли во внутренние сети компании и зашифровали файлы. За восстановление документов вымогатели потребовали свыше $20 млн - один из крупнейших выкупов за всю историю вымогательских атак.

В конце минувшей недели вымогатели опубликовали скриншоты похищенных данных на своем web-сайте. Информация включает сканы паспортов и удостоверений личности сотрудников Software AG, корпоративные письма, финансовые документы и папки из внутренней сети компании.

Software AG сообщила об инциденте в прошлый понедельник. В уведомлении представители компании отметили, что работа корпоративной сети была нарушена в результате кибератаки, но инцидент не повлиял на предоставление услуг клиентам, включая облачные сервисы. Однако тремя днями позже в компании признали факт хищения данных. В настоящее время неизвестно, заплатила ли компания требуемый выкуп». ***(Вымогатели потребовали более $20 млн у немецкого техногиганта Software AG // SecurityLab.ru (https://www.securitylab.ru/news/512909.php). 11.10.2020).***

***

«В этом месяце хакеры дважды поразили немецкую корпоративную интеграцию и платформу Интернета вещей Software AG с помощью программ-вымогателей.

5 октября данные были загружены с серверов и ноутбуков сотрудников компании, а ее внутренние системы были нарушены. По сообщениям, хакеры потребовали более 20 миллионов долларов США для расшифровки данных.

Когда Software AG отказалась, хакеры опубликовали скриншоты паспортов сотрудников компании, сканы документов, электронные письма и финансовые документы из ее внутренней сети в Dark Web, сообщает ZDNet.

Атака Software AG - это так называемое «двойное вымогательство», когда хакеры извлекают конфиденциальную коммерческую информацию перед тем, как зашифровать данные жертв. Затем хакеры угрожают опубликовать его, если их требования выкупа не будут выполнены, согласно Check Point Research, которая предоставляет аналитические данные о киберугрозах клиентам своей материнской компании Check Point Software, а также разведывательному сообществу в целом.

Как сообщает международная сеть профессиональных услуг KPMG, атаки с двойным вымогательством - один из «более творческих способов» получения выкупа, к которому стремятся хакеры.

Банды вымогателей увеличивают обороты

«Банды программ-вымогателей становятся все более смелыми и изощренными, преследуя более крупные и прибыльные цели с помощью своих преступных атак», - сказал Сарью Найяр, генеральный директор глобальной компании по кибербезопасности Gurucul. Атака на Software AG «является одной из крупнейших атак программ-вымогателей, но, конечно же, не последней».

Нет никаких сомнений в том, что хакеры становятся все более амбициозными - средний спрос на выкуп увеличился с 29000 долларов в 2018 году до более 302000 долларов в 2019 году, согласно данным Группы практики управления цифровыми активами и данными юридической фирмы BakerHostetler.

Самый большой выкуп, потребованный в прошлом году, составил 18,8 миллиона долларов, а самый крупный выкуп - 5,6 миллиона долларов. «Мы видим, что выплаты производятся ежедневно», - заявила группа BakerHostetler. «Вот насколько велика эта проблема».

«Программы-вымогатели прошли путь от оппортунистических и транзакционно-независимых атак до более целенаправленных и постоянных атак, направленных на уничтожение крупной игры», - сказал TechNewsWorld Марк Сангстер, вице-президент и специалист по стратегии безопасности в компании eSentire по управляемому обнаружению и реагированию.

Банды также стали более активными - по данным Check Point Research, за последние три месяца в США было почти вдвое больше атак с использованием программ-вымогателей, чем в период с января по июнь.

Отчасти это связано с тем, что пандемия вынуждает организации менять свои бизнес-структуры, что часто оставляет пробелы в их ИТ-системах, сказал Checkpoint. «Эти бреши дали киберпреступникам возможность использовать недостатки безопасности и проникнуть в сеть организации. Хакеры шифруют сотни тысяч файлов, выводя пользователей из строя и часто беря в заложники целые сети».

По заявлению КПМГ, удаленная работа «значительно увеличивает риск успешной атаки программы-вымогателя». Это «связано с сочетанием более слабого

контроля над домашними ИТ-системами и более высокой вероятностью того, что пользователи будут нажимать на электронные письма с приманками, посвященными COVID-19. Учитывая уровень беспокойства, преступные группировки все чаще переключаются на тематические приманки COVID-19 для фишинга».

Платить или не платить?

Данные жертвы зашифрованы почти в 75% атак с использованием программ-вымогателей, как показал глобальный опрос 5000 ИТ-менеджеров, проведенный по заказу фирмы Sophos, занимающейся кибербезопасностью.

Опрос также показал, что 56 процентов жертв получили свои данные из резервных копий и только 26 процентов получили их обратно, заплатив выкуп.

Однако «в определенных ситуациях выплата выкупа может быть не единственным вариантом, но может быть лучшим оперативным вариантом по разным причинам», - сказал TechNewsWorld Рон Пеллетье, основатель и директор по работе с клиентами компании Pondurance по управляемому обнаружению и реагированию.

Возьмите муниципалитет Лафайет в Колорадо, который заплатил хакерам выкуп в размере 45 000 долларов в июле после того, как они захватили его систему и заблокировали доступ к его данным.

Лафайет заплатил после того, как рассмотрел альтернативные решения, потому что «в сценарии рентабельности восстановления данных города вместо уплаты выкупа вариант вымогателя намного перевешивает попытки восстановления», - заявили в Сити. «Также было учтено неудобство длительного перерыва в обслуживании жителей».

Пеллетье отметил, что Pondurance работала с «несколькими новыми клиентами», которые заплатили выкуп и обратились к нему за помощью.

ФБР предлагает жертвам связаться с ним, вместо того, чтобы платить выкуп, как в противном случае они будут считаться легкими отметками злоумышленниками.

Выплата выкупа также удорожает борьбу с атаками программ-вымогателей. Sophos обнаружил, что средняя стоимость устранения последствий составляет чуть более 730 000 долларов для организаций, которые не платят, и более 1,4 миллиона долларов для тех, которые платят.

Правовые вопросы выплаты выкупа

Закон США не запрещает платить выкуп как таковой; но когда жертвы платят деньги людям или организациям, попавшим под санкции правительства США... они попадают в еще большие неприятности.

Управление по контролю за иностранными активами Министерства финансов США (OFAC) выпустило в октябре рекомендацию, в которой говорится, что американцам «как правило, запрещено прямо или косвенно участвовать в сделках» с организациями, включенными в его Список граждан особого назначения и заблокированных лиц (SDN). List), а также с другими заблокированными лицами и лицами, на которые распространяется полное эмбарго страны или региона.

OFAC налагает санкции на киберпреступные банды «других лиц, которые оказывают материальную помощь, спонсируют или предоставляют финансовую,

материальную или технологическую поддержку для этой деятельности» в соответствии с Законом о международных чрезвычайных экономических полномочиях (IEEPA) или Законом о торговле с врагами (TWEA). 1917 г.

IEEPA - это федеральный закон США, уполномочивающий президента регулировать международную торговлю после объявления чрезвычайного положения в стране в ответ на любую необычную и чрезвычайную угрозу стране, которая частично или полностью находится за границей. Он использовался для нацеливания на негосударственных лиц и группы, такие как террористы и киберпреступники.

TWEA - это федеральный закон США, который дает президенту право контролировать или ограничивать любую торговлю между нацией и ее врагами во время войны.

Любая транзакция, которая вызывает нарушение в соответствии с IEEPA, в том числе транзакции лица, не являющегося гражданином США, в результате которого лицо из США нарушает какие-либо санкции на основе IEEPA, также запрещена в соответствии с этими законами.

OFAC может налагать гражданско-правовые санкции за нарушение санкций на основе строгой ответственности, что означает, что лицо, подпадающее под юрисдикцию США, может быть привлечено к гражданской ответственности, даже «если оно не знало или не имело оснований знать, что оно совершает транзакцию с лицом, которое запрещено. "согласно постановлениям OFAC и законам о санкциях.

Гражданские и уголовные санкции «могут превысить миллионы долларов,» Григорий Шевчик и Филипп Yannella юридической фирмы Ballard Spahr написали.

Платежи также могут нарушать законы о борьбе с отмыванием денег и привести к тому, что компания будет отнесена к категории финансовых услуг в соответствии с Законом США о банковской тайне и постановлениями Министерства финансов, предупреждают Шевчик и Яннелла.

Это потребует от компании регистрации в Министерстве финансов и «подчинения сложной совокупности законов и постановлений», направленных на борьбу с отмыванием денег.

Должная осмотрительность имеет решающее значение

Тем не менее, не все преступники связаны с объектом санкций, сказал TechNewsWorld Тед Кобус, председатель группы управления цифровыми активами и данными BakerHostetler. «На самом деле подавляющее большинство - нет».

В сообщении OFAC четко указано, что сотрудничество с ФБР имеет решающее значение и что это сотрудничество «будет рассматриваться как существенный смягчающий фактор», когда дело доходит до правоприменения, отметил Кобус.

BakerHostetler говорит, что компании обычно привлекают третью сторону для проведения должной осмотрительности, чтобы гарантировать, что выкуп не выплачивается лицу, на которое наложены санкции, и гарантировать, что законы об отмывании денег не нарушаются.

«Процесс комплексной проверки не требует больших затрат, и если вы привлечете нужных экспертов, это может произойти без огромных затрат и усилий», - отметил Кобус. «Таким образом, ожидается, что компании любого

размера будут проводить соответствующие процедуры комплексной проверки». ***(Richard Adhikari. The Trials and Tribulations of Paying Ransomware Hackers // TechNewsWorld (https://www.technewsworld.com/story/86894.html). 23.10.2020).***

***

«Опытные киберпреступники похитили $15 млн у одной из американских компаний в результате тщательно подготовленной мошеннической операции, продолжавшейся в течение двух месяцев.

Как сообщает портал BleepingComputer, кибератаку с уверенностью можно назвать ювелирной работой. Сначала злоумышленники получили доступ к электронной переписке о переводе денежных средств, а затем внедрились в переговоры и переадресовали платежи на подложные счета. При этом им удалось достаточно долго скрывать факт хищения и успеть вывести краденые деньги.

Хотя проводившие расследование инцидента специалисты компании Mitiga изучили только данный конкретный случай, они обнаружили свидетельства того, что список жертв киберпреступников насчитывает десятки предприятий, в том числе архитектурных бюро, финансовых организаций и юридических фирм.

По словам специалистов, никакого вредоносного ПО в сетях пострадавшей компании обнаружено не было, зато был выявлен факт компрометации учетных данных электронной почты. Однако одного лишь доступа к электронному ящику киберпреступникам было мало, поскольку они могли лишиться его в любой момент. В связи с этим злоумышленники создали правила переадресации писем с целью получения всех входящих писем из нужного ящика.

С помощью сервиса электронной почты Microsoft Office 365 киберпреступники подделали домены двух сторон, участвовавших в транзакции. Использование Microsoft Office 365 позволило им сделать письма не вызывающими подозрений и способными обходить защитные решения. Кроме того, через регистратора доменов GoDaddy злоумышленники зарегистрировали два домена, очень похожие на домены, принадлежащие настоящим компаниям.

В течение четырех недель киберпреступники методично следовали разработанному плану, используя информацию, собранную из перехваченных электронных писем высшего руководства атакуемой компании. Когда дело дошло до обсуждения перевода денег, они «вклинились» в беседу с поддельного домена, похожего на домен одной из сторон переговоров, и предоставили подложные банковские реквизиты.

Банки могут блокировать денежные транзакции, если средства переводятся на неправильный счет, и киберпреступники заранее к этому подготовились. Для того чтобы скрыть кражу, они перевели деньги на счета в зарубежных банках и запутали след. Злоумышленники также создали правила фильтрации, согласно которым письма с определенных электронных адресов попадали в скрытую папку. Поэтому легитимные владельцы электронных ящиков не видели писем с обсуждением перевода денег. Таким образом, за две недели злоумышленники «заработали» $15 млн.» ***(Как киберпреступники украли $15 млн у одной из американских компаний // SecurityLab.ru (https://www.securitylab.ru/news/512784.php). 06.10.2020).***

***

«Эксперты американской компании Visa сообщили, что в начале нынешнего года были взломаны системы двух североамериканских компании в сфере гостеприимства. В ходе атак преступники заразили системы вредоносным ПО для PoS-терминалов.

Вредоносное ПО для PoS-систем заражает компьютеры под управлением Windows, ищет PoS-приложения, а затем сканирует память устройства на предмет данных платежных карт, которые обрабатываются в приложениях для PoS-платежей.

Компания Visa не указала названия компаний-жертв кибератак из-за соглашений о неразглашении, связанных с расследованием инцидентов.

По результатам расследования июньской атаки, Visa обнаружила в сети жертвы три разных вида вредоносного ПО для PoS-систем — RtPOS, MMon (также известный как Kaptoxa) и PwnPOS. Злоумышленники взломали сеть компании в сфере гостеприимства, «использовали инструменты для удаленного доступа и утилиты для сброса учетных данных с целью получить начальный доступ, перемещаться по сети и развернуть вредоносное ПО для PoS».

Специалисты не смогли определить, как злоумышленники проникли в сеть компании. Однако они смогли определить точку входа в первой атаке, произошедшей в мае.

«Первоначальный доступ к торговой сети был получен посредством фишинговой кампании, нацеленной на сотрудников организации. Учетные записи пользователей, включая учетную запись администратора, были скомпрометированы в рамках фишинг-атаки и использовались злоумышленниками для входа в среду компании. Затем участники использовали легитимные административные инструменты для доступа к среде данных о держателях карт (cardholder data environment, CDE) в сети компании», — пояснили эксперты.

Установив доступ к CDE, преступники развернули скраперы памяти для сбора данных о платежных счетах, а затем использовали пакетный скрипт для массового развертывания вредоносного ПО в сети организации. Вредоносное ПО для PoS, использованное в рамках данной атаки, было идентифицировано как версия TinyPOS». ***(Хакеры атаковали PoS-системы двух североамериканских компаний // SecurityLab.ru (https://www.securitylab.ru/news/512730.php). 05.10.2020).***

***

«Компанія McAfee, що спеціалізується на кібербезпеці, опублікувала рейтинг зірок, інформацію про яких потрібно шукати з особливою обережністю - велика ймовірність підхопити вірус. Очолила список акторка Анна Кендрік. Відзначається, що результати пошуку можуть привести її шанувальників на сайти, які потай заразять їх комп'ютери шкідливим ПЗ і вкрадуть їх особисту інформацію.

У списку також опинилися (від найбільш небезпечного до менш): Шон Комбс, Блейк Лайвлі, Мерайя Кері, Джастін Тімберлейк, Тейлор Свіфт, Джиммі Кіммел, Джулія Робертс, Кейт МакКіннон і Джейсон Деруло.

Особливо, йдеться в офіційній заяві, потрібно уникати піратського контенту і торрентів:

«Якщо нічого не підозрюючи користувач клацне на шкідливе посилання, коли буде шукати фільм зі знаменитістю, на його девайс можуть несподівано потрапити рекламні або шкідливі програми». ***(Джастін Тімберлейк і Блейк Лайвлі увійшли до списку найбільш небезпечних знаменитостей в Мережі // Новини шоу бізнесу (http://glianec.com/fishka/36437dzhastin-timberleik-i-bleik-laivli-uviishli-do-spisku-naibilsh-nebezpechnih-znamenitostei-v-merezhi.html). 20.10.2020).***

***

«Pingvin Pro вже піднімав на сайті питання небезпеки під'єднання до безкоштовного Wi-Fi у громадських місцях. Річ у тім, що шахраї мають способи за допомогою яких вони отримують ваші конфіденційні дані. Федеральне бюро розслідувань США повідомило про зростання таких кібератак.

У світлі останніх подій, багато людей перейшли на віддалену роботу та дистанційне навчання. При цьому, не всі використовують домашній Wi-Fi – дехто йде у кафе чи інші заклади з безкоштовним підключенням до Інтернету. Шахраям достатньо дізнатися назву точки доступу і створити свою з подібною назвою. В цьому випадку, розрахунок на тих користувачів, які неуважно вчитуються у назви і підключаться до шахрайської мережі. Далі зловмисник може отримати контроль над ноутбуком чи іншим ґаджетом жертви і робити, що заманеться. Зокрема, атакувати спамом, скерувати жертву на фішингові сторінки чи вкрасти конфіденційні дані.

Один з варіантів – уважно дивитися, до якої мережі ви підключаєтесь у громадських місцях. Проте, все ж краще уникнути цього і скористатися мобільним Інтернетом – буде безпечніше для пристрою та ваших даних». ***(Грицина Вікторія. Кількість атак через безкоштовний Wi-Fi зростає // Pingvin Pro (https://pingvin.pro/gadgets/news-gadgets/kilkist-atak-cherez-bezkoshtovnyj-wi-fi-zrostaye.html). 14.10.2020).***

***

«Корпорация Intcomex, базирующаяся в Майами (штат Флорида), подтвердила в опубликованном вчера интервью, что стала жертвой кибератаки, результатом которой стала масштабная утечка пользовательских данных.

Порядка терабайта информации о клиентах Intcomex, включающей паспортные данные, снимки водительских прав, сведения о кредитных карточках и т.п., были выложены на русскоязычном хакерском форуме в два захода — 14 и 20 сентября. Взломщики пообещали опубликовать ещё больше данных в будущем.

Intcomex заявила, что предприняла шаги для исправления ситуации, привлекла сторонних экспертов и внедрила дополнительные усиленные меры безопасности. Она также связалась с правоохранительными органами и, по

необходимости, уведомляет пострадавшие стороны». ***(Intcomex потеряла терабайт данных о клиентах // Компьютерное Обозрение (https://ko.com.ua/intcomex_i_barnes_noble_podtverdili_chto_stali_zhertvami_kiberatak_134890). 15.10.2020).***

***

«Как стало известно кибератаки ввергла в хаос сервисы одного из крупнейших американских книготорговцев, Barnes & Noble. Компания подтвердила возникшие проблемы.

Сообщается, что некоторые клиенты не могли получить доступ к своим библиотекам Nook, а их предыдущие покупки «растворялись в воздухе», другие не смогли войти на онлайн-платформу фирмы, серьёзные проблемы испытывались с отправкой или загрузкой новых книг.

Как отмечается, компания частично восстановила работоспособность своих систем во вторник, но лишь теперь признала факт кибератаки. В электронном письме сообщается, что 10 октября она стала жертвой вторжения, которое привело к «несанкционированному и незаконному доступу к определенным корпоративным системам Barnes & Noble».

Книготорговец не располагает доказательствами, но не исключает того, что в результате взлома достоянием хакеров стали адреса e-mail, адреса для выставления счетов и доставки, номера телефонов и истории транзакций клиентов Barnes & Noble». ***(Barnes & Noble подверглась кибератаке и потеряла информацию о клиентах // Компьютерное Обозрение (https://ko.com.ua/barnes_noble_podverglas_kiberatake_i_poteryala_informaciyu_o_klientah_134892). 16.10.2020).***

***

«Как сообщило в пятницу иранское информационное агентство, одной из целей крупных кибератак на два иранских правительственных учреждения на этой неделе была электронная инфраструктура портов страны.

Правительственная организация по информационным технологиям заявила в четверг о взломе двух учреждений, не сообщив других деталей. Крупные кибератаки произошли в понедельник и вторник. "Заклятые враги в течение некоторого времени пытались осуществить кибератаки", - цитирует полуофициальное информационное агентство "Tasnim" заявление Управления портов.

В заявлении сообщается, что были приняты меры сдерживания, чтобы не допустить прерывания "миссии организации". После кибератак несколько государственных органов временно отключили интернет-сервисы в качестве меры предосторожности». ***(Целью кибератаки стали иранские порты // ISRAland Online (http://www.isra.com/news/251600). 16.10.2020).***

***

«Международная юридическая фирма Seyfarth Shaw объявила в понедельник, что в минувшие выходные стала жертвой атаки вымогателя.

Имея более 900 юристов в 17 офисах в Америке, Европе и Азиатско-Тихоокеанском регионе, компания получила более 700 миллионов долларов валового дохода в прошлом году, что поместило ее в нижнюю половину 100 самых прибыльных юридических фирм в мире.

Атака выходного дня

Инцидент произошел в субботу, и компания описала его как «изощренную и агрессивную атаку вредоносного ПО». Время типично для кибератак, в частности для программ-вымогателей, поскольку в компаниях работает меньше сотрудников по выходным.

В своем уведомлении об атаке Сейфарт Шоу говорит, что, насколько им известно, «этой же атакой одновременно были поражены несколько других сущностей».

Компания заявляет, что ее системы мониторинга зафиксировали несанкционированную деятельность, и ИТ-отдел быстро остановил распространение.

Эти шаги не помешали развертыванию процедуры шифрования файлов «во многих наших системах». В качестве меры предосторожности зашифрованные компьютеры были отключены…

Неясно, насколько разрушительна эта атака, но Сейфарт Шоу говорит, что они не нашли доказательств того, что злоумышленники получили доступ или украли данные клиентов или компании.

Сейфарт Шоу объявил, что их система электронной почты в настоящее время не работает, но телефонная система продолжает работать. Связаться с юридической фирмой через Интернет можно, заполнив контактную форму.

BleepingComputer обратился к Сейфарту Шоу за дополнительной информацией об атаке. Представитель компании ответил со своего личного адреса электронной почты, сказав, что в настоящее время у них нет никакой дополнительной информации.

Риск программ-вымогателей и кражи данных

Получив доступ к сети, операторы программ-вымогателей обычно тратят некоторое время на разведку и переходят к наиболее ценным машинам (серверам, резервным копиям).

С момента получения первоначального доступа до перехода к шифрованию компьютеров могут пройти недели. В этот период большинство злоумышленников крадут незашифрованные данные.

Информация часто используется как рычаг, чтобы заставить жертву заплатить выкуп под угрозой разглашения ее общественности. Эта тактика была впервые применена с программой-вымогателем Maze в ноябре 2019 года, и ее применяют все больше и больше групп, работающих в сфере программ-вымогателей.

BleepingComputer известно о 19 бандах вымогателей, которые в настоящее время крадут данные своих жертв и угрожают опубликовать их, если их требования не будут выполнены.

Из них у 16 есть специальные сайты, рекламирующие украденные данные и предлагающие их бесплатно или устанавливающие аукционы для продажи их тому,

кто предложит самую высокую цену. Иногда они продают данные на форумах киберпреступников.

Показательный пример: в июне банда вымогателей REvil опубликовала сайт аукциона по продаже данных, украденных у известной юридической фирмы Grubman Shire Meiselas & Sacks (GSMLaw). Этот шаг был предпринят после того, как юридическая фирма отказалась выплатить выкуп в размере 42 миллионов долларов (первоначально 21 миллион долларов). До этого, в мае, просачивались какие-то документы, связанные с клиентами компании». ***(Ionut Ilascu. International law firm Seyfarth discloses ransomware attack // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/international-law-firm-seyfarth-discloses-ransomware-attack/). 13.10.2020).***

***

«Фишинговые кампании начали использовать Basecamp как часть злонамеренных фишинговых кампаний, которые распространяют вредоносное ПО или воруют ваши учетные данные.

Basecamp - это веб-решение для управления проектами, которое позволяет людям сотрудничать, общаться друг с другом, создавать документы и обмениваться файлами

При создании документов они могут быть отформатированы с помощью HTML-ссылок, изображений и стилизованного текста. Basecamp также позволяет пользователям загружать в проект любые файлы, включая форматы файлов, которые обычно считаются небезопасными, такие как исполняемые файлы, файлы JavaScript и т. д.

Чтобы предоставить общий доступ к загруженным файлам, пользователи могут создать общедоступную ссылку, которая позволяет людям за пределами организации предварительно просмотреть файл и загрузить его.

Когда пользователи нажимают на эту ссылку [пример общего файла], они попадают на страницу с предварительным просмотром файла и другой ссылкой для загрузки файла на ваш компьютер.

Поскольку Basecamp предлагает бесплатную лицензию, пользователи получают бесплатный хостинг, который они могут использовать для распространения любого типа файлов по своему желанию.

Basecamp используется для распространения исполняемых файлов вредоносных программ

Исследователи безопасности MalwareHunterTeam и Джеймс обнаружили, что злоумышленники распространяют исполняемые файлы BazarLoader, используя общедоступные ссылки для скачивания Basecamp.

BazarLoader - это скрытый троян-бэкдор от банды TrickBot, который используется против важных целей для взлома их сетей. После установки BazarLoader развернет маяки Cobalt Strike, которые позволяют злоумышленникам получить доступ к сети и в конечном итоге развернуть программу-вымогатель Ryuk.

Злоупотребляя безопасными службами, такими как Basecamp, для размещения вредоносных файлов и фишинговых страниц, пользователи могут

впасть в ложное чувство доверия и открывать файлы, которые обычно не открываются.

Кроме того, используя URL-адреса Basecamp, злоумышленники могут создавать тщательно продуманные и целевые кампании для проникновения в сеть, поскольку пользователи могут почувствовать, что файл принадлежит их проекту Basecamp.

В связи с этим важно, чтобы все относились ко всем общим ссылкам или загрузкам как к подозрительным, независимо от их происхождения.

На этой неделе исследователь безопасности Уилл Томас обнаружил, что злоумышленники также злоупотребляют Basecamp в рамках фишинговых кампаний.

В отчете компании Cyjax, занимающейся кибербезопасностью, Томас объясняет, что фишинговые кампании теперь используют Basecamp для размещения промежуточных страниц, которые перенаправляют пользователей на фишинговые целевые страницы.

Поскольку Basecamp считается надежным сервисом, он позволяет злоумышленникам создавать страницы, которые обходят решения безопасности, которые являются безопасным трафиком.

«Этот метод эффективен, потому что хостинг Basecamp и Google Cloud часто используется для бизнес-операций и по умолчанию считается безопасным большинством систем обнаружения. Облачные платформы также сохраняют анонимность своих пользователей и могут быть настроены в кратчайшие сроки. Они «Человеческим аналитикам SOC трудно распознать угрозу, потому что трафик к этим службам и от них кажется законным», - поясняет Томас в своем отчете.

Например, Томас обнаружил недавнюю фишинговую кампанию, в которой общий документ Basecamp использовался для перенаправления на фишинговую фишинговую страницу учетных данных Office 365.

В дополнение к решениям безопасности, рассматривающим референт как «безопасный» трафик, преимуществом использования Basecamp для промежуточных страниц является то, что их можно редактировать по мере необходимости.

Предположим, фишинговая целевая страница отключена. В этом случае злоумышленники могут просто войти в Basecamp и изменить свою промежуточную страницу, чтобы перенаправить на другую страницу для кражи учетных данных.

Эта способность позволяет злоумышленникам поддерживать кампанию даже после удаления их фишинговых страниц». ***(Lawrence Abrams. Hackers now abuse BaseCamp for free malware hosting // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/hackers-now-abuse-basecamp-for-free-malware-hosting/). 17.10.2020).***

***

«Amazon, Apple, Netflix, Facebook и WhatsApp - ведущие бренды, которых киберпреступники используют для фишинговых и мошеннических атак, включая недавнюю атаку на полмиллиона пользователей Facebook.

До сих пор в этом году Facebook был одним из основных фишинговых атак киберпреступников, а недавнее исследование пролило свет на 4,5 миллиона попыток фишинга с использованием платформы социальных сетей в период с апреля по сентябрь 2020 года.

После Facebook приложение для обмена сообщениями WhatsApp является второй по величине платформой, которую используют злоумышленники (с 3,7 млн попыток фишинга), за ним следуют Amazon (3,3 млн попыток), Apple (3,1 млн попыток) и Netflix (2,7 млн попыток).

Согласно анализу, опубликованному Kaspersky во вторник, предложения Google (включая YouTube, Gmail и Google Drive) заняли шестую позицию с 1,5 миллионами попыток фишинга в целом.

Следует отметить, что многие из этих целевых веб-сервисов также часто используются сотрудниками малого и среднего бизнеса во время работы, что потенциально создает риски для конфиденциальных корпоративных данных, предупреждают исследователи.

«Мы не можем представить нашу повседневную жизнь и работу без различных веб-сервисов, включая социальные сети, приложения для обмена сообщениями и платформы для обмена файлами», - заявила Татьяна Сидорина, эксперт по безопасности Kaspersky. «Однако для любой организации важно понимать, откуда могут исходить угрозы, и какие технологии и меры по повышению осведомленности необходимы для их предотвращения. Компаниям также необходимо обеспечить своим сотрудникам комфортное использование необходимых им услуг, поэтому крайне важно соблюдать баланс».

Невероятная база пользователей Facebook - более 2,7 миллиардов активных пользователей в месяц по состоянию на второй квартал 2020 года - делает его привлекательным брендом для киберпреступников. Доступ гиганта социальных сетей к множеству частных данных, таких как личные сообщения, - еще одна причина, по которой злоумышленники используют Facebook.

Фактически, только на этой неделе отчет пролил свет на фишинговую кампанию Facebook, жертвами которой стали не менее 450 000 человек. Атака отправила пользователям Facebook ссылку через Messenger, которая, по всей видимости, была видео на YouTube. Однако, когда жертвы нажимали на ссылку, они перенаправлялись на несколько веб-сайтов и в конечном итоге попадали на фишинговую страницу Facebook. Затем злоумышленники смогли получить учетные данные жертв в Facebook.

Предыдущие киберпреступники также на протяжении многих лет нацеливались на Facebook с помощью новой хитрой тактики, включая воспроизведение запроса входа в социальную сеть в «очень реалистичном формате» внутри блока HTML и нацеливание на рекламную платформу Facebook в течение многих лет в ходе атаки, которая выкачала 4 миллиона долларов из рекламы пользователей. учетные записи.

Facebook также является одним из наиболее часто используемых корпоративными служащими сервисов: «Лаборатория Касперского» обнаружила, что YouTube и Facebook являются двумя основными сервисами, к которым

сотрудники малого и среднего бизнеса получают доступ на своих корпоративных устройствах (за ними следуют Google Drive, Gmail и WhatsApp).

«Учитывая, что в двух списках используются многие службы, эти результаты только подтверждают тенденцию, согласно которой популярные приложения становятся ценными платформами для злонамеренных действий мошенников», - считают исследователи.

С другой стороны, платформа социальных сетей также является популярным приложением, заблокированным корпоративными компаниями. Другие популярные заблокированные приложения включают Twitter, Pinterest, Instagram и LinkedIn.

Исследователи также отметили, что мессенджеры, обмен файлами или почтовые службы обычно не блокируются, «вероятно, потому, что они часто используются в рабочих целях, а также для личных нужд». Эти продукты, включая сервисы Google (Gmail и Google Drive), по-прежнему часто используются киберпреступниками в целевых атаках.

Эта статистика, которая была получена за период с апреля по сентябрь с использованием распределенной антивирусной сети Kaspersky (Kaspersky Security Network или KSN), состоит из обезличенных метаданных, которые добровольно предоставляются участниками KSN среди клиентов Kaspersky, сообщил Threatpost представитель пресс-службы.

Исследователи заявили, что в будущем компаниям следует следить за новыми популярными брендами, такими как приложение для коротких видео TikTok, с большими пользовательскими базами, к которым неизбежно будут стремиться мошенники для фишинговых атак и других вредоносных целей.

«Хотя организации могут иметь разные приоритеты и разрешения на то, какие веб-сервисы могут использоваться их сотрудниками, важно, чтобы организации понимали все соответствующие угрозы, с которыми они могут столкнуться, и то, как они могут проникнуть в корпоративные конечные точки», - считают исследователи. «Как только веб-сервис станет популярным, вполне вероятно, что он станет более привлекательной целью среди мошенников». ***(Lindsey O'Donnell. Facebook: A Top Launching Pad For Phishing Attacks // Threatpost (https://threatpost.com/facebook-launching-pad-phishing-attacks/160351/). 20.10.2020).***

***

«Злоумышленники нацелены на пользователей Microsoft Office 365 с помощью атаки на тему Coinbase, стремясь получить контроль над их почтовыми ящиками через OAuth.

Пользователи Office 365 получают электронные письма, якобы отправленные с криптовалютной платформы Coinbase, в которых им предлагается загрузить обновленные Условия использования через приложение для получения согласия OAuth. Но когда они соглашаются сделать это, пользователи неосознанно предоставляют злоумышленникам полный доступ к своей электронной почте.

OAuth - это открытый стандарт авторизации на основе токенов, который позволяет сторонним службам использовать информацию учетной записи

пользователя без раскрытия пароля. Например, вместо того, чтобы создавать новую учетную запись с нуля, пользователи могут решить войти на веб-сайт с помощью опции «Войти через Google» или «Войти через Facebook».

Однако эта функция, которая закрывает почтовые ящики жертв, также привлекла киберпреступников, которые используют OAuth для получения разрешений с помощью вредоносных сторонних приложений. Эти типы атак «согласия» не новы, но эта тактика набирает силу, как видно из этого конкретного инцидента, говорят исследователи в анализе.

«Мы наблюдаем атаки на основе приложений согласия с начала этого года, - сказал Стю Сьюверман, генеральный директор KnowBe4, во вторник. «Пользователи должны быть обучены с помощью тренинга по вопросам безопасности, что им следует искать подобные атаки и предоставлять доступ только законным издателям приложений (например, Outlook для мобильных устройств)».

В этой конкретной атаке пользователи получают электронное письмо, имитирующее Coinbase, платформу, позволяющую пользователям покупать и продавать криптовалюту, такую как биткойн. У него 35 миллионов пользователей, что составляет значительную целевую аудиторию для злоумышленников. В электронном письме также содержится просьба к пользователям обновить свои Условия использования. Здесь злоумышленники делают ставку на то, что нацелены на пользователей Office 365, которые также являются пользователями Coinbase, говорят исследователи.

По словам исследователей, после нажатия ссылки в электронном письме для ознакомления с новыми Условиями использования пользователи попадают на законную страницу входа в Office 365.

Затем им предоставляется запрос согласия OAuth для доступа на чтение и запись к их почтовым ящикам, электронным письмам, профилям и другой информации, с указанием «coinbaseterms.app» в качестве отправителя запроса, что соответствует уловке, что запрос поступает от Coinbase как часть обновленных Условий обслуживания.

Если пользователи Office 365 попадают на эту уловку и нажимают «да», они невольно предоставляют злоумышленникам доступ к своим почтовым ящикам, позволяя им просматривать конфиденциальные данные, использовать свою электронную почту для последующих фишинговых или целевых фишинговых атак и других злонамеренных целей.

«После предоставления доступа приложение теперь имеет доступ для чтения электронной почты жертвы, удаления сообщений и многого другого», - заявили исследователи. «Единственный способ закрыть доступ - административно».

Microsoft ранее предупреждала о рискованных приложениях OAuth, в июле предупреждая, что повсеместная удаленная работа и более широкое использование приложений для совместной работы побуждают злоумышленников наращивать атаки на основе приложений, использующие OAuth.

«Когда пользователи устанавливают эти приложения, они часто нажимают кнопку «Принять», не просматривая подробности в приглашении, включая предоставление разрешений приложению», - говорится в предыдущем сообщении

Microsoft. «Принятие разрешений сторонних приложений представляет собой потенциальную угрозу безопасности вашей организации».

В сентябре APT, известный как TA2552, был обнаружен с использованием OAuth или других методов авторизации на основе токенов для доступа к учетным записям Office 365 с целью кражи контактов и почты пользователей.

В другом инциденте, раскрытом в октябре, медицинское исследовательское подразделение в университете было атаковано фишинговой приманкой, которая продвигала бесплатное приложение для оптимизации календаря и управления временем. После того, как один человек заглотил наживку и установил вредоносное приложение OAuth, злоумышленники получили полный доступ к Office 365 и использовали его для отправки внутренних фишинговых писем, используя надежные идентификаторы и средства связи для дальнейшего распространения внутри университета.

Microsoft, со своей стороны, рекомендует пользователям исследовать любые приложения OAuth, используя возможности и информацию, предоставленные на портале Cloud App Security (предложение Microsoft по безопасности для своих облачных приложений), чтобы отфильтровать приложения с низкой вероятностью быть опасными и сосредоточиться на подозрительных. Программы. Технический гигант также предупредил пользователей, что следует внимательно следить за следующими признаками опасного приложения OAuth:

Чем реже используется приложение, тем меньше вероятность, что оно будет безопасным.

Приложение должно требовать только тех разрешений, которые связаны с его назначением. Если это не так, приложение потенциально может быть рискованным.

Приложения, требующие высоких привилегий или согласия администратора, более рискованны.

Threatpost обратился к Microsoft и Coinbase за дальнейшими комментариями по поводу этого инцидента». ***(Lindsey O'Donnell. Office 365 OAuth Attack Targets Coinbase Users // Threatpost (https://threatpost.com/office-365-oauth-attack-coinbase/160337/). 20.10.2020).***

***

«Мошенники BEC теперь имеют базы операций по крайней мере в 39 округах и несут ответственность за ежегодные убытки в размере 26 миллиардов долларов, и этот показатель продолжает расти.

Исследование более 9000 случаев атак компрометации деловой электронной почты (BEC) по всему миру показывает, что их число резко возросло за последний год, и что афера с социальной инженерией вышла далеко за пределы своих исторических корней в Нигерии.

В отчете отдела кибербразведки Agari (ACID), озаглавленном «Глобальный охват компрометацией деловой электронной почты», было обнаружено, что эти атаки обходятся предприятиям в 26 миллиардов долларов ежегодно. И эта тенденция, похоже, усиливается. Фактически, исследователи обнаружили, что атаки BEC в настоящее время составляют целых 40 процентов потерь от киберпреступлений во всем мире, затрагивая как минимум 177 стран.

Для контекста рабочая группа по борьбе с фишингом недавно обнаружила, что средний банковский перевод при мошенничестве с BEC составляет около 80 000 долларов.

За пределами Нигерии

При атаке BEC мошенник выдает себя за руководителя компании или другую доверенную сторону и пытается обманом заставить сотрудника, ответственного за платежи или другие финансовые операции, перевести деньги на поддельный счет. Злоумышленники обычно проводят изрядное количество разведывательных работ, изучая стили руководителей и выявляя поставщиков организации, методы биллинговой системы и другую информацию, чтобы помочь провести убедительную атаку.

Это началось как эволюция приманок старой школы, которые использовались нигерийскими кибергангами, чтобы обманом заставить людей давать им деньги: фальшивые принцы, обещание найти настоящую любовь или даже концерты на дому, которые звучат слишком хорошо, чтобы быть правдой.

«Большинство опытных актеров связаны с Нигерией», - говорится в отчете. «В конце концов, именно здесь BEC впервые приобрела всемирную известность еще в 2015 году, когда мошенники по электронной почте впервые начали обманывать организации, выдавая себя за их генеральных директоров и финансовых директоров в мошеннических электронных сообщениях, нацеленных на сотрудников».

Растущая отдача от этих преступлений привела к периоду инноваций, согласно отчету, который выявил новую «разновидность» атаки, называемую компрометацией электронной почты поставщика, которую Агари приписывает преступной организации Silent Starling, расположенной в Западной Африке.

При атаке VEC мошенники сначала взламывают учетные записи, принадлежащие сотрудникам поставщиков, а затем нацеливаются на клиентов поставщиков, выдавая себя за владельца скомпрометированной учетной записи и прося клиентов перевести деньги «поставщику», который на самом деле является учетной записью мула..

Между тем, эти типы атак стали более мощными и их труднее остановить, в основном потому, что эти операции получили распространение по всему миру, выходя за рамки их нигерийских корней.

Больше денег, больше атак BEC

Информация, полученная Agari при анализе 9000 оборонительных боев в период с мая 2019 года по июль 2020 года, показала, что только половина исследованных случаев возникла в Нигерии. Репрессии со стороны правоохранительных органов заставили этих мошенников повсюду, а растущие доходы вовлекают в драку другие преступные группировки, а это означает, что базы для операций от этих мошенников могут исходить откуда угодно.

Вместо этого исследователи обнаружили, что 25% этих атак были совершены в США, в частности, в штатах Калифорния, Флорида, Джорджия, Нью-Йорк и Техас. Не случайно, что это те же самые штаты, которые стали объектом репрессий BEC Министерства юстиции США.

10 сентября Министерство юстиции объявило, что по всему миру был произведен 281 арест в рамках операции «ReWired», и подробно описало, где следователи обнаружили мошенников из США, в том числе в городских районах Атланты, Чикаго, Далласа и Майами.

Денежные мулы BEC

Возможно, наиболее важным аспектом любой аферы с бандами BEC является роль «денежного мула». Эти люди, сознательно или невольно, выполняют за них грязную работу мошенников, например открывают банковские счета и переводят деньги. В качестве еще одного доказательства растущего глобального присутствия BEC, Агари определила мулов, разбросанных по 39 странам.

Тем не менее, большинство этих аккаунтов мулов находится в США (80 процентов) и сгруппированы во многих из тех же городских районов, что и сами мошенники, но, как добавлено в отчете, эти аккаунты были обнаружены в каждом штате и округе Колумбия.

Интересно, что они также заметили, что суммы депозитов на мул-счетах в США были значительно меньше, чем в других странах. В отчете говорится, что из 2 900 проанализированных аккаунтов мулов средняя сумма, запрошенная американскими мошенниками, составила 39 500 долларов, что составляет лишь небольшую часть того, что запрашивали в других точках мира. Для сравнения, в Гонконге средняя сумма электронного перевода составляла 257 300 долларов.

«Субъекты BEC теперь можно найти в 50 странах, и хотя половина из них все еще имеет базовую базу в Нигерии, географическое распределение этих субъектов угроз намного выше, чем было всего несколько лет назад», - говорится в отчете. «Это свидетельствует о том, что киберпреступные организации здоровы, растут, становятся более диверсифицированными и не демонстрируют никаких признаков слабости». ***(Becky Bracken. BEC Attacks: Nigeria No Longer the Epicenter as Losses Top $26B // Threatpost (https://threatpost.com/bec-attacks-nigeria-losses-snowball/160118/). 14.10.2020).***

***

«Исследователи безопасности в Check Point провели исследование по всему миру, которое показало, что среднесуточное количество атак вымогателей выросло на 50% за последние 3 месяца по сравнению с первой половиной 2020 года. Россия входит в первую пятерку стран по количеству атак с использованием таких программ.

Используя базу данных для анализа угроз Threat Cloud, исследователи Check Point проанализировали ряд аналитических данных и наблюдений, которые касаются последних мировых тенденций в области программ-вымогателей.

Ключевые выводы

Среднесуточное количество атак вымогателей за последние 3 месяца подскочило на 50% по сравнению с 1-й половиной 2020 года.

Программа-вымогатель Ryuk теперь атакует 20 организаций в неделю.

Россия занимает 4 место в топ-5 стран по количеству атак с использованием программ-вымогателей за последние 3 месяца

Топ-5 стран по количеству атак с использованием программ-вымогателей за последние 3 месяца:

США (рост на 98,1%)

Индия (рост на 39,2%)

Шри-Ланка (рост на 436%)

Россия (рост на 57,9%)

Турция (рост на 32,5%)

Топ-5 отраслей в мире, которые пострадали от угроз вымогателей за последние 3 месяца сильнее всего:

Коммуникации, связь

Образование и исследования

Правительство и военные

Поставщики программного обеспечения

Коммунальные услуги

Самыми популярными программами-вымогателями за последние 3 месяца стали Maze и Ryuk.

Лотем Финкельстин, ведущий эксперт по анализу угроз Check Point: «Атаки с использованием программ-вымогателей бьют рекорды в 2020 году. Их рост подтолкнула пандемия коронавируса, когда организации пытались наладить удаленную работу, оставляя значительные пробелы в своих ИТ-системах. Однако резкий всплеск вымогателей наблюдается только в последние три месяца. Естественный вопрос: почему именно сейчас? Я думаю, что основными факторами могут быть:

Более изощренные атаки, такие как двойное вымогательство. В этом типе атак хакеры сначала извлекают и шифруют большие объемы конфиденциальной информации жертвы. После этого злоумышленники угрожают опубликовать эту информацию, если не будет выплачен выкуп. Это оказывает значительное давление на организации, чтобы они подчинились требованиям.

Готовность платить. Хакеры сознательно устанавливают такой размер выкупа, который жертвы будут готовы выплатить. Таким образом, большинство пострадавших от программ-вымогателей предпочитают просто заплатить, чтобы потом не мучиться и не тратить свое время на восстановление ИТ-систем. Кроме того, сейчас жертвы платят охотнее, чем обычно, чтобы избежать дополнительного стресса — учитывая сложные коронавирусные времена. Хотя это может измениться, когда пандемия закончится. Но, к сожалению, выплата выкупа создает порочный круг: чем больше «успешных» атак такого типа, тем чаще они происходят.

Возвращение Emotet открывает новые возможности. После пятимесячного отсутствия Emotet снова занял 1-е место в рейтинге самых распространенных вредоносных программ, затронув 5% организаций во всем мире. Emotet — продвинутый самораспространяющийся модульный троян. Изначально он был банковским трояном, но в последнее время он использовался в качестве распространителя других вредоносных программ. Операторы Emotet продают информацию о своих зараженных жертвах другим распространителям программ-вымогателей, и, поскольку они уже заражены, эти жертвы уязвимы для новых атак.

Это делает атаки вымогателей еще более эффективными для злоумышленников, поскольку большее количество зараженных устройств означает большее количество возможностей для атак.

К сожалению, я подозреваю, что с наступлением нового года ситуация с программами-вымогателями станет только хуже. Я настоятельно призываю организации во всем мире проявлять особую бдительность». ***(За последние 3 месяца количество атак вымогателей в России возросло почти на 58% // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5696414-Za-poslednie-3-mesyacza-kolichestvo.html). 12.10.2020).***

***

«Управление финансовых услуг штата Нью-Йорк (New York Department of Financial Services) представило отчет по результатам расследования взлома Twitter, имевшего место в июле нынешнего года. Согласно отчету, на осуществление взлома у киберпреступников ушло 24 часа.

Как установило следствие, атака началась 14 июля и закончилась на следующий день, когда стало очевидно, что учетные записи целого ряда публичных личностей, в том числе политиков и основателей крупных компаний, были взломаны хакерами в мошеннических целях.

Злоумышленники, идентифицированные вскоре после инцидента, воспользовались доступом к внутренней сети Twitter для изменения электронных адресов и учетных данных интересующих их пользователей и захвата контроля над их аккаунтами. В общей сложности хакеры пытались атаковать 130 учетных записей, и у 45 из них были изменены пароли.

Спустя несколько недель после инцидента администрация Twitter сообщила, что в ходе атаки злоумышленники связались с сотрудниками компании по телефону и обманом получили доступ к нужным внутренним инструментам поддержки. По данным Управления финансовых услуг штата Нью-Йорк, с момента телефонного звонка до взлома прошли почти сутки.

Атаку предположительно осуществили 17-летний житель Флориды Грэм Айвен Кларк (Graham Ivan Clark), он же Kirk#5270, 19-летний британец Мэйсон Джон Шепперд (Mason John Sheppard), известный как Chaewon, и 22-летний житель Флориды Нима Фазели (Nima Fazeli), также известный как Rolex.

14 июля после обеда злоумышленники позвонили нескольким сотрудникам Twitter и, представившись сотрудниками IT-отдела, сообщили о проблемах с VPN (весьма распространенная проблема, учитывая количество сотрудников, работающих удаленно). Затем они попросили сотрудников ввести свои учетные данные в форму на фишинговой странице.

Каких-либо свидетельств того, что сотрудники намеренно помогли хакерам, следствие не обнаружило. С помощью персональной информации сотрудников злоумышленникам удалось убедить их, что они действительно те, за кого себя выдают. Хотя некоторые сотрудники все-таки сообщили о подозрительном звонке во внутренний отдел Twitter по борьбе с мошенничеством, по крайней мере одна жертва попалась на удочку.

Хотя у первой жертвы не было доступа к интересующим хакеров внутренним системам, они воспользовались ее учетными данными для перемещения по сети и поиска сотрудников, у которых такой доступ был. 15 июля злоумышленники атаковали этих сотрудников, в том числе ответственных за рассмотрение деликатных глобальных юридических запросов.

Вскоре после того, как атакующие получили контроль над учетными записями Twitter (в том числе учетными записями OG – «original gangster»), они начали обсуждать продажу имен пользователей OG и демонстрировать наличие у себя доступа ко внутренним системам Twitter.

Затем киберпреступники переключились на подтвержденные учетные записи с целью придать убедительность своей мошеннической схеме с криптовалютой. В течение нескольких часов они атаковали учетные записи криптовалютного трейдера AngeloBTC, криптовалютной биржи Binance и еще десяти связанных с криптовалютой аккаунтов, в том числе Coinbase, Gemini Trust Company и Square.

Еще через несколько часов хакеры стали публиковать твиты со взломанных учетных записей, в том числе Apple, Uber, Билла Гейтса, Илона Маска, Канье Уэста, Флойда Мэйвезера, Ким Кардашьян и пр. В результате им удалось похитить $118 тыс. в биткойнах.

Как установило Управление финансовых услуг штата Нью-Йорк, в результате инцидента были скомпрометированы непубличные данные некоторых пользователей, и Twitter своевременно не обновляла информацию об инциденте». ***(На взлом Twitter у хакеров ушло 24 часа // SecurityLab.ru (https://www.securitylab.ru/news/513130.php). 16.10.2020).***

***

«Операторы вымогательского ПО начали активно обращаться к подпольным продавцам доступа к корпоративным сетям с целью избежать трудностей в процессе кибератак. Команда специалистов Accenture Cyber Threat Intelligence опубликовала результаты исследований новых тенденций в области кибербезопасности, рассказав о характере отношений между операторами программ-вымогателей и продавцами эксплоитов.

Во время атак операторы программ-вымогателей должны сначала найти точку входа в сеть. Взломанные учетные записи сотрудников, неправильная конфигурация в общедоступных системах и уязвимые конечные точки могут использоваться для развертывания вредоносного кода, что приводит к шифрованию файлов, дисков и требованию оплаты в обмен на ключ дешифрования.

По словам экспертов, приобретение точек доступа к сети и уже проверенные способы проникновения в целевую систему становятся все популярнее, включая покупку украденных учетных данных и эксплоитов. Продавцы доступа к сети обычно сначала обнаруживают уязвимость, а затем продают необходимую хакерам информацию на подпольных форумах по цене от $300 до $10 тыс.

«Успешная атака программ-вымогателей зависит от разработки и поддержания стабильного доступа к сети, который сопряжен с более высоким риском обнаружения и требует времени и усилий. Продавцы доступа заполняют эту нишу рынка для групп программ-вымогателей», — пояснили специалисты.

Эксперты из Accenture выявили более 25 продавцов постоянного доступа к сети. Многие из продавцов активны на одних и тех же подпольных форумах, популярных среди таких группировок, как Maze, NetWalker, Sodinokibi, Lockbit, Avaddon и пр». ***(Операторы вымогательского ПО покупают доступ к сетям в даркнете // SecurityLab.ru (https://www.securitylab.ru/news/512961.php). 13.10.2020).***

***

«Десятки сайтів пенсійних об'єднань, районних управ і бізнес-компаній у Франції зазнали хакерських атак

Атаки здійснили в ніч на вівторок, 27 жовтня…

На сайтах з'явилися гасла, що закликають до перемоги ісламу і пророка Мохаммеда і смерті Франції, а також зображення президента країни Емманюель Макрона у вигляді свині.

Французькі експерти з кібербезпеки були ще в неділю попереджені про хвилі кібернападів, багато в чому повторюють кібератаки 2015 року, коли ними супроводжувалися ісламістські теракти.

Приводом для атаки стали висловлювання Макрона про вбивство 47-річного вчителя Самюеля Паті, показав на уроці карикатури на пророка. Макрон назвав загиблого викладача "тихим героєм", убитим боягузами, оскільки він втілював собою республіку.

"Самюель Паті був убитий, тому що ісламісти хочуть забрати у нас майбутнє і знають, що це не вийде зробити з такими тихими героями, як він", - підкреслив президент.

Нагадаємо, 24 жовтня президент Туреччини Реджеп Таїп Ердоган заявив, що Макрону потрібно "лікувати психіку" через політику президента Франції щодо мусульманської меншини.

Після цього Франція відкликала свого посла в Туреччині для консультацій.

Глава європейської дипломатії Жозеп Боррель розкритикував президента Туреччини, назвавши його висловлювання неприйнятними». ***(Макрон у вигляді свині: у Франції ісламісти атакували десятки сайтів // Espreso.tv (https://espreso.tv/news/2020/10/27/u_franciyi_islamisty_atakuvaly_desyatky_saytiv). 27.10.2020).***

***

«Неизвестные хакеры вывели из строя сайт предвыборной кампании Дональда Трампа. По словам его окружения, на сайте не было конфиденциальных данных, которые могли бы быть похищены.

Неизвестные хакеры взломали сайт предвыборного штаба президента США Дональда Трампа. Об этом во вторник, 27 октября, сообщил в соцсети Twitter пресс-секретарь кампании Трампа Тим Мертоу.

"Ранее этим вечером сайт кампании Трампа был взломан, и мы с правоохранительными органами работаем над расследованием, которое приведет нас к источнику атаки", - написал Мертоу. По его словам, злоумышленники не

получили доступ к конфиденциальным данным, потому что на "сайте они не хранятся". Позже работа домашней страницы была восстановлена.

В последние недели американские власти неоднократно сообщали о кибератаках на американские госучреждения. В частности, Агентство по кибербезопасности и обеспечению защиты инфраструктуры США обвинило в них группу хакеров, действующую под именем "Energetic Bear" и "Dragonfly". Аналитики считают, что она действует в интересах российских властей…» ***(Дмитрий Вачедин. Хакеры атаковали сайт штаба Трампа // Deutsche Welle (https://www.dw.com/ru/hakery-atakovali-sajt-kampanii-trampa/a-55416853). 28.10.2020).***

***

«Всего за двенадцать календарных месяцев на горячую линию 119 было получено около десяти тысяч звонков от физических и юридических лиц, заявивших о том, что они стали жертвами кибернетических злоумышленников.

Как сообщает Национальное управление кибербезопасности, сообщения, полученные за период с сентября 2019 года по сентябрь 2020 года, касались взлома учетных записей в социальных сетях, домашних маршрутизаторов и камер, частных ящиков электронной почты и др. Около трех тысяч звонков касались взлома учетных записей в «WhatsApp».

Недавно управление запустило новую кампанию, в рамках которой пользователи могут получить полезную информацию о том, как быстро и эффективно защитить свои учетные записи в «Facebook», «Instagram» и «WhatsApp». Потратив несколько минут, можно узнать, как усложнить задачу хакерам». ***(Насколько часто израильтяне страдают от кибератак? // ISRAland Online Ltd (http://www.isra.com/news/251938). 26.10.2020).***

***

«Несколько бизнесменов, играющих заметные роли в криптовалютной отрасли, подверглись атакам через «систему сигнализации №7»: злоумышленники смогли перенаправить звонки и SMS-сообщения другому провайдеру. Кибератаки через «систему сигнализации №7» в последние годы участились, но их выполнение требует высокого уровня подготовки.

Сигнал семь

Неизвестные киберзлоумышленники воспользовались системой ОКС-7 (SS7), объединяющей мобильные сети всего мира, и с ее помощью получили доступ к аккаунтам в Telegram и почтовым ящикам нескольких крупных игроков на рынке криптовалют.

Система сигнализации №7, или ОКС-7 (общий канал сигнализации № 7) — это набор сигнальных телефонных протоколов, используемых для настройки большей части телефонных станций по всему миру на основе сетей с канальным разделением по времени. В основе ОКС-7 лежит использование аналоговых или цифровых каналов для передачи данных и соответствующей управляющей информации.

Злоумышленникам удалось перехватить коды двухфакторной авторизации, которые прошли через систему SMS мобильного оператора жертвы. Как поясняется в материале Bleeping Computer, злоумышленники могут перехватывать текстовые сообщения и звонки, подменяя местоположение оператора жертвы — так, будто она перешла в роуминг.

Атака состоялась 20 сентября 2020 г. Ее объектами стали как минимум двадцать клиентов сотовой компании Partner Communications Company (ранее известной как Orange Israel). Все они вовлечены в крупные проекты, связанные с криптовалютами. По словам Цахи Ганота (Tscahi Ganot), эксперта компании Pandora Security, который занимался расследованием, все указывает, что атака была произведена именно через SS7.

Работали профессионалы

По мнению Ганота, хакеры, вероятно, скомпрометировали систему отправки коротких сообщений (short message service center — SMSC) неназванного мобильного оператора, который направил в сети Partner запросы на смену локации (и сети) для номеров жертв. Запрос сводился к тому, чтобы Partner перенаправлял все звонки и SMS-сообщения, предназначенные для жертв атаки, в скомпрометированный мобильный центр коммутации (MCS).

По-видимому, злоумышленники обладали большим количеством информации о своих жертвах и их телефонах. Им были известны идентификаторы MSISDN (Mobile Station International Subscriber Directory Number) и IMSI (International Mobile Subscriber Identity) и даже некоторые пароли. При этом их цель была совершенно приземленной: добраться до криптовалютных кошельков.

«Атаки через ОКС-7 требуют обширных знаний об архитектуре мобильных сетей, того, как они обмениваются данными и каким образом производится маршрутизация данных, — говорит Дмитрий Кирюхин, эксперт по информационной безопасности компании SEC Consult Services. — В последние годы они участились, но остаются пока что “привилегией” профессионалов в сфере киберкриминала. На то же указывает тщательный сбор данных о жертвах, предшествовавший атакам. В принципе, часть этих данных могла быть использована для столь же эффективных, но менее затратных атак».

По словам Ганота, часть почтовых аккаунтов, которые удалось скомпрометировать злоумышленникам, являлись резервами для других почтовых ящиков, в которых содержались более критичные для бизнеса жертв сведения.

«В некоторых случаях хакеры выдавали себя за своих жертв в переписке через Telegram, и обращались к их знакомым с просьбами сконвертировать BTC (биткоины) в ETC (Ethereum, другая криптовалюта) и т. д.», — отметил Ганот, добавив, что как раз это и оказалось самым слабым местом во всей операции, поскольку операторы криптовалют хорошо знают, что обычно ничего хорошего за такими запросами не стоит.

«Насколько мы знаем, никто не поддался», — заметил исследователь. По словам Ганота, двухфакторная авторизация через SMS или звонки сегодня уже не считается надежным методом защиты пользовательских данных. Существуют куда более надежные средства, в том числе специализированные приложения и

физические ключи. Но многие сервисы продолжают полагаться именно на традиционную двухфакторную авторизацию.

Ганот также заметил, что телеком-операторам давно бы следовало уже перейти на более современные протоколы соединений, нежели ОКС-7. Эта система была разработана еще в 1975 г. для фиксированных линий и многих современных проблем она решить не может по определению. Любопытно, что в расследование данного инцидента были вовлечены также представители Национальной разведывательной службы Израиля («Моссада») и Национального управления по кибербезопасности этого государства». ***(Роман Георгиев. Хакеры взломали Telegram, чтобы обчистить криптокошельки крупных бизнесменов // CNews (https://safe.cnews.ru/news/top/2020-10-21_hakery_vzlomali_telegramchtoby). 21.10.2020).***

***

«Многонациональная энергетическая компания Enel Group во второй раз в этом году подверглась атаке программ-вымогателей. На этот раз Netwalker просит выкуп в размере 14 миллионов долларов за ключ дешифрования и не раскрывать несколько терабайт украденных данных.

Enel - один из крупнейших игроков в европейском энергетическом секторе с более чем 61 миллионом клиентов в 40 странах. По состоянию на 10 августа компания занимает 87-е место в рейтинге Fortune Global 500 с выручкой почти 90 миллиардов долларов в 2019 году.

Enel ударил по Netwalker Ransomware

В начале июня внутренняя сеть Enel была атакована программой-вымогателем Snake, также известной как EKANS, но эта попытка была обнаружена до того, как вредоносная программа могла распространиться.

19 октября исследователь поделился с BleepingComputer запиской о выкупе Netwalker, которая, по всей видимости, возникла в результате атаки на Enel Group.

В записке о выкупе была ссылка на URL http://prnt.sc/, который показывал данные, украденные в результате атаки. По именам сотрудников в папках было установлено, что атака была направлена на Enel Group.

На прошлой неделе BleepingComputer отправила в группу Enel письмо по поводу атаки, но ответа так и не получила.

Несколько дней спустя Netwalker подтвердил, что жертвой была группа Enel, после того как они добавили сообщение в свой чат поддержки, в котором говорилось: «Привет, Enel. Не бойтесь писать нам».

Обычно, если компания никоим образом не привлекает оператора выкупа, через некоторое время выкуп удваивается. Похоже, что то же самое произошло и с Enel, поскольку в приватном чате, предоставленном злоумышленником, нет разговоров с компанией.

Злоумышленник использовал этот канал, чтобы объявить, что он предпримет первый шаг к утечке украденных данных. Это означает публикацию доказательств того, что у них есть товары, и попытка заставить компанию выплатить выкуп, который сейчас составляет 14 миллионов долларов (1234,02380000 BTC).

Сегодня банда вымогателей Netwalker добавила Enel Group на свой сайт утечки данных и поделилась снимками экрана с незашифрованными файлами компании во время кибератаки в этом месяце.

По данным Netwalker, они украли у Enel около 5 терабайт данных и готовы обнародовать их часть в течение недели. Они также заявили, что «проанализируют каждый файл на предмет интересных вещей» и опубликуют его на своем сайте утечки.

Эта тактика предназначена для усиления давления и принуждения компании-жертвы к выплате. Во многих случаях это работает на пользу злоумышленнику». ***(Ionut Ilascu. Enel Group hit by ransomware again, Netwalker demands $14 million // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/). 27.10.2020).***

***

«Гигант офисной мебели Steelcase пострадал от атаки программ-вымогателей, которые вынудили их отключить свою сеть, чтобы сдержать распространение атаки.

Steelcase - крупнейший в мире производитель офисной мебели с 13000 сотрудников и 3,7 миллиарда долларов в 2020 году.

Steelcase подвергается атаке программы-вымогателя Ryuk

В форме 8-K, поданной в Комиссию по ценным бумагам и биржам (SEC), Steelcase сообщил, что они стали жертвой кибератаки 22 октября 2020 года.

22 октября 2020 года Steelcase Inc. («Компания») обнаружила кибератаку на свои системы информационных технологий. Компания незамедлительно приняла ряд мер сдерживания для решения этой ситуации, включая временное отключение затронутых систем и связанных операций.

Компания активно занимается восстановлением поврежденных систем и возвращением к нормальному режиму работы. В настоящее время Компании не известно о потере данных из ее систем или любой другой потере активов в результате этой атаки. Хотя кибератаки могут быть непредсказуемыми, в настоящее время Компания не ожидает, что этот инцидент окажет существенное влияние на ее бизнес-операции или финансовые результаты.

BleepingComputer активно отслеживает эту атаку после того, как на прошлой неделе источник в индустрии кибербезопасности сообщил нам, что Steelcase подвергся атаке программы-вымогателя Ryuk.

Нам сказали, что устройства Steelcase были зашифрованы Рюком после того, как они впервые были атакованы той же группой, которая стояла за недавней атакой на Sopra Steria и Universal Health Services.

В этих атаках использовались заражения BazarLoader или TrickBot, которые в конечном итоге обеспечивали удаленный доступ злоумышленникам Ryuk Ransomware, которые затем скомпрометировали остальную сеть и развернули Ryuk.

Неизвестно, сколько устройств было зашифровано или пострадали ли бизнес-операции, кроме отключения сети.

BleepingComputer связался со Steelcase с дополнительными вопросами, но не получил ответа». ***(Lawrence Abrams. Steelcase furniture giant hit by Ryuk ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/steelcase-furniture-giant-hit-by-ryuk-ransomware-attack/). 27.10.2020).***

***

«Федеральное бюро расследований (ФБР) выпустило экстренное предупреждение о хакерах, крадущих данные из правительственных агентств США и корпоративных организаций через открытые в Интернете и небезопасные экземпляры SonarQube.

SonarQube - это платформа с открытым исходным кодом для автоматического аудита качества кода и статического анализа для обнаружения ошибок и уязвимостей в проектах с использованием 27 языков программирования.

Уязвимые серверы SonarQube активно эксплуатируются злоумышленниками с апреля 2020 года для получения доступа к репозиториям исходного кода данных, принадлежащих как государственным, так и корпоративным организациям, а затем их извлекают и публикуют.

У десятков компаний уже произошла утечка исходного кода

ФБР заявляет, что выявило несколько таких инцидентов, когда злоумышленники злоупотребляли уязвимостями конфигурации SonarQube с момента начала атак.

«Начиная с апреля 2020 года ФБР обнаружило утечки исходного кода, связанные с небезопасными экземплярами SonarQube, из правительственных агентств США и частных американских компаний в секторах технологий, финансов, розничной торговли, продуктов питания, электронной коммерции и производства», - говорится в сообщении ФБР в TLP: WHITE флэш-оповещение.

Несмотря на то, что ФБР не указывает на публичные сообщения о таких атаках, BleepingComputer сообщила в июле о том, что у десятков компаний был украден исходный код и просочился в сеть.

Разработчик и реверс-инженер Тилли Коттманн собрала и опубликовала утечку кода более чем 50 компаний, включая Microsoft, Adobe, Lenovo, AMD, Qualcomm, Motorola, Hisilicon (принадлежит Huawei), Mediatek, GE Appliances, Nintendo, Roblox, Disney и других в публичный репозиторий GitLab.

Коттманн сказал, что на данный момент существуют тысячи компаний, которые раскрывают проприетарный исходный код, не в состоянии должным образом защитить свои установки SonarQube.

Коттманн также просочился примерно 20 ГБ конфиденциальных документов Intel в августе, после получения их от анонимного источника, который якобы ранее взломал серверы компании.

Позже компания сообщила BleepingComputer, что «информация, по всей видимости, поступает из Центра ресурсов и проектирования Intel, в котором размещена информация для использования нашими клиентами, партнерами и другими внешними сторонами, зарегистрировавшимися для доступа».

Предыдущие атаки и меры по смягчению

Злоумышленники начинают свои атаки, сначала сканируя экземпляры SonarQube, подключенные к Интернету, используя номер порта по умолчанию (например, 9000), как объясняет ФБР.

После обнаружения открытого сервера они пытаются получить доступ к уязвимым экземплярам, используя учетные данные администратора / администратора по умолчанию.

Не называя имен, ФБР выделяет два таких события во флэш-предупреждении, одно из которых было проведено идентифицированным актером, а другое, где злоумышленники до сих пор неизвестны:

• В июле 2020, идентифицированного кибер актер exfiltrated собственности исходного кода от предприятий через плохо обеспеченные экземпляры SonarQube и опубликовал exfiltrated исходного кода на самопринятом общедоступном хранилище.

• В августе 2020 года неизвестные злоумышленники осуществили утечку внутренних данных двух организаций через общедоступный репозиторий жизненного цикла. Похищенные данные были получены из экземпляров SonarQube, которые использовали настройки порта по умолчанию и учетные данные администратора, работающие в сетях затронутых организаций.

ФБР предлагает следующие меры по предотвращению атак:

• Измените настройки SonarQube по умолчанию, включая изменение имени пользователя, пароля и порта администратора по умолчанию (9000).

• Поместите экземпляры SonarQube за экраном входа в систему и проверьте, получили ли к экземпляру доступ неавторизованные пользователи.

• Отменить доступ к любым ключам интерфейса программирования приложений или другим учетным данным, которые были представлены в экземпляре SonarQube, если это возможно.

• Настройте экземпляры SonarQube так, чтобы они находились за брандмауэром вашей организации и другими средствами защиты периметра, чтобы предотвратить доступ без аутентификации». ***(Sergiu Gatlan. FBI: Hackers stole government source code via SonarQube instances // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-hackers-stole-government-source-code-via-sonarqube-instances/). 27.10.2020).***

***

«Американский оператор горнолыжных и гольф-курортов Boyne Resorts подвергся кибератаке из-за операции WastedLocker, которая затронула системы бронирования в масштабах всей компании.

Boyne Resorts владеет и управляет одиннадцатью объектами, расположенными в США и Канаде, и имеет 11 000 сотрудников. Многие из этих отелей расположены в известных горнолыжных горах, включая Биг-Скай, Монтана, Сахарная голова, штат Мэн, и Брайтон, штат Юта.

Boyne Resorts поражен программой-вымогателем WastedLocker

Сегодня BleepingComputer получил анонимный совет от предполагаемого сотрудника Boyne Resorts, который заявил, что на прошлых выходных компания подверглась нераскрытой атаке с использованием программ-вымогателей.

Нам сообщили, что атака затронула их корпоративные офисы, а затем распространилась на ИТ-системы курортов, которыми они управляют, вынуждая их отключать части своей сети, чтобы предотвратить распространение программ-вымогателей.

С тех пор BleepingComputer подтвердил со вторым источником, что Boyne Resorts подверглась атаке с использованием вымогателя WastedLocker, того же самого, который использовался при атаке на Garmin в июле.

Из-за этой атаки невозможно забронировать проживание на курорте, поскольку атака затронула системы бронирования в масштабах компании, в том числе системы онлайн-бронирования на веб-сайтах каждого отеля.

BleepingComputer сообщили, что системы бронирования, как ожидается, не будут работать еще пару дней. Это нападение происходит в неподходящее время для Бойна, поскольку люди начинают планировать возможные лыжные поездки на зиму.

В рамках этой атаки нам сообщают, что зашифрованные файлы были переименованы, так что к имени каждого файла добавлялось расширение.easy2lock.

BleepingComputer смог найти образец вымогателя WastedLocker, загруженный на VirusTotal 14 октября 2020 года и использующий расширение.easy2lock. Из-за более ранней даты мы не считаем, что это точный образец, использованный при нападении на курорт Boyne.

Ниже приведен пример записки с выкупом, созданной этим вариантом программы-вымогателя WastedLocker. Эта записка с требованием выкупа может отличаться от той, что использовалась во время атаки курорта Бойн.

BleepingComputer обратился в Boyne Resorts с дополнительными вопросами об этой атаке, но не получил ответа.

WastedLocker связан с санкционированной США хакерской группой

Охранные фирмы приписывают WastedLocker находящейся в России хакерской группировке, известной как Evil Corp (также известной как банда Dridex).

Эта группа действует по крайней мере с 2007 года и известна разработкой вредоносного ПО Dridex и штамма вымогателей, известного как BitPaymer.

В декабре 2019 года Министерство финансов США наложило санкции на Evil Corp за причинение финансового ущерба на сумму более 100 миллионов долларов.

В связи с этим возникнет сложная ситуация, если Boyne Resorts захотят заплатить выкуп, поскольку они потенциально нарушат санкции США.

Выплаты выкупа в пользу WastedLocker в этом месяце стали более рискованными, поскольку Управление по контролю за иностранными активами Министерства финансов США (OFAC) выпустило предупреждение о том, что организации, осуществляющие выплаты выкупа, сталкиваются с рисками санкций, если их действия нарушают правила OFAC». ***(Lawrence Abrams. WastedLocker ransomware hits Boyne Resorts ski resort operator // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/wastedlocker-ransomware-hits-boyne-resorts-ski-resort-operator/). 23.10.2020).***

***

«Ущерб, который кибератаки наносят бизнесу, многообразен: прямое вымогательство, хищение технологий и чувствительной информации, вынужденные простои, снижение качества продуктов и услуг, из-за которого предприятия упускают прибыль и теряют доверие клиентов и партнеров. Потери бизнеса в 2018 году оценивались в $45 млрд, но реальная сумма, вероятно, гораздо больше: многие инциденты замалчиваются или выявляются с задержкой. А в этом году из-за пандемии ситуация осложнилась еще и глобальным переходом компаний на удаленную работу.

Rusbase совместно с компанией Fortinet осматривают ландшафт киберугроз 2020 года.

Специалисты называют пять основных типов киберугроз: программы-вымогатели, целевые кибератаки, DDoS-атаки, фишинг и внутренние угрозы, связанные с деятельностью инсайдеров и человеческими ошибками. Согласно последнему отчету Verizon по киберпреступности, 86% атак финансово мотивированы: злоумышленники либо напрямую вымогают деньги у жертвы, либо выполняют сторонний заказ, например, конкурентов или иных недоброжелателей.

По словам технического директора компании Fortinet в России Алексея Андрияшина, в наибольшей степени сегодня подвержены атакам операторы связи, финансовые организации, ритейл-сети и промышленный сектор. При этом малый и средний бизнес по мере его цифровизации привлекает все больше внимания киберпреступников. Это объясняется тем, что конкуренция в нем достаточно высока, а возможности киберзащиты и оценки рисков зачастую ограничены. Усугубляет проблему массовый переход на удаленную работу, из-за чего периметр сети компаний по сути распространился на дома сотрудников и их личные устройства. Хотя этот шаг в целом соответствует духу прогресса, из-за стихийного характера он умножил слабые места в цифровой обороне предприятий.

Программы-вымогатели

Вирусы-вымогатели шифруют данные на компьютере пользователя и требуют выкуп за возможность восстановить доступ к ним. Обычно предлагается заплатить выкуп криптовалютой. Проникнув в корпоративную сеть, вирусы-вымогатели способны блокировать сразу большое количество компьютеров.

Согласно отчету Verizon, в прошлом году на вымогателей приходилось 27% инцидентов, связанных с вредоносным ПО. По данным исследования Global Threat Landscape Report компании Fortinet, в наибольшей степени подвержены атакам с целью вымогательства телекоммуникационные компании, интернет-провайдеры, образовательные учреждения, правительственные и технологические организации.

И если раньше кибервымогатели действовали по принципу spray and pray («распыляй и молись», то есть стремились заразить как можно больше любых жертв), то в последние годы они перешли к более целенаправленным атакам, сосредотачиваясь на конкретных отраслях с их характерными уязвимостями. Таков был, например, вирус WannaCry, поразивший в 2017 году более 100 тысяч компаний не менее чем в 150 странах.

Более свежий пример – вымогатель EKANS, созданный для атак на промышленные сети и системы управления. В начале 2020 года, по данным

Министерства внутренней безопасности США, из-за атаки EKANS работа неназванного оператора газопровода оказалась парализована на два дня.

Традиционные программы-антивирусы эффективны лишь против уже известных вирусов-вымогателей. В основе работы антивируса – картотека сигнатур («подписей»), по которым он определяет врага. Поэтому он может выявлять только «рецидивистов». Более современные средства защиты используют элементы искусственного интеллекта и распознают вирусы-вымогатели не по сигнатурам, а по особенностям поведения.

Но для полноценной защиты от вымогателей требуется не только современное программное обеспечение, но и системная профилактика, включающая оценку рисков, установку межсетевых экранов, создание резервных копий, разработку сценариев реагирования и другие меры.

Целевые кибератаки

Целевая атака или APT (advanced persistent threat – «развитая устойчивая угроза») – это высший пилотаж киберпреступности, спланированная операция, обычно из нескольких этапов, примерно как в шпионском кино.

Сначала злоумышленники ищут способ внедриться в корпоративную сеть: собирают информацию, ищут уязвимости компании (не только цифровые, но и физические), изучают расписание, маршруты, слабости интересующих сотрудников и так далее.

Затем осуществляется собственно проникновение: злоумышленники могут прислать таргетированное на конкретного сотрудника фишинговое письмо, украсть телефон сотрудника для извлечения каких-либо корпоративных паролей, втереться в доверие компании под видом подрядчика или проникнуть в офис в качестве курьера – вариантов множество. Целью на этом этапе является скрытая установка ПО на корпоративной технике.

Когда плацдарм готов, злоумышленники, действуя уже изнутри компании, подбираются к интересующей их информации и похищают ее в обход средств защиты. Затем, как правило, следует «уборка»: злоумышленники заметают следы, чтобы атака не была обнаружена. В целевой атаке могут использоваться любые другие киберпреступные методы – фишинг, вымогательство и так далее.

Целевые кибератаки сложны и дорогостоящи, поэтому ассоциируются с деятельностью государственных разведок или с крупным бизнесом. Но их целью может стать и, например, стартап с какой-то перспективной технологией. То есть никто не застрахован.

Как пример актуальной APT-угрозы компания Fortinet приводит киберпреступную группировку HIDDEN COBRA (название дано американской разведкой), существующую с 2014 года. ФБР предполагает, что она связана с правительством Северной Кореи, которое в условиях санкций не брезгует любыми способами для зарабатывания денег. Группировка стояла за уже упомянутым вирусом-вымогателем WannaCry и представляет угрозу по сей день.

Предотвращение целевых атак – сложная задача. Однако современные средства защиты при их правильном и комплексном использовании позволяют понять, что в компании происходит какая-то неавторизованная активность. Например, Network Access Control позволяет исключить внедрение в сеть

постороннего устройства. Каждый пользователь должен сначала пройти идентификацию, то есть доказать системе, что это он, а затем авторизацию, то есть получить строго определенные права в системе.

Для предотвращения целевых атак требуется строгое и четкое распределение прав доступа внутри компании и соблюдение принципа минимальной достаточности: то есть выполняются лишь те действия, которые нужны для бизнес-процессов.

DDoS-атаки

DDoS-атака – это атака на какую-либо вычислительную систему (например, сервер) с целью исчерпать ее аппаратный ресурс путем огромного количества одновременных обращений к ней. Когда система не справляется с обработкой этих обращений, происходит отказ в обслуживании (Denial of Service) и система выходит из строя. Первая буква D в DDoS описывает характер атаки – она распределенная (Distributed), то есть совершается одновременно с большого количества устройств, которые предварительно были заражены злоумышленниками и превращены в послушную армию (ботнет, сеть ботов). Как правило, сначала киберпреступники создают ботнет, а потом через даркнет ищут заказы на его использование.

DDoS-атаки представляют опасность в первую очередь для компаний, деятельность которых напрямую связана с интернетом (вся электронная коммерция), а также для операторов связи. DDoS-атаки длятся недолго, поскольку это довольно дорогое удовольствие. Редко больше недели, но может быть достаточно и пары часов. Скажем, кто-то хочет убрать конкурентов с тендера, начало и продолжительность которого известны: достаточно обрушить сайт конкурента на время тендера – и цель достигнута.

В последнее время злоумышленники охотно «рекрутируют» в свои ботнеты устройства интернета вещей (IoT), то есть, к примеру, бытовые приборы с подключением к интернету: принтеры, умные колонки, кондиционеры, системы освещения в умном доме и так далее. Производители IoT-устройств, как и пользователи этих устройств, зачастую уделяют мало внимания их безопасности, поэтому заразить IoT-устройство относительно просто.

Среди ботнетов 2020 года можно выделить специализированный на IoT-устройствах Dark Nexus, который атакует роутеры Dasan Zhone, DLink и ASUS, а также видеорекордеры, тепловые камеры и другие устройства. По мнению специалистов, Dark Nexus имеет особенности, дающие ему преимущество перед другими ботнетами. Например, при попадании на устройство он анализирует запущенные на нем процессы и прерывает те из них, которые оценивает как опасные для себя.

Для борьбы с DDoS-атаками применяют DDoS-фильтры, позволяющие избирательно отсекать «мусорные» обращения к серверу, идущие от ботов. Профилактика DDoS-атак включает обеспечение резервных мощностей, а также разумную минимизацию контактов системы с другими устройствами: доступ к системе должен быть закрыт для портов, протоколов и приложений, взаимодействие с которыми не предусмотрено.

Фишинг

Название этого типа угроз, образованное от английского слова fishing – «рыбалка», – вполне точно его описывает. Подобно рыбаку, злоумышленник готовит приманку и «крючок», только охотится он на людей, а сам процесс разворачивается в цифровом пространстве. Чаще всего приманкой является электронное письмо, способное заинтересовать получателя, а крючком – заложенный в это письмо вредоносный исполняемый файл или гиперссылка на него.

Сейчас, когда всех волнует тема Covid-19, это может быть ссылка якобы на свежую статистику по данной теме или какую-то иную животрепещущую информацию, которая интересна многим пользователям. При открытии ссылки запускается вредоносный файл. По данным исследования Global Threat Landscape Report компании Fortinet, больше всего от атак, связанных с тематикой пандемии, в этом году страдают организации США, Китая и России.

Актуальный пример – троян Dridex, который прячется в таблицах Microsoft Excel. Фишинговое письмо, которое получает пользователь, выглядит в точности как письмо от службы доставки (UPS, FedEx, DHL). В условиях пандемии спрос на услуги доставки существенно вырос, поэтому вероятность, что пользователь ожидает доставку и откроет вложение, весьма велика. На это и расчет.

Опасность фишинга в том, что главный элемент в нем не технический, а психологический. Злоумышленники знают, что человека обмануть легче, чем машину. Современные средства защиты позволяют в автоматическом режиме во всех файлах, которые передаются по почте или через интернет, вырезать исполняемое содержание, оставляя только текст и изображения. Также они могут анализировать ссылки в процессе открытия и прерывать этот процесс, если фиксируют запуск исполняемых файлов.

Внутренние угрозы

Обнаружение внутренних или инсайдерских атак – одна из наиболее сложных задач, потому что регламенты информационной безопасности обычно построены исходя из защиты от внешних угроз. А инсайдер – это сотрудник компании, по умолчанию ему доверяют, он имеет доступ к ресурсам организации, может свободно перемещаться и обмениваться информацией. То есть речь идёт уже не об IT-безопасности, а о физической безопасности.

IT-безопасность построена на автоматизированном обнаружении угроз, что в данном случае может не сработать. Здесь требуется взаимодействие IT-подразделения со службой безопасности компании и регламентация физического доступа сотрудников к тем или иным помещениям в то или иное время. Но все равно это не гарантирует, что угроза будет своевременно обнаружена.

Инсайдерские угрозы могут быть связаны как со злым умыслом, так и со случайными действиями, с человеческой ошибкой. С ненамеренными действиями бороться проще – здесь нужны проработка регламентов, разграничение прав, отлаженность систем идентификации и авторизации. И опять же – принцип минимальной достаточности: сотруднику нужно давать только те права, которые ему нужны для выполнения рабочих обязанностей. С инсайдерами-злоумышленниками бороться гораздо сложнее. Очищать память сотрудников на

выходе из компании невозможно (тем более, что сегодня многие сотрудники сидят по домам).

Против инсайдерских атак, помимо регламентов и прав доступа, помогут средства, которые анализируют поведение пользователей – User Experience Behavioral Analytics. Эти решения, построенные на технологиях искусственного интеллекта и способные к обучению на основе статистики, постоянно мониторят активность сотрудников на рабочих местах. Если те отклоняются от заранее заданных сценариев деятельности, то формируются оповещения для службы безопасности, которая может заблокировать то или иное действие». ***(Как обезопасить бизнес от киберпреступников: главные угрозы 2020 года и стратегии защиты от них // ООО РБ.РУ (https://rb.ru/longread/threats-of-2020/). 28.10.2020).***

***

«До выборов остается всего неделя, и киберпреступники наращивают мобильные атаки на граждан под видом агитационных сообщений.

Граница между нашей личной и профессиональной жизнью стирается беспрецедентным образом по мере приближения президентских выборов 2020 года. От планов Oracle и Walmart по инвестированию в TikTok до ошибки в приложении кампании Джо Байдена, из-за которой были обнаружены миллионы файлов избирателей, - роль мобильных технологий в продвижении выборов является критической.

До выборов всего неделя, и было много дискуссий о том, как заочное и досрочное голосование повлияют на результат. Но даже до того, как бюллетени начали попадать в почтовую службу, распространение дезинформации уже шло полным ходом, оставляя за собой сбитых с толку американцев.

Человеческая ошибка неизбежна даже среди самых образованных пользователей. И хотя 2020 год принес много проблем, возможно, наиболее важным с социальной точки зрения является то, как мы интегрировали мобильные устройства в нашу повседневную жизнь. К сожалению, реальность сегодняшнего ландшафта угроз такова, что успешные атаки целевого фишинга больше не полагаются исключительно на электронную почту. Итак, при чем здесь выборы?

Атаки, направленные на срыв выборов, обычно проводятся скрытно, с использованием кампаний, направленных на то, чтобы заманить жертв в фишинговые атаки. В последнее время в ходе президентских кампаний пытались связаться с избирателями напрямую, отправив SMS-сообщения с вопросом, зарегистрировались ли они для голосования или планируют ли они поддержать кандидата. Злоумышленники могут легко имитировать эту стратегию и включить в сообщение вредоносную ссылку. Мы видели аналогичную тактику, используемую в текущей кампании мобильного фишинга, при которой отправляется сообщение, якобы являющееся пропущенной доставкой пакета, со ссылкой на поддельную страницу заявки, которая является атакой мобильного фишинга.

Теперь у злоумышленников есть бесконечные способы заставить вас использовать вредоносную ссылку в социальных сетях - от приложений для обмена сообщениями и социальных сетей до приложений для знакомств. Также не

помогает то, что мобильные устройства имеют меньшие экраны и упрощенный пользовательский интерфейс, из-за чего трудно понять, что подделка, а что настоящее.

В сентябре этого года по крайней мере три профиля TikTok продвигали несколько мошеннических мобильных приложений, которые принесли почти полмиллиона долларов общей прибыли. Как сообщается, эти аккаунты с помощью социальной инженерии заставляли своих подписчиков скачивать вредоносные приложения. Хотя они гораздо менее целенаправленны, чем атаки социальной инженерии, о которых мы обычно думаем, процессы и цели идентичны.

Мы должны помнить, что злоумышленники тоже деловые люди. Они нацелены на жертв и используют методы, которые, по их мнению, принесут наибольшую отдачу. Одна из больших возможностей в 2020 году - президентские выборы в США, и их цель - мобильные пользователи. Планшеты и смартфоны стали неотъемлемой частью того, как мы работаем и играем, и активность в сезон голосования не исключение. Политические кампании используют их в качестве средств взаимодействия с избирателями. Общественность получает информацию со своих мобильных устройств. Были даже попытки провести местные выборы и праймериз с помощью мобильных приложений.

Все более широкое использование мобильных устройств имеет множество преимуществ, таких как более активное участие и более высокая явка избирателей. Но это должно происходить только в том случае, если мобильная безопасность является частью более масштабного плана обеспечения безопасности на выборах. Приложение Vote Joe было ярким примером приложения для кампании, которое имело серьезные недостатки в безопасности. В приложении была обнаружена ошибка, которая позволяла злоумышленникам видеть домашний адрес избирателя, дату рождения, пол, этническую принадлежность и партийную принадлежность.

В процессе регистрации в Vote Joe не только отсутствовали базовые функции проверки электронной почты, но и непроверенным пользователям был предоставлен доступ к базе данных зарегистрированных избирателей. Хотя целью было повысить вовлеченность избирателей, в конечном итоге личная информация людей была раскрыта ненадлежащим образом.

Мобильная безопасность и кибергигиена необходимы для обеспечения безопасности политических кампаний и их данных, и не только для выборов 2020 года. Хорошая новость заключается в том, что осведомленность о проблемах безопасности на выборах и избирательных кампаниях растет, и есть ресурсы для оказания помощи. Такие организации, как Defending Digital Campaigns, некоммерческая организация, целью которой является обеспечение безопасности кампаний, предлагают кандидатам бесплатные или недорогие решения по обеспечению безопасности и обучение. В дополнение к мерам безопасности нам также необходимо информировать широкую общественность о том, что мобильные устройства являются основными целями для злоумышленников…». ***(Hank Schless. Election Security: How Mobile Devices Are Shaping the Way We Work, Play and Vote // Threatpost (https://threatpost.com/mobile-devices-vote-election-security/160648/). 28.10.2020).***

***

«Сложный набор перенаправлений и сотни URL-адресов составляют широкомасштабную аферу с технической поддержкой.

Изощренная кампания «шкафчика браузера» распространяется через Facebook, в конечном итоге подталкивая к мошенничеству с техподдержкой. По словам исследователей, эта попытка является более продвинутой, чем многие другие, поскольку она включает в себя использование уязвимости межсайтового скриптинга (XSS) на популярном новостном сайте.

Блокировщики браузера - это тип атаки с перенаправлением, при которой пользователи сети нажимают на сайт только для того, чтобы попасть на страницу с предупреждением о том, что их компьютер заражен «вирусом» или вредоносным ПО. Затем страница обычно побуждает пользователей позвонить по номеру, отображаемому на экране, для «технической поддержки». Если они на это попадают, их подключают к колл-центру, где их просят заплатить плату за «чистку» их машин.

По словам исследователей, в недавней широко распространенной кампании кибератаки используют Facebook для распространения вредоносных ссылок, которые в конечном итоге перенаправляют на страницу блокировки браузера. Ссылки могут распространяться через игры Facebook, отметили исследователи Malwarebytes в опубликованном в среду сообщении с изложением своих выводов.

«Кампания, которую мы рассмотрели, похоже, использует исключительно ссылки, размещенные на Facebook, что довольно необычно, учитывая, что традиционно мошенничество с техподдержкой распространяется через вредоносную рекламу», - сказал исследователь Malwarebytes Жером Сегура.

Facebook выдает всплывающее окно для пользователей, предлагая им подтвердить перенаправление, но пункт назначения скрыт из-за того, что ссылка является немного сокращенным URL-адресом, добавил он.

В целом, фирма обнаружила 50 различных ссылок bit.ly, использовавшихся для мошенничества за трехмесячный период, «что говорит о регулярной ротации, чтобы избежать попадания в черный список», - сказал Сегура.

XSS-уязвимость

URL-адреса bit.ly перенаправляют на перуанский веб-сайт под названием RPP, который «совершенно законен и привлекает более 23 миллионов посещений в месяц», - сказал Сегура. Он добавил, что сообщил об этой проблеме Grupo RPP, но на момент публикации не получил ответа.

Он обнаружил, что сайт содержит ошибку XSS, которая допускает открытое перенаправление. Открытые перенаправления происходят, когда значения параметров (часть URL после «?») В HTTP-запросе GET допускают информацию, которая перенаправит пользователя на новый веб-сайт без какой-либо проверки того, является ли цель преднамеренной или законной. Таким образом, злоумышленник может манипулировать этим параметром, чтобы отправить жертву на поддельную страницу, но действие будет выглядеть законным действием, задуманным веб-сайтом.

«Злоумышленники любят злоупотреблять открытыми перенаправлениями, поскольку это придает легитимность URL-адресам, которые они отправляют жертвам», - утверждают исследователи.

В этом случае злоумышленники используют ошибку XSS для загрузки внешнего кода JavaScript из buddhosi [.] Com, вредоносного домена, контролируемого злоумышленниками, который заменяет код в URL-адресе для создания перенаправления.

«JavaScript, в свою очередь, создает перенаправление на целевую страницу браузера с помощью метода replace ()», - говорится в анализе. Метод replace () ищет в строке указанное значение и возвращает новую строку, в которой указанные значения заменяются.

Сегура отметил, что помимо перенаправления пользователей на другие сайты, злоумышленник может использовать XSS, чтобы переписать текущую страницу во что угодно.

В любом случае, окончательная целевая страница шкафчика браузера размещается на одном из примерно 500 «одноразовых» доменов со случайными названиями, которые используют множество новых доменов верхнего уровня (таких как.casa;.site;.space;. club;.icu; или.bar).

Браузер Locker

Как только пользователь попадает на страницу блокировки браузера, он снимает отпечатки пальцев в браузере пользователя, чтобы отобразить соответствующее контексту сообщение.

«Он показывает анимацию, имитирующую сканирование текущих системных файлов, и угрожает удалить жесткий диск через пять минут», - отметил Сегура. «Конечно, это все подделка, но это достаточно убедительно, чтобы некоторые люди звонили по бесплатному номеру для получения помощи».

Номера телефонов, как и сами страницы, тоже объемные. Malwarebytes нашел почти 40 различных телефонных номеров и отметил, что их, вероятно, намного больше.

В целом цепочка событий сложна и достаточно обширна, чтобы помочь злоумышленникам избежать отключения. Сегура сказал, что у Facebook тоже есть здравый смысл.

Как всегда, лучшая защита от мошенничества такого рода - простая осведомленность.

В качестве отправной точки «ссылки, размещаемые на платформах социальных сетей, всегда следует тщательно проверять, поскольку они являются часто используемым способом мошенников и авторов вредоносных программ для перенаправления пользователей на нежелательный контент», - отметил он». ***(Tara Seals. Facebook, News and XSS Underpin Complex Browser Locker Attack // Threatpost (https://threatpost.com/facebook-xss-browser-locker/160465/). 22.10.2020).***

***

«Тысячи конфиденциальных документов оказались скомпрометированы в результате взлома шведской компании Gunnebo, занимающейся производством продуктов, ПО и сервисов для обеспечения безопасности.

Во вторник, 27 октября, Gunnebo подтвердила, что стала жертвой операции по ограблению, которая могла затронуть парламент Швеции и европейские банки. Названия компаний и организаций, пострадавших от кибератаки, не раскрываются. Как сообщил пресс-секретарь компании изданию Euronews, инцидент был «чрезвычайно прискорбным».

Расследованием инцидента занялась Служба государственной безопасности Швеции (СЭПО) после того, как криминалисты установили, что атака была «хорошо организована».

«Мы можем только догадываться о причинах атаки, но не исключено, что это была попытка промышленного шпионажа», – сообщил президент Gunnebo Стефан Сюрен (Stefan Syrén).

В августе 2020 года сотрудники IT-отдела Gunnebo обнаружили, что неавторизованные злоумышленники попытались получить доступ к серверам компании. По данным газеты Dagens Nyheter, в общей сложности было похищено 19 ГБ данных (порядка 38 тыс. файлов), в том числе подробности о средствах безопасности в шведском парламенте, сейфах как минимум в двух банках и конфиденциальную информацию о новом офисе налогового управления в Стокгольме.

Обнаружив попытку вторжения, сотрудники IT-отдела сразу же отключили серверы. Через несколько дней Gunnebo сообщила об инциденте пострадавшим клиентам и проанализировала данные на серверах по всему миру.

18 ГБ похищенной информации злоумышленники загрузили в даркнет. На одной из web-страниц со ссылкой для загрузки утекших данных представлена финансовая информация Gunnebo, банковские реквизиты и пароли, а также сведения о транзакциях клиентов, пишет Reuters.

Как отметил Сюрен, компания даже не рассматривает возможность уплаты выкупа злоумышленникам. Единственный способ борьбы с такими преступниками – не идти у них на поводу.

Gunnebo – многонациональная корпорация со штаб-квартирой в Гетеборге (Швеция) специализирующаяся на продуктах, услугах и решениях в области безопасности, главным образом в области управления денежными средствами, контроля доступа, безопасного хранения и комплексной безопасности». ***(Парламент Швеции мог пострадать в результате взлома компании Gunnebo // SecurityLab.ru (https://www.securitylab.ru/news/513420.php). 28.10.2020).***

***

«Компьютерные системы крупнейшего индийского информационного агентства Press Trust of India (PTI) подверглись масштабной атаке с использованием программ-вымогателей, которая нарушила работу серверов на несколько часов…

Атака операторов вымогательского ПО LockBit затронула почти все серверы главного информагентства Индии. Вредонос зашифровал все данные и приложения, что привело к прекращению доставки новостей подписчикам PTI. Программа-вымогатель через сообщение на экране компьютера потребовала выкуп для предоставления ключа для ее расшифровки.

По словам представителя компании, IT-инженеры PTI работали над поэтапным восстановлением систем 11 часов, и никакого выкупа уплачено не было.

Программы-вымогатели остаются одной из основных проблем, особенно с учетом того, что подобные группировки все чаще демонстрируют высокий уровень навыков и изощренности. Во многих случаях вымогатели не просто шифруют данные с помощью вредоносного ПО и требуют сотни тысяч или миллионов долларов в биткойнах, но они также угрожают утечкой украденных конфиденциальных корпоративных файлов или персональной информации жертв, если их требования не будут выполнены…». ***(Вымогатель LockBit нарушил работу крупнейшего индийского информагенства // SecurityLab.ru (https://www.securitylab.ru/news/513390.php). 27.10.2020).***

***

«Специалисты компании Trend Micro рассказали о новой вредоносной кампании с использованием бэкдора SLUB, получившей название Operation Earth Kitsune. В ходе кампании злоумышленники шпионят за пользователями через скомпрометированные сайты.

Исследователи Trend Micro впервые обнаружили SLUB в прошлом году, теперь же они выявили вредоносную кампанию watering hole, в ходе которой злоумышленники используют новый вариант вредоноса. В свое время вредоносное ПО получило название SLUB, поскольку использовало Slack и GitHub, однако в новом варианте бэкдора эти платформы не используются. Вместо них SLUB теперь полагается на сервис для общения с открытым исходным кодом Mattermost.

В ходе кампании Operation Earth Kitsune используется пять C&C-серверов, семь образцов вредоносного ПО и четыре новые уязвимости для компрометации сайтов с целью хостинга вредоносного ПО.

Исследователи начали свое расследование после того, как сайт организации Korean American National Coordinating Council (KANCC) стал переадресовывать пользователей на сайт Hanseattle, который перенаправлял их на эксплоит для уязвимости CVE-2019-5782 в Google Chrome. Копнув глубже, специалисты обнаружили, что атака включает не только упомянутый эксплоит, но и три отдельных образца вредоносного ПО (SLUB, dneSpy и agfSpy). В то время как цель SLUB в этой кампании – кража системной информации, два других варианта вредоносного ПО предназначены для получения дополнительного контроля над компьютером жертвы.

Помимо уязвимости в Google Chrome злоумышленники также эксплуатируют уязвимости в Internet Explorer (CVE-2020-0674, CVE-2016-0189, CVE-2019-1458)». ***(Операторы бэкдора SLUB шпионят за пользователями через взломанные сайты // SecurityLab.ru (https://www.securitylab.ru/news/513280.php). 22.10.2020).***

***

«Группа Roaming Mantis нацелена на Штаты с помощью вредоносного ПО, которое может красть информацию, собирать финансовые данные и отправлять тексты для самораспространения.

Троян мобильного банкинга Wroba совершил серьезный поворот, впервые нацелившись на людей в США.

По словам исследователей «Лаборатории Касперского», волна атак нацелена на пользователей Android и iPhone в США, начавшаяся в четверг. Кампания использует текстовые сообщения для распространения, используя фальшивые уведомления о «доставке посылок» в качестве приманки.

Сообщение внутри SMS содержит ссылку и гласит: «Ваша посылка отправлена. Пожалуйста, проверьте и примите его», - отметили исследователи из «Лаборатории Касперского» в уведомлении по электронной почте в пятницу.

Если пользователи нажимают на ссылку, следующее, что происходит, зависит от того, какая операционная система используется на устройстве. Щелчок приводит пользователей Android на вредоносный сайт, который, в свою очередь, выводит предупреждение для пользователей о том, что браузер устарел и нуждается в обновлении. Если пользователь нажимает «ОК», начинается загрузка троянизированного пакета браузера с вредоносным приложением.

Но если пользователям Android предоставляется полная загрузка Wroba, по мнению исследователей, исполняемый файл не работает на iPhone. Для пользователей iOS операторы Wroba вместо этого создают перенаправление на фишинговую страницу. Страница имитирует страницу входа в систему Apple ID, чтобы получить учетные данные от поклонников Apple, но никаких вредоносных программ не установлено.

По состоянию на май Apple занимала более половины всей доли рынка смартфонов в США.

Wroba существует уже много лет, но ранее он был ориентирован на пользователей Азиатско-Тихоокеанского региона. Впервые он был разработан как троян для мобильного банкинга для Android, способный красть файлы, связанные с финансовыми транзакциями, но с тех пор расширил свои функции. Исследователи полагают, что оператор Wroba находится в Китае и известен как Roaming Mantis.

По словам исследователей, эта последняя версия Wroba может отправлять SMS-сообщения, проверять, какие приложения установлены, открывать веб-страницы, собирать любые файлы, связанные с финансовыми транзакциями, красть списки контактов, звонить по указанным номерам и показывать поддельные фишинговые страницы для кражи учетных данных жертвы.

После заражения устройства Wroba использует некоторые из своих функций - похищенные списки контактов и возможность SMS-сообщений - для распространения, используя зараженные устройства для дальнейшего распространения, отправляя SMS с вредоносными ссылками, якобы исходящими с хоста.

«Wroba показывает, как доставка вредоносного ПО на устройство может обеспечить долгосрочную выгоду для атаки», - сказал Хэнк Шлесс, старший менеджер по решениям безопасности в Lookout, который также отслеживает Wroba.

«Ссылка для сбора учетных данных нацелена на вас только для одной цели, например, когда вы получаете SMS-сообщение, в котором говорится, что ваш

банковский счет был взломан, и целью является фишинг ваших банковских учетных данных», - сказал он Threatpost.

«С другой стороны, Wroba может молча сидеть в фоновом режиме и по желанию доставлять страницы сбора учетных данных в ваш браузер», - сказал он. «Пока он остается незамеченным, он может пытаться захватить ваши данные для входа даже в самые личные учетные записи».

По словам исследователей, вредоносная программа с начала года нацелена на пользователей по всему миру, в основном в Китае, Японии и Российской Федерации.

«США в настоящее время не возглавляют список, но похоже, что киберпреступники направляются в этот регион, и количество пользователей, видящих Wroba, будет увеличиваться», - считает Касперский. «Волна была обнаружена 29 октября и нацелена на пользователей в разных штатах США (судя по телефонным номерам, которые были целью этой кампании)».

Фирма добавила: «Ранее проводившиеся кампании были нацелены на пользователей из Азиатско-Тихоокеанского региона, поэтому интересно посмотреть, как киберпреступники расширяют свои цели».

В 2018 году компания Wroba пережила серьезную перезагрузку, когда она начала ориентироваться не только на страны Азии, но и на Европу и Ближний Восток. По словам исследователей Kaspersky в то время, он также расширил свои возможности, включив криптомайнинг, а также упомянутую ранее тактику фишинга iOS. В тот момент он распространялся посредством перехвата DNS, который перенаправлял пользователей на вредоносную веб-страницу, которая, как и в текущей кампании, распространяла троянизированное приложение (в то время оно выдавало себя либо Facebook, либо Chrome).

Следует отметить, что в прошлом Roaming Mantis наполнил США. Этим летом было замечено проведение другой SMS-фишинг-кампании, распространяющей инфостилер FakeSpy. Вредоносная программа, которая была замаскирована под законные глобальные почтовые приложения, также крадет SMS-сообщения, финансовые данные и многое другое с устройств жертв. Сначала он преследовал жителей Южной Кореи и Японии, но затем расширил этот таргетинг на Китай, Тайвань, Францию, Швейцарию, Германию, Соединенное Королевство и США.

Шлесс сообщил Threatpost, что согласно данным Lookout, 88% фишинговых атак потребителей в США в 2020 году были попытками доставить вредоносное ПО на мобильное устройство.

Чтобы не стать жертвой Wroba или любого другого мобильного вредоносного ПО, пользователи должны соблюдать базовые правила безопасности, подчеркнули исследователи, например, загружать приложения только из официальных магазинов; отключение установки приложений из сторонних источников в настройках смартфона; и избегайте нажатия на подозрительные ссылки от неизвестных отправителей или даже на подозрительные ссылки от известных отправителей.

«Люди по-прежнему пытаются избежать фишинговых атак по электронной почте», - сказал Threatpost Рэй Келли, главный инженер по безопасности WhiteHat

Security. «Теперь SMS-сообщения еще больше усложняют ситуацию. С SMS следует обращаться так же, как с электронной почтой, никогда не переходите по ссылкам от неизвестных или подозрительных отправителей». ***(Tara Seals. Wroba Mobile Banking Trojan Spreads to the U.S. via Texts // Threatpost (https://threatpost.com/wroba-mobile-banking-trojan-spreads-us/160785/). 30.10.2020).***

***

Діяльність хакерів та хакерські угруповування

«Еще на прошлой неделе появилась информация, что хакерам удалось разработать и выпустить джейлбрейк для процессоров T2. Кто не знает, T2 – это специальные чипы, обеспечивающие безопасность в компьютерах Mac. В них есть своя операционная система SepOS, в которой еще летом была обнаружена уязвимость.

Комбинируя два эксплойта – checkra1n и blackbird – вместе с физическим доступом к устройству, можно провести джейлбрейк процессора, потому что «Apple оставила интерфейс дебаггинга в процессорах, что позволяет любому войти в режим DFU без аутентификации». Короче, используя эту информацию, потенциально можно создать USB-C кабель, который будет «взламывать» Mac при загрузке. Потенциально это может обеспечить злоумышленникам доступ к данным, которые хранятся на устройствах зашифрованными, но не сразу. Автоматически доступа к зашифрованным файлам получить нельзя, но можно воткнуть кейлоггер в прошивку Mac, и собрать пароль к расшифровке файлов.

Еще большая часть проблемы – в том, что уязвимость на процессоре T2 неисправима, поскольку она аппаратная. Короче, если все так ужасно (а обещают, что это еще не все новости), то владельцам текущих Mac теперь можно посоветовать не оставлять свои компьютеры без присмотра в обозримом будущем. Apple пока что не комментирует эту проблему, и интересно, смогут ли каким-то софтверным апдейтом хотя бы уменьшить вероятность успешной атаки с использованием этих уязвимостей…» ***(Александр Пацай. Джейлбрейк T2 // Компьютерное Обозрение (https://ko.com.ua/dzhejlbrejk_t2_134786). 07.10.2020).***

***

«Компания Eset обнаружила APT-группу, которая, по меньшей мере, с 2011 г. похищает конфиденциальные документы государственных учреждений в странах Восточной Европы и Балканского полуострова. Деятельность группы, которая получила название XDSpy, оставалась практически незамеченной в течение девяти лет. Среди целей киберпреступников – государственные учреждения, в том числе военные организации, министерства иностранных дел, и частные компании.

Для компрометации своих целей операторы XDSpy используют фишинговые электронные письма разного типа. Некоторые вредоносные письма содержат вложение, которым, как правило, является архив в формате ZIP или RAR, а другие – ссылку на ZIP-архив с файлом LNK без каких-либо документов-приманок. Когда

жертва дважды щелкает на файл, LNK загружает дополнительный сценарий, который устанавливает XDDown – основной компонент вредоносной программы.

В конце июня киберпреступники расширили свою вредоносную деятельность, начав использовать уязвимость в Internet Explorer – CVE-2020-0968, заплатка на которую была выпущена в апреле. Вместо архива с файлом LNK командный сервер (C&C) уже отправлял RTF-файл, при открытии которого загружался HTML-файл, использовавший вышеупомянутую уязвимость». ***(Преступная киберргруппа XDSpy 9 лет скрытно атаковала госучреждения Восточной Европы // Компьютерное Обозрение (https://ko.com.ua/prestupnaya_kibergruppa_xdspy_9_let_skrytno_atakovala_gosuchrezhdeniya_vostochnoj_evropy_134778). 07.10.2020).***

***

«В прошлом месяце, в журнале Information Systems Research вышла статья, в которой её авторы из Делавэрского университета проводит интригующую параллель между опасностью взлома компаний и степенью проявляемой ими социальной ответственности.

«Новые факты свидетельствуют, что хакерское сообщество неоднородно, и, по крайней мере, некоторые хакеры, похоже, мотивированы тем, что им не нравится, а не исключительно финансовой выгодой, — пишет один из авторов, профессор Джон Д'Арси (John D'Arcy). — Недавние взломы Всемирной организации здравоохранения из-за её действий (или предполагаемого бездействия), связанных с пандемией COVID-19, являются показательным примером».

Согласно Д'Арси, компании, пытающиеся создать видимость социальной ответственности, не внедряя такие практики во всю свою организацию, с большей вероятностью столкнутся с проблемами со стороны взломщиков. Хакеры всех мастей — от недовольных сотрудников до внешних групп хактивистов — как показало исследование, особенно резко реагируют на «показуху» если та служит не просто улучшению имиджа компании, но маскировке её плохой социальной ответственности.

В качестве примера такой показушной компании Д'Арси приводит Walmart. Широко известная своей благотворительностью и программами защиты окружающей среды, Walmart критикуется за низкий уровень заработной платы и за отсутствие внимания к физическим и психологическим условиям труда персонала

"В эту эпоху повышенной информационной прозрачности и больших социальных ожиданий от фирм, участие только в периферийных действиях может привести к негативной реакции заинтересованных сторон, — считает Д'Арси. Компаниям, по его мнению, следует с осторожностью подходить к рекламированию корпоративных социальных инициатив, если они не готовы показать, что эти действия имеют подлинную мотивацию и распространяются на ключевые аспекты их бизнеса». ***(Хакеры выбирают компании, имитирующие социальную ответственность // Компьютерное Обозрение (https://ko.com.ua/hakery_vybirayut_kompanii_imitiruyushhie_socialnuyu_otvetstvennost_134737). 02.10.2020).***

***

«Emotet теперь принимает участие в президентских выборах в США в 2020 году с новой спам-кампанией, выдавая себя за инициативу Team Blue от Демократического национального съезда.

Когда банда Emotet рассылает спам, их основная цель - убедить получателей открыть прикрепленный вредоносный документ. Обычно это делается с помощью тем электронной почты, которые представляют собой отгрузочные документы, счета-фактуры, квитанции об оплате и голосовые сообщения.

Известно, что во время праздников или крупных политических событий Emotet рассылает электронные письма с более сложной тематикой, чтобы убедить пользователей открыть вложения. Эти электронные письма включают приглашения на праздничные вечеринки или даже на демонстрацию Греты Тунберг.

После открытия вложений и включения макросов вредоносная программа Emotet будет установлена на компьютер. Затем он украдет ваши электронные письма и использует ваш компьютер для дальнейшей рассылки спама.

В конечном итоге Emotet установит другие вредоносные программы, такие как TrickBot или QakBot, которые могут привести к атаке программ-вымогателей в вашей сети.

Emotet пытается извлечь выгоду из выборов 2020 года

Спустя всего несколько дней после первых президентских дебатов злоумышленники, стоящие за Emotet, изрыгают новую спамерскую кампанию, якобы исходящую от DNC.

Эта новая кампания якобы исходит из инициативы Демократической партии «Team Blue Take Action», в которой просят добровольцев помочь демократам избраться на выборах 2020 года…

Согласно ProofPoint, который обнаружил эту новую кампанию Emotet, в спам-письмах используются такие темы, как «Team Blue Take Action», «Valanters 2020», «Список работ» и «Волонтер».

Названия вредоносных документов также совпадают с тематикой добровольцев и включают такие имена файлов, как «Team Blue Take Action.doc», «List of works.doc», «Valanters 2020.doc» и «Volunteer.doc».

При открытии прикрепленные документы будут делать вид, что они созданы на устройстве iOS, и предлагать вам «Включить контент» для правильного просмотра.

Однако после того, как вы включите контент, будут запущены вредоносные макросы, которые загрузят и установят троян Emotet на ваш компьютер.

В случае успеха троянец будет спокойно работать в фоновом режиме, используя ваш компьютер для дальнейшей рассылки спама и загрузки других вредоносных программ на ваш компьютер…». ***(Lawrence Abrams. Emotet malware takes part in the 2020 U.S. elections // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/emotet-malware-takes-part-in-the-2020-us-elections/). 02.10.2020).***

***

«Исследователи обнаружили изощренный, невероятно хорошо оснащенный APT, который участвует в широкомасштабных кампаниях по шпионажу и дезинформации.

Группа кибершпионажа, известная как BAHAMUT, была связана с «ошеломляющим» количеством продолжающихся атак на государственных чиновников и частных лиц на Ближнем Востоке и в Южной Азии, а также участвовала в широкомасштабных кампаниях по дезинформации.

Это согласно исследователям BlackBerry, которые заявили, что группа с большим количеством ресурсов, вероятно, действует на корыстной основе, предлагая свои услуги тому, кто больше заплатит.

«BAHAMUT стоит за рядом чрезвычайно целенаправленных и продуманных фишинговых кампаний по сбору учетных данных, сотнями новых образцов вредоносного ПО для Windows, использованием эксплойтов нулевого дня, тактикой анти-криминалистики / уклонения от антивирусных программ и многим другим, - сказал Эрик Милам, вице-президент исследовательских операций BlackBerry, в отчете, опубликованном в среду.

Он добавил: «Они полагаются на вредоносное ПО как на последнее средство, хорошо разбираются в фишинге, имеют тенденцию нацеливаться на мобильные телефоны конкретных людей как путь в организацию, проявляют исключительное внимание к деталям и, прежде всего, терпеливы - они были известно, что они следят за своими целями и в некоторых случаях ждут год или больше ».

Исследователи также обнаружили, что BAHAMUT использует множество фейковых новостных сущностей - от мошенников в социальных сетях до управления целыми новостными веб-сайтами, которые содержат дезинформацию.

«Изощренность и масштаб злонамеренных действий, которые наша команда смогла связать с BAHAMUT, ошеломляют», - сказал Милам.

По словам исследователей, BAHAMUT - в арабских преданиях название морского чудовища, обеспечивающего опорную структуру, удерживающую землю, - в основном занимается классической шпионской деятельностью.

Мобильные и фишинговые кибератаки

Несмотря на то, что компания распространяет нестандартное вредоносное ПО для Windows и использует различные программы нулевого дня, группа, в частности, недавно обратилась к мобильным устройствам: в отчете были обнаружены девять вредоносных приложений для iOS, которые были доступны в Apple App Store, а также ряд приложений для Android, которые, по словам BlackBerry, «напрямую являются приписывается» BAHAMUT на основании уникальных отпечатков пальцев.

«В приложениях были хорошо продуманные веб-сайты, политики конфиденциальности и письменные условия обслуживания, которые часто игнорируются злоумышленниками, что помогло им обойти меры безопасности, установленные как Google, так и Apple», - заявили исследователи.

На самом деле приложения функционировали как бэкдоры, а возможности шпионажа варьировались от выборки. Все они имели возможность перечислять типы файлов на устройствах и загружать любой потенциально интересующий файл. По словам исследователей, другие функции включали возможность

перечисления информации об устройстве, доступа к контактам, доступа к записям вызовов, доступа к SMS-сообщениям, записи телефонных звонков, записи звука, записи видео, загрузки и обновления бэкдора и отслеживания местоположения по GPS.

Они добавили, что некоторые из целей для мобильных приложений были специфичны для Объединенных Арабских Эмиратов (загрузки были привязаны к региону ОАЭ); Кроме того, они наблюдали за заявлениями, посвященными Рамадану, и заявлениями, относящимися к сикхскому сепаратистскому движению.

Фишинг - это еще одна часть основной компетенции группы, и его методы уникальны.

«Торговля фишингом и сбором учетных данных у BAHAMUT значительно лучше, чем у большинства других широко известных APT-групп», - отметили в компании. «Это главным образом связано с быстротой работы группы, ее приверженностью одноразовой и сильно разобщенной инфраструктуре, а также их способностью адаптироваться и изменяться, особенно когда их фишинговые инструменты раскрываются».

Исследователи отметили, что фишинговые упражнения, которые группа выполняет для сбора учетных данных, происходят только после «согласованных и надежных разведывательных операций», направленных на очень точные цели.

BAHAMUT также поддерживает новую фишинговую инфраструктуру на постоянной основе, при этом целевые операции целевого фишинга длятся от нескольких часов до нескольких месяцев, в зависимости от домена и уровня успешности.

«Это стремление к постоянно меняющейся инфраструктуре делает обнаружение в реальном времени практически невозможным», - говорится в отчете.

Поддельные сайты для атак и дезинформации

По мнению исследователей, в дополнение к своим более традиционным усилиям, BAHAMUT также отличается использованием оригинальных, тщательно созданных веб-сайтов, приложений и персонажей для проведения кибератак, а также распространения фейковых новостей и дезинформации.

Было замечено, что десятки поддельных сайтов обслуживают вредоносное ПО или эксплойты; в то время как другие были связаны с фишинговыми серверами BAHAMUT или выступали в качестве командно-управляющих доменов для бэкдоров BAHMAUT.

Что касается дезинформации, то некоторые из выявленных исследователями поддельных веб-сайтов напрямую связаны с общей темой: сикхским референдумом 2020 года, который с конца прошлого года является рассадником в Индии. По сути, это сепаратистское движение, детище организации под названием «Сикхи за справедливость» (SFJ), которая была запрещена правительством Индии в июле 2019 года.

В некоторых случаях создавались учетные записи в социальных сетях, на которые ссылались новостные сайты, чтобы они казались более законными.

Один сайт, названный Techsprouts, когда-то был легальным сайтом новостей в области технологий, которым управлял журналист из Индии, но сейчас он не существует. Его цель заставляла исследователей ломать голову.

«Группа взяла на себя домен того, что изначально было новостным веб-сайтом по информационной безопасности, и начала распространять контент, посвященный геополитике, исследованиям, отраслевым новостям и другим группам взлома по найму», - говорится в отчете - вместе с новостями о брокерах эксплойтов. как NSO Group.

«В течение прошлого года… BAHAMUT, похоже, перерегистрировал домен Techsprouts и продолжил управлять им», - говорится в отчете, в котором добавлено, что новый сайт имеет внушительный список «участников».

«Их биографии впечатляют, но при дальнейшем изучении становится очевидным, что миниатюрные фотографии каждого автора, которые можно увидеть на сайте, были заимствованы с других сайтов и у других людей с совершенно другими именами», - поясняется в отчете. «Например, образ Элис Джейн, старшего писателя, на самом деле был изображением Джули Лак, вечерней ведущей местной станции CBS в Гринсборо, Северная Каролина».

В этом случае контент не является явно поддельным или злонамеренным, и исследователи задаются вопросом, какова его цель.

«[Другие исследователи] утверждали, что группа использовала подобные сайты (но не специально для Techsprouts) как способ определить привычки кликов у своих целей», - говорится в отчете. «BlackBerry не может подтвердить эту теорию, хотя она определенно кажется вполне вероятной».

Хакеры по найму

В целом группа использует широкий спектр инструментов, тактик и техник (ДТС), и исследователи заявили, что «по крайней мере один разработчик нулевого дня отражает уровень навыков, превышающий уровень большинства других известных сегодня групп злоумышленников» - все это предполагает что группа очень хорошо финансируется и обеспечена хорошими ресурсами.

Об этом также свидетельствует поразительно хорошая операционная безопасность BAHAMUT (OpSec). Примечательно, что в текущих торговых процессах группы нет перекрестного перехода между доменами или IP-адресами между операционными функциями.

«Например, мы обнаружили, что никакие домены или IP-адреса, используемые для контроля или распространения вредоносных программ Windows, не используются для фишинга или администрирования вредоносных программ, предназначенных для любой другой операционной системы», - говорится в отчете. «Точно так же редко когда какой-либо отдельный сервер используется более чем для одного мобильного приложения в любой момент времени. BAHAMUT гарантирует, что ни один хостинг-провайдер не используется слишком активно, и распространяет свою текущую активную инфраструктуру на более чем 50 различных хостинг-провайдеров, тем самым обеспечивая непрерывность работы в случае выявления какой-либо отдельной кампании или раскрытия набора образцов вредоносного ПО. Это, вероятно, занимает очень много времени, дорого и требует значительного внимания к деталям».

Что касается виктимологии, то помимо несколько сгруппированных таргетингов в Южной Азии и на Ближнем Востоке, цели охватывают широкий спектр с точки зрения политической идеологии, что подтверждает теорию «хакера по найму» - таргетинг «повсюду», по мнению исследователей.

Изучая сходства на основе кода и уникальные сходства на основе строк, исследователи заявили, что смогли соединить точки между теневыми, «нераскрытыми» инцидентами APT, которые наблюдались на протяжении многих лет.

«BAHAMUT использует общедоступные инструменты, имитирует другие группы угроз и часто меняет свою тактику, что в прошлом затрудняло атрибуцию», - говорят исследователи. «Однако BlackBerry с большой уверенностью сообщает, что группа угроз стоит за эксплойтами, исследованными более чем 20 различными компаниями по обеспечению безопасности и некоммерческими организациями».

В частности, группы угроз, идентифицированные как EHDevel, Windshift, Urpage и White Company, а также неназванная группа угроз в исследовании Kaspersky «InPage нулевого дня» 2016 года.

В целом, учитывая обширные возможности, связи с разрозненной APT-деятельностью, связанной с национальным государством, и отсутствие целенаправленного таргетинга, исследователи пришли к выводу, что BAHAMUT - это одна разросшаяся группа, которая продает услуги тому, кто предлагает самую высокую цену, включая правительства.

«Операционная безопасность будет приобретать все большее значение, поскольку все больше и больше разведывательных функций передается на аутсорсинг правительствами, корпорациями и частными лицами таким группам, как БАХАМУТ», - говорится в отчете. «Эти третьи стороны добавляют уровень правдоподобного отрицания для тех, кто их нанимает». ***(Tara Seals. BAHAMUT Spies-for-Hire Linked to Extensive Nation-State Activity // Threatpost (https://threatpost.com/bahamut-spies-nation-state/159925/). 07.10.2020).***

***

«Хакери кібер-угруповання Kimsuky з Північної Кореї вчинили атаку на військові підприємства України, Росії, Туреччини та Словаччини. Турецькі фахівці розповіли, що шахраї створили підроблену сторінку авторизації в поштовому сервісі Outlook…

Угруповання Kimsuky ще відоме під назвами Velvet Chollima і Black Banshee. З 2010 року кібершахраї періодично здійснюють атаки на важливі об’єкти військової та оборонної промисловості. Спочатку злочинці здійснювали атаки тільки на об’єкти на території Південної Кореї, але пізніше расширили географію.

Цього разу кібератака велась на військові організації в сфері виробництва артилерійської техніки і бронетехніки в Україні, Росії, Словаччини, Туреччині та Південній Кореї. Сервіс Outlook використовується співробітниками компаній для доступу, хакери спробували заволодіти даними для входу в робочу пошту.

Керівник відділу дослідження складних загроз компанії Group-IB Анастасія Тихонова розповіла, що ще навесні кіберзлочинці здійснювали шкідливі розсилки,

в тому числі через соцмережі. Головною метою були дані аерокосмічних і оборонних компаній.

«Судячи з доступних в інтернеті документів, в атаках використовувався цілеспрямований фішинг (шахрайські розсилки). Наприклад, при атаці на турецького виробника військової техніки хакери навіть створили підроблену сторінку авторизації в поштовому сервісі Outlook, яким користувалися співробітники компанії, щоб отримати їх дані для входу в робочу пошту», – уточнюється в повідомленні.

Експерт з кібербезпеки «Лабораторії Касперського» Денис Легеза пояснив, що угруповання хакерів з Північної Кореї стали використовувати в своїх документах-принадах дані про вакансії в аерокосмічній і оборонній галузях.

Можна припустити, що тепер кіберзлодії зацікавлені в промисловому шпигунстві, тоді як раніше вони робили спроби кібершпіонажу, пов'язані з політикою, або комерційними проектами.

З початку року СБУ вдалося нейтралізувати 460 кібератак і припинити діяльність 20 хакерських угруповань. Були попереджені спроби нападу на органи державної влади та критично важливі об'єкти інфраструктури.

Хакери систематично проводять атаки на японські компанії, залучені до розробки вакцини від коронавируса починаючи з квітня. Головне підозра впала на Китай…». ***(Хакери з Північної Кореї атакували військові підприємства України та РФ // UA.NEWS (https://ua.news/ua/hakery-iz-severnoj-korei-atakovali-voennye-predpriyatiya-ukrainy-i-rf/). 19.10.2020).***

***

«Хакеры из группы The Black Pirate взломали сайт парламента Киргизии. Они требуют 10 тысяч долларов в качестве выкупа за оказавшуюся в их распоряжении базу данных…

"Сециалисты разбираются с проблемой и намерены закрыть сайт", — рассказал он.

Вместе с тем на сайте парламента после кибератаки появилось сообщение, что он взят под контроль группой The Black Pirate.

"Логины и пароли, личные данные, номера телефонов, а также еще несколько государственных сайтов находятся под нашим контролем.

У нас имеется база данных граждан Киргизии. Во избежание продажи личных данных, просим отправить 10 тысяч долларов", — говорится в сообщении.

Представитель парламента со своей стороны заявил, что платить хакерам администрация сайта не намерена.

"Это не вирус, а конкретные люди работали над взломом сайта. Ни о каком выкупе речи быть не может. С донорами у нас разработан проект по модернизации сайта. После случившегося мы намерены полностью его закрыть и разработать новый", — сказал собеседник агентства.

Ранее ЦИК Киргизии предложил провести повторные выборы 20 декабря». ***(Хакеры взломали сайт парламента Киргизии и потребовали выкуп // Каспаров.Ru (https://www.kasparov.ru/material.php?id=5F8D6F40097DC). 19.10.2020).***

***

«FIN11, финансово мотивированная хакерская группа, история которой началась по крайней мере с 2016 года, адаптировала вредоносные почтовые кампании для перехода на программы-вымогатели в качестве основного метода монетизации.

Группа занимается крупномасштабными операциями, в последнее время ориентируясь на компании в основном в Северной Америке и Европе практически из всех секторов промышленности, чтобы украсть данные и развернуть программу-вымогатель Clop.

Вредоносные кампании в ранней истории банды были сосредоточены на организациях в финансовом, розничном и ресторанном секторах. За последние пару лет атаки FIN11 стали более неизбирательными как с точки зрения типа жертвы, так и с точки зрения географии.

Начиная с августа киберпреступники атаковали организации в сфере обороны, энергетики, финансов, здравоохранения / фармацевтики, права, телекоммуникаций, технологий и транспорта.

Исследователи безопасности из Mandiant от FireEye сообщили BleepingComputer, что FIN11 нацелился на своих жертв с помощью вредоносных писем, распространяющих загрузчик вредоносных программ, которые они отслеживают как FRIENDSPEAK.

Они использовали различные приманки, такие как документы о денежных переводах, доставка счетов-фактур или конфиденциальная информация о бонусах компании с вредоносными HTML-вложениями для загрузки контента (iframe или встраиваемых тегов) с вероятного взломанного веб-сайта, часто с устаревшим контентом, указывающим на отказ.

Кимберли Гуди, старший менеджер по анализу в Mandiant Threat Intelligence, сообщила нам, что жертвы должны были выполнить проверку CAPTCHA, прежде чем им была предоставлена электронная таблица Excel с вредоносным кодом макроса.

После выполнения код доставил FRIENDSPEAK, который загрузил MIXLABEL, еще одно вредоносное ПО, которое, как считается, специфично для FIN11. Последний во многих случаях был настроен для связи с доменом управления и контроля, который выдавал себя за Microsoft Store (us-microsoft-store [. [Com)

Эта тактика была активна в кампаниях с сентября, хотя актер изменил макросы в документах Office, а также добавил методы геозон, сказал Гуди по электронной почте.

Mandiant сегодня опубликовал обзор деятельности FIN11 и ее перехода на сцену вымогателей. Исследователи рассматривают группу как отдельного субъекта угрозы, отмечая ее значительное совпадение в тактике, методах и вредоносных программах, используемых TA505.

TA505 - еще одна известная банда киберпреступников, использующая вымогатель Clop. Недавно он начал использовать критическую уязвимость

ZeroLogon в Windows, чтобы получить права администратора для контроллера домена организации.

Различие между двумя участниками основано на наблюдаемой активности и «развивающемся арсенале тактик, техник и процедур после компромисса (TTП), о которых не сообщалось публично в TA505».

FIN11 также использует FlawedAmmyy, загрузчик вредоносных программ, замеченный в атаках TA505 и Silence, группы хакеров, нацеленных на банки по всему миру. Это означает, что у всех трех групп есть общий разработчик вредоносных программ.

Несмотря на сильное сходство с TA505, отнести определенные кампании к FIN11 сложно, поскольку обе группы используют вредоносное ПО и поставщиков криминальных услуг, что в некоторых случаях могло привести к неправильной атрибуции.

Mandiant отслеживает FIN11 с 2016 года и определяет его по наблюдаемой активности, которую они могут проверить независимо. TA505 существует по крайней мере с 2014 года, и исследователи не связывают его первые операции с FIN11.

Тактика зарабатывания денег

Отвечая на инциденты, когда FIN11 сбрасывал вымогатель Clop, Mandiant обнаружил, что злоумышленник не покинул цель после потери доступа.

В одном случае через несколько месяцев они повторно скомпрометировали организацию с помощью нескольких кампаний по электронной почте. В другом случае FIN11 восстановил доступ после того, как компания восстановила зараженные серверы из резервных копий.

Исследователи не указывают требования FIN11 о выкупе в связи с расследованными инцидентами, но отмечают, что компания Coveware, занимающаяся восстановлением программ-вымогателей, указывает суммы от нескольких сотен тысяч до 10 миллионов долларов.

По словам Mandiant, в одном случае, когда они не развернули программу-вымогатель Clop, актер попытался вымогать у жертвы, угрожая раскрыть или продать украденные данные.

Актер из СНГ

Основываясь на своем анализе, исследователи имеют умеренную уверенность в том, что FIN11 действует на территории Содружества Независимых Государств (СНГ - страны бывшего Советского Союза).

В пользу этой оценки говорят метаданные файлов на русском языке, развертывание программы-вымогателя Clop только на компьютерах с раскладкой клавиатуры, используемой за пределами стран СНГ, а также снижение активности во время русского Нового года и православных рождественских праздников.

Mandiant считает, что FIN11 имеет «доступ к сетям гораздо большего числа организаций, чем они могут успешно монетизировать», и выбирает, стоит ли эксплуатация усилий, исходя из местоположения жертвы, ее географического положения и уровня безопасности.

Поскольку кража данных и вымогательство теперь являются частью их методов монетизации, FIN11, вероятно, проявит больший интерес к жертвам, у

которых есть конфиденциальные проприетарные данные, у которых есть более высокие шансы заплатить выкуп либо за восстановление своих файлов». ***(Ionut Ilascu. FIN11 hackers jump into the ransomware money-making scheme // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/fin11-hackers-jump-into-the-ransomware-money-making-scheme/). 14.10.2020).***

***

«…Злоумышленники Ryuk снова нанесли удар, всего за пять часов перейдя от отправки фишингового письма к полному шифрованию в сети жертвы.

По словам исследователей, такая головокружительная скорость частично является результатом того, что банда использовала ошибку повышения привилегий Zerologon (CVE-2020-1472), менее чем через два часа после первоначального фишинга.

Согласно Microsoft, уязвимость Zerologon позволяет злоумышленнику, не прошедшему проверку подлинности и имеющему сетевой доступ к контроллеру домена, полностью скомпрометировать все службы идентификации Active Directory. Он был исправлен в августе, но многие организации остаются уязвимыми.

В этой конкретной атаке после того, как злоумышленники повысили свои привилегии с помощью Zerologon, они использовали различные стандартные инструменты, такие как Cobalt Strike, AdFind, WMI и PowerShell, для достижения своей цели, согласно анализу исследователей в отчете DFIR, опубликованном в воскресенье.

Атака начинается

По словам исследователей, атака началась с фишингового письма, содержащего версию загрузчика Bazar. Оттуда злоумышленники выполнили базовое сопоставление домена с помощью встроенных утилит Windows, таких как Nltest. Однако им нужно было расширить свои привилегии, чтобы нанести какой-либо реальный ущерб, поэтому они использовали недавно обнаруженную уязвимость Zerologon, говорят исследователи.

Согласно анализу, получив повышенные права администратора, киберпреступники смогли сбросить машинный пароль основного контроллера домена.

Затем они перешли на дополнительный контроллер домена, выполняя больше операций по обнаружению домена через сеть и модуль PowerShell Active Directory.

«Оттуда злоумышленники, похоже, использовали на сервере модуль повышения привилегий именованного канала по умолчанию», - говорят исследователи. «На этом этапе злоумышленники использовали [протокол удаленного рабочего стола] RDP для подключения вторичного контроллера домена к первому контроллеру домена, используя встроенную учетную запись администратора».

Кобальтовый удар

По словам исследователей, боковое перемещение было инициировано посредством выполнения Server Message Block (SMB) и Windows Management

Instrumentation (WMI) маяков Cobalt Strike. SMB - это сетевой протокол обмена файлами, включенный в Windows 10, который обеспечивает возможность чтения и записи файлов на сетевые устройства. Между тем WMI позволяет управлять данными и операциями в операционных системах на базе Windows.

Cobalt Strike принадлежит к группе инструментов двойного назначения, которые обычно используются как для задач эксплуатации, так и для задач после эксплуатации. Другие находящиеся в обращении примеры включают PowerShell Empire, Powersploit и Metasploit, согласно недавним исследованиям Cisco.

«Из анализа памяти мы также смогли сделать вывод, что актеры использовали пробную версию Cobalt Strike со строкой EICAR, присутствующей в конфигурации сети для маяка. Использовались как переносимые исполняемые файлы, так и DLL-маяки», - добавили исследователи.

На главном контроллере домена был сброшен и запущен еще один маяк Cobalt Strike.

Анализ атаки показал, что примерно через четыре часа 10 минут банда Рюка перешла с основного контроллера домена, используя RDP для подключения к резервным серверам.

«Затем с помощью AdFind была проведена дополнительная проверка домена. Как только это будет завершено... участники угроз были готовы к достижению своей конечной цели», - говорится в отчете DFIR.

Пять часов спустя: Рюк

На заключительном этапе атаки операторы Ryuk сначала развернули исполняемый файл программы-вымогателя на серверах резервного копирования. После этого вредоносная программа была сброшена на другие серверы среды, а затем и на рабочие станции.

Ryuk - очень активная вредоносная программа, ответственная за ряд недавних атак, в том числе за громкую атаку, в результате которой была остановлена компания Universal Health Services (UHS), которая входит в список Fortune-500 и является владельцем общенациональной сети больниц.

«Злоумышленники завершили свою задачу, запустив программу-вымогатель на основном контроллере домена, и через пять часов атака завершилась», - говорят исследователи.

Использование Zerologon значительно упростило действия киберпреступников, поскольку атака не должна была быть нацелена на пользователя с высокими привилегиями, у которого, вероятно, будет больше средств контроля безопасности.

Фактически, самой сложной частью кампании было начало атаки - успешная установка Bazar из первоначального фишингового письма, что потребовало взаимодействия с пользователем. Исследователи отмечают, что пользователь был пользователем домена и не имел никаких других разрешений, но благодаря Zerologon это оказалось не проблемой.

Атака показывает, что организации должны быть готовы действовать быстрее, чем когда-либо, в ответ на любую обнаруженную вредоносную активность.

«Вы должны быть готовы к действию менее чем за час, чтобы убедиться, что вы можете эффективно уничтожить исполнителя угрозы», - считают исследователи.

Всплеск атак зерологона

Данный пример представляет собой всплеск попыток эксплуатации Zerologon. Правительственные чиновники на прошлой неделе предупредили, что передовые постоянные угрозы (APT) теперь используют ошибку для нацеливания на системы поддержки выборов.

Это произошло всего через несколько дней после того, как Microsoft забила тревогу о том, что иранское национальное государство активно использовало уязвимость (CVE-2020-1472). APT - это MERCURY (также известный как MuddyWater, Static Kitten и Seedworm). И, исследователи Cisco Talos также недавно предупреждали о спайке в попытках эксплуатации против Zerologon…» ***(Tara Seals. Ryuk Ransomware Gang Uses Zerologon Bug for Lightning-Fast Attack // Threatpost (https://threatpost.com/ryuk-ransomware-gang-zerologon-lightning-attack/160286/). 19.10.2020).***

***

«Иранская хакерская группа нацелена на университеты 12 стран.

Кампания Silent Librarian возобновилась на осенней школьной сессии, активно нацеливаясь на студентов и преподавателей университетов с помощью целевых фишинговых кампаний.

Группа угроз (также известная как TA407 и Cobalt Dickens), действующая за пределами Ирана, с начала 2019 учебного года активно рассылает мелкие, узконаправленные, социально спроектированные электронные письма, которые в конечном итоге обманывают жертв. передача их учетных данных. По словам исследователей, цель состоит в том, чтобы собрать не только логины для продажи в Интернете, но и собственные исследования и данные университетов.

Электронные письма обычно маскируются под сообщения из университетских библиотечных систем или других отделений университетского городка. В течение последнего учебного года кибератаки отточили свои усилия и начали использовать сокращенные URL-ссылки в своих фишинговых письмах, что затрудняет обнаружение перенаправления жертв на целевую страницу, размещенную злоумышленником. Злоумышленники также обновили свои целевые страницы с помощью новых баннеров для конкретных университетов, основанных на погодных предупреждениях или уведомлениях о чрезвычайных ситуациях, чтобы они выглядели более аутентично.

Теперь эта APT-группа возвращается в школу с новой кампанией, которая, похоже, нацелена на учреждения по всему миру, согласно анализу Malwarebytes во вторник. Цели охватывают дюжину стран и на данный момент включают: Университет Аделаиды в Австралии; Глазго Каледониан, Кентский университет, Йоркский университет, Королевский колледж Лондона, Кембридж и другие в Великобритании; Университет Торонто и Макгилла в Канаде; и Университет Стоуни Брук, Университет Северного Техаса и другие в США

Методика работы, применявшаяся в прошлом году, остается в силе: Silent Librarian размещает серию фишинговых сайтов, которые созданы для имитации законных университетских доменов. Например, электронные письма, якобы отправленные из библиотеки Университета Аделаиды, направляли жертв на URL-адрес «library.adelaide.crev [точка] me», который очень близок к законному домену «library.adelaide.edu.au» школы..

«Многие из них были выявлены и устранены, [но] злоумышленник собрал достаточно из них, чтобы продолжить успешную кампанию против сотрудников и студентов», - говорится в анализе. «Очевидно, что мы раскрыли лишь небольшую часть этой фишинговой операции. Хотя по большей части сайты блокируются быстро, злоумышленник имеет преимущество в том, что он на шаг впереди и атакует сразу несколько возможных целей ».

APT использует сеть доставки контента Cloudflare для размещения большинства фишинговых имен хостов, чтобы скрыть реальное происхождение хостинга.

«Однако с некоторой внешней помощью нам удалось идентифицировать часть их инфраструктуры, расположенную на иранских хостах», - отмечают исследователи. «Злоумышленнику может показаться странным использовать инфраструктуру в своей стране, возможно, указывая на нее пальцем. Однако здесь он просто становится еще одним надежным вариантом хостинга из-за отсутствия сотрудничества между правоохранительными органами США или Европы и местной полицией в Иране»…». ***(Tara Seals. Silent Librarian Goes Back to School with Global Research-Stealing Effort // Threatpost (https://threatpost.com/silent-librarian-school-research-stealing/160099/). 14.10.2020).***

***

«Исследователи безопасности из ИБ-компаний Profero и ClearSky сообщили о предотвращении вредоносной кампании, организованной иранскими хакерами. Масштабная хакерская операция, получившая название Operation Quicksand, была нацелена на «крупные израильские организации».

Согласно отчету, хакерская группировка MuddyWater отправляла израильским организациям вариант вредоносного ПО PowGoop (вредоносная замена DLL-библиотеки обновлений Google). PowGoop представляет собой загрузчик для вымогателя Thanos с разрушительными возможностями.

Эксперты определили два основных вектора атаки:

• Первый вектор предполагал отправку вредоносного документа (PDF или Excel), который обменивался данными через OpenSSL с C&C-сервером киберпреступников и загружал файлы для дальнейшего развертывания полезной нагрузки PowGoop;

• Второй вектор предполагал использование уязвимости CVE-2020-0688 в Microsoft Exchange и развертывание той же полезной нагрузки через файл aspx (WebShell). Злоумышленник создавал внутренний сокет-туннель между скомпрометированными устройствами в сети. Для этого использовался модифицированный SSF (Socket). Затем злоумышленник загружал PowGoop.

Изначально атака выглядела так, словно злоумышленники хотели получить выкуп, однако «настоящей их целью была не кража данных, а нанесение ущерба». MuddyWater (также известная как Static Kitten) сосредоточена исключительно на кибершпионаже и атаках на правительственные структуры.

Как ранее сообщила Microsoft, MuddyWater также использовала уязвимость ZeroLogon (CVE-2020-1472).» ***(Иранская группировка MuddyWater атаковала крупные израильские организации // SecurityLab.ru (https://www.securitylab.ru/news/513162.php). 19.10.2020).***

***

«Білоруське угрупування хакерів Кіберпартізани 26 жовтня заблокувало сайт Національного банку Білорусі. Нацбанк не приєднався до загальнонаціонального страйку, який оголосила опозиціонер Світлана Тихановська.

Про кібератаку хакери написали у соціальних мережах. Вони стверджують, якщо установа не хоче підтримати народний страйк, то вони переконають її приєднатися.

– Нацбанк не дуже хотів приєднуватися до народного страйку. Ми їх переконали, – йдеться в повідомленні.

В період з 12.45 до 15.00 інтернет-користувачі сайту Нацбанку не могли отримати доступ до нього. З'ясувалося, що це була зовнішня DDoS атака. Уповноважені органи вже працюють над вирішенням проблем.

Станом на 17.30, доступу до офіційного сайту Національного банку Білорусі немає.

Термін ультиматуму закінчився: у Білорусі розпочався загальнонаціональний страйк

26 жовтня у Білорусі розпочався протест робітників на найбільших підприємствах, до якого раніше закликала екс-кандидат у президенти країни Світлана Тихановська.

13 днів тому Тихановська оголосила ультиматум, згідно з яким невизнаний США, ЄС і Україною президент Олександр Лукашенко повинен був оголосити про відхід, зупинити жорстокі затримання учасників протестів у Білорусі та відпустити політв'язнів. Але Лукашенко його проігнорував». ***(Хакери заблокували сайт Нацбанку Білорусі // ФАКТИ. ICTV (https://fakty.com.ua/ua/svit/20201026-hakery-zablokuvaly-sajt-natsbanku-bilorusi/). 26.10.2020).***

***

«Будущих хакеров в настоящее время привлекают через Telegram-каналы и хакерские форумы. После этого их обучают проведению атак. Об этом сообщает РИА Новости со ссылкой на руководителя департамента расследований инцидентов информационной безопасности Group-IB Андрея Колмакова.

«На протяжении всего 2020 года Group-IB наблюдала активный набор в преступные мошеннические сообщества. Порог входа существенно снизился: новых участников привлекают через Telegram-каналы и хакерские форумы с последующим обучением и вступительными бонусами», — сообщил Колмаков.

По его словам, в «серой зоне» тоже быстро подстроились под требования рынка: «билетная мафия» переориентировала свои ресурсы на доставку продуктов питания и лекарств по завышенным ценам.

Колмаков отметил, что рынок криминальных услуг cybercrime-as-a-service также активно развивается. В рамках него сдаются в аренду компьютерные сети, зараженные вредоносным программным обеспечением (ботнетов), организуются DDoS-атаки, рассылка фишинговых писем». ***(Анастасия Марьина. Group-IB рассказала, на каких площадках вербуют будущих хакеров // ООО РБ.РУ (https://rb.ru/news/group-ib-hackers/). 23.10.2020).***

***

«Киберпреступная группировка Maze прекращает свою вредоносную деятельность. Как сообщил один из источников издания BleepingComputer, Maze останавливает свою работу, а также прекратила шифрование новых жертв с сентября 2020 года и пытается получить от последних жертв выплаты выкупа. Преступники также начали удалять информацию о своих жертвах, которых они указали на сайте утечек данных.

По словам источников, многие филиалы Maze перешли к операторам нового вымогательского ПО под названием Egregor. Egregor начал работу в середине сентября, когда Maze прекратили свои операции. Предположительно, Egregor представляет собой то же программное обеспечение, что и Maze и Sekhmet, поскольку они используют одинаковые записки с требованиями о выкупе, одинаковые названия сайтов платежей и имеют большую часть одного и того же кода.

Группировка Maze начала работать в мае 2019 года, но активизировалась лишь в ноябре. Преступники произвели революцию в атаках программ-вымогателей, применив тактику двойного вымогательства. В декабре 2019 года они создали web-сайт, на котором были указаны последние компании-жертвы, решившие самостоятельно восстановить свои компьютерные системы без оплаты выкупа.

Метод двойного вымогательства был быстро принят другими крупными операторами вымогательского ПО, включая REvil, Clop, DoppelPaymer, которые запустили собственные сайты утечек данных. Maze продолжал развивать операции с программами-вымогателями, сотрудничая с Ragnar Locker и LockBit для обмена информацией и тактиками». ***(Операторы Maze прекращают свою киберпреступную активность // SecurityLab.ru (https://www.securitylab.ru/news/513513.php). 29.10.2020).***

***

«В начале текущей недели журналист Брайн Кребс получил от проверенного источника информацию о том, что агрессивная группировка хакеров из России, специализирующаяся на вымогательском ПО, готовится вывести из строя информационные системы в сотнях медицинских учреждений США. В среду, 28 октября, эту информацию подтвердили ФБР и Министерство внутренней безопасности США. Оба ведомства организовали

экстренный конференц-звонок с руководителями отрасли здравоохранения и предупредили их о «надвигающейся киберугрозе больницам и поставщикам медицинских услуг в США». В этот же день ФБР, Министерство внутренней безопасности и Министерство здравоохранения и социальных служб выпустило совместное предупреждение.

Менее чем за сутки до публикации предупреждения Кребс получил сообщение от основателя ИБ-компании в Милуоки Hold Security Алекса Холдена (Alex Holden). По словам Холдена, ему удалось ознакомиться с перепиской участников русскоязычной киберпреступной группировки Ryuk, в которой они обсуждали план развертывания вымогательского ПО в сетях более 400 учреждений здравоохранения на территории США.

«Они (участвовавшие в конференц-звонке ведомства – ред.) не предоставили никаких индикаторов компрометации, и их совет заключался лишь в том, чтобы “обновить свои системы и сообщать обо всем подозрительном”», – сообщил участвовавший в конференции медработник со стажем.

Однако другие участники конференции отметили, что индикаторы компрометации мало чем помогут пострадавшим от Ryuk организациям, так как для каждой отдельной жертвы операторы вредоноса используют разные инфраструктуры, начиная от загружаемых на атакуемые хосты исполняемых файлов Microsoft Windows и заканчивая C&C-серверами.

Тем не менее, ИБ-компания Mandiant опубликовала в среду список доменов и интернет-адресов, использовавшихся Ryuk (UNC1878 в классификации Mandiant) на протяжении всего 2020 года.

Пока что известно о кибератаках Ryuk только на несколько медучреждений. На этой неделе жертвами вымогательского ПО стали медцентр Sky Lakes в Орегоне и ряд больниц в округе Сент-Лоренс». ***(Операторы Ryuk планируют обрушить лавину кибератак на больницы в США // SecurityLab.ru (https://www.securitylab.ru/news/513510.php). 29.10.2020).***

***

Вірусне та інше шкідливе програмне забезпечення

«Набор вредоносных модулей MontysThree, существующий как минимум с 2018 г. и предназначенный для целевых атак на промышленные предприятия, обнаружила «Лаборатория Касперского». Он использует техники, помогающие избежать детектирования, в том числе сообщение с контрольно-командным сервером через публичные облачные сервисы и стеганографию.

Вредоносное ПО MontysThree состоит из четырех модулей. Атака начинается с распространения загрузчика с помощью фишинга через самораспаковывающиеся архивы. Названия файлов в таких архивах могут быть связаны со списками контактов сотрудников, технической документацией или результатами медицинских анализов. Загрузчик расшифровывает основной вредоносный модуль из растрового изображения со стеганографией. Для этого применяется специально разработанный алгоритм.

Основной вредоносный модуль использует несколько алгоритмов шифрования, чтобы избежать детектирования, преимущественно RSA для коммуникаций с контрольным сервером и для расшифровки конфигурационных данных. В этих основанных на формате XML данных описываются задачи зловреда: поиск документов с заданными расширениями в указанных директориях и на съемных носителях. Данная информация позволила выяснить, что операторов MontysThree интересуют документы Microsoft Office и Adobe Acrobat.

Помимо этого, модули могут снимать скриншоты рабочего стола, определять, интересна ли жертва операторам, анализируя ее сетевые и локальные настройки и т.д. Найденная информация шифруется и передается в публичные облачные сервисы (Google Drive, Microsoft Onedrive, Dropbox), через них же происходит получение новых файлов.

MontysThree также использует простой метод для закрепления в зараженной системе – панель быстрого запуска Windows Quick Launch. Пользователи, сами того не зная, запускают первичный модуль вредоносного ПО каждый раз, когда с помощью этой панели открывают легитимные приложения, например, браузеры.

Атаки с использованием инструментов MontysThree выделяются не только тем, что нацелены на промышленные предприятия (хотя это и не уникально, но они не самые популярные мишени для целевых атак), но и сочетанием продвинутых и любительских тактик и методов. Уровень технических решений в этом наборе инструментов заметно разнится. Разработчики MontysThree используют современные надежные криптографические стандарты и кастомизированную стеганографию. Уровень разработки не такой высокий, как у крупных APT-игроков, но авторы вложили много сил в создание этого набора инструментов и продолжают его развивать». ***(Вредоносный набор MontysThree создан для шпионажа против промышленных предприятий // Компьютерное Обозрение (https://ko.com.ua/vredonosnyj_nabor_montysthree_sozdan_dlya_shpionazha_protiv_promyshlennyh_predpriyatij_134824). 09.10.2020).***

***

«Компания Eset выявила признаки сотрудничества между киберпреступниками, которые распространяют семейства банковских троянов в Латинской Америке. Из-за большого количества похожих функций эти банковские трояны часто рассматривают как одну группу угроз. На самом деле среди них обнаружено по крайней мере 11 различных семейств вредоносных программ. В частности, в течение прошлого года были зафиксированы такие банковские трояны – Amavaldo, Casbaneiro, Mispadu, Guildma, Grandoreiro и Mekotio.

Исследователи Eset обнаружили большое количество признаков, которые свидетельствуют о сотрудничестве авторов вредоносного ПО. Несмотря на латиноамериканское происхождение троянов, с конца прошлого года целями киберпреступников были также пользователи Испании и Португалии.

Первым общим признаком, выявленным исследователями Eset, была идентичная реализация функционала и методов атак с помощью поддельных всплывающих окон, которые подталкивают жертв предоставить

конфиденциальную информацию. Кроме того, эти семейства вредоносов используют сторонние библиотеки, как правило, неизвестные алгоритмы шифрования строк, а также различные методы обфускации (запутывания).

Похожими также являются техники распространения вредоносного ПО. Трояны обычно проверяют наличие маркера, который указывает на заражение устройства, и загружают данные в ZIP-архивы. Кроме этого, исследователи Eset обнаружили идентичные цепи распространения, которые использовали различные компоненты и одинаковые методы выполнения.

Также разные семейства банковских троянов используют похожие шаблоны спама в своих последних кампаниях. Поскольку сходство такого количества идей в отдельных авторов вредоносного ПО маловероятна, можно сделать вывод, что несколько групп киберпреступников сотрудничают между собой». ***(Создатели банковских троянов сотрудничают для атак на пользователей // Компьютерное Обозрение (https://ko.com.ua/sozdateli_bankovskih_troyanov_sotrudnichayut_dlya_atak_na_polzovatelej_134774). 06.10.2020).***

***

«Специалисты «Лаборатории Касперского» обнаружили целевую кампанию кибершпионажа с использованием сложной модульной структуры MosaicRegressor, куда, в том числе, входит буткит для встроенной в материнскую плату микропрограммы UEFI (Unified Extensible Firmware Interface). На данный момент — это первый случай заражения UEFI при помощи специально разработанного для такого типа атак вредоносного ПО.

UEFI загружается еще до операционной системы и контролирует все процессы на «раннем старте». Отсюда и главная опасность, связанная с компрометацией этой среды: если внести изменения в код UEFI, можно получить полный контроль над компьютером. Например, изменить память, содержание диска или, как в случае с буткитом MosaicRegressor, заставить операционную систему запустить вредоносный файл. А поскольку речь идет о низкоуровневой вредоносной программе, избавиться от нее не поможет ни замена жесткого диска, ни переустановка ОС.

Этот файл представляет собой загрузчик, он связывается с сервером управления, собирает все недавние документы на компьютере, архивирует их и передает обратно на сервер. Поэтому по сути речь идет о шпионаже.

Обнаружены также другие компоненты MosaicRegressor, которые, предположительно, сбрасываются с самого сервера управления, выполняют полезную вредоносную нагрузку, а затем удаляются. Сейчас есть информация о двух жертвах буткита UEFI, а также нескольких жертвах кампании, столкнувшихся с целевым фишингом. Все они являются дипломатами, либо членами НКО, а их деятельность связана с Северной Кореей.

В ходе исследования инфраструктуры MosaicRegressor установлено также, что в основу компонентов буткита UEFI положен код Vector-EDK. Это специальный конструктор, который был создан кибергруппой Hacking Team и в том числе содержит инструкцию по созданию модуля для перепрошивки UEFI. В

2015 г. эти и другие исходники Hacking Team в результате утечки оказались в свободном доступе, что позволило злоумышленникам создать собственное ПО с минимальными усилиями: они просто дополнили исходный код вредоносным компонентом». ***(Обнаружен вредонос для шпионажа, заражающий микрокод UEFI материнской платы // Компьютерное Обозрение (https://ko.com.ua/obnaruzhen_vredonos_dlya_shpionazha_zarazhayushhij_mikrokod_uefi_materinskoj_platy_134768). 06.10.2020).***

***

«Чтобы оставаться в безопасности в Интернете, каждый должен распознавать вредоносные вложения, которые обычно используются в фишинговых письмах для распространения вредоносных программ.

Распространяя вредоносное ПО, злоумышленники создают спам-кампании, которые выдают себя за счета, приглашения, платежную информацию, информацию о доставке, электронные факсы, голосовую почту и т. Д. В эти электронные письма входят вредоносные вложения Word и Excel или ссылки на них, которые при открытии и включении макросов устанавливают вредоносное ПО на компьютер.

Однако, прежде чем Word или Excel выполнит макросы в документе, Office требует, чтобы вы нажимали кнопки «Разрешить редактирование» или «Разрешить содержимое», чего никогда не следует делать.

Чтобы обманом заставить пользователей нажимать эти кнопки, распространители вредоносного ПО создают документы Word и Excel, содержащие текст и изображения, указывающие на наличие проблемы с отображением документа. Затем он предлагает получателям щелкнуть «Включить содержимое» или «Разрешить редактирование», чтобы правильно просмотреть содержимое.

Комбинация текста и изображений в этих вредоносных вложениях называется «шаблонами документов».

Ниже приведены различные шаблоны документов, которые использовались в кампаниях по рассылке спама для некоторых из наиболее распространенных вредоносных программ.

Следует отметить, что эти шаблоны документов также могут использоваться с различными вредоносными программами, отличными от описанных ниже. Кроме того, это образец наиболее распространенных шаблонов, но существует и множество других.

BazarLoader

BazarLoader - это вредоносное ПО для предприятий, разработанное той же группой, что и троян TrickBot. После установки злоумышленники используют BazarLoader / BazarBackdoor для удаленного доступа к вашему компьютеру, который затем используется для компрометации остальной части вашей сети.

Когда сеть заражена BazarLoader, злоумышленники обычно развертывают программу-вымогатель Ryuk для шифрования всех устройств в сети.

Фишинговые электронные письма, которые распространяют BazarBackdoor через фишинговые электронные письма, обычно содержат ссылки на

предполагаемые документы Word или Excel, размещенные в Google Docs и Google Sheets.

Однако эти документы Google Docs представляют собой проблему и предлагают вам загрузить документ. Эта загрузка на самом деле является исполняемым файлом, который устанавливает BazarLoader, как показано ниже.

Дридекс

Dridex - это усовершенствованный модульный банковский троян, впервые обнаруженный в 2014 году и постоянно обновляемый.

При заражении Dridex загружает различные модули, которые можно использовать для кражи паролей, предоставления удаленного доступа к компьютеру или выполнения других вредоносных действий.

Когда Dridex компрометирует сети, это обычно приводит к развертыванию атак программ-вымогателей BitPaymer или Dridex.

Еще одна программа-вымогатель, известная как WastedLocker, также считается связанной с Dridex, но одна фирма, занимающаяся кибербезопасностью, не согласна с этими оценками.

В отличие от других кампаний по распространению вредоносных программ, банда Dridex имеет тенденцию использовать более стилизованные шаблоны документов, которые показывают небольшой или запутанный контент и предлагают вам нажать `` Включить контент '', чтобы увидеть его лучше.

Например, в шаблоне ниже указано, что документ был создан в более ранней версии Microsoft Office Word, а под ним отображается трудночитаемый документ.

Dridex также использует более стилизованные шаблоны документов, выдавая себя за информацию о доставке для DHL и UPS.

Наконец, Dridex покажет небольшие трудночитаемые счета на оплату, в которых вам будет предложено нажать «Разрешить редактирование», чтобы просмотреть их правильно.

Как видно из приведенных выше примеров, Dridex любит использовать изображения встроенных документов с логотипами компании и фирменными бланками, чтобы обманом заставить пользователей включить макросы.

Emotet

Emotet - наиболее распространенное вредоносное ПО через спам-сообщения, содержащие вредоносные документы Word или Excel. После заражения Emotet украдет электронную почту жертвы и использует зараженный компьютер, чтобы рассылать дальнейший спам получателям по всему миру.

Пользователи, зараженные Emotet, в конечном итоге будут заражены троянами, такими как TrickBot и QakBot. Оба этих трояна используются для кражи паролей, файлов cookie, файлов и компрометации всей сети организации.

В конечном итоге при заражении TrickBot сеть, скорее всего, подвергнется атаке программ-вымогателей Ryuk или Conti. Те, кто пострадал от QakBot, могут быть поражены программой-вымогателем ProLock.

В отличие от Dridex, Emotet не использует изображения реальных документов в своих шаблонах документов. Вместо этого они используют широкий спектр шаблонов, которые показывают окно с предупреждением о том, что

документ не может быть просмотрен правильно и что пользователям необходимо нажать «Включить контент», чтобы прочитать его.

Например, в шаблоне « Красный рассвет », показанном ниже, указано, что «Этот документ защищен», а затем предлагается включить содержимое, чтобы прочитать его…

QakBot

QakBot или QBot - это банковский троян, который распространяется с помощью фишинговых кампаний, доставляющих вредоносные документы Microsoft Word, как правило, предприятиям.

QakBot - это модульный троян, который может похищать банковскую информацию, устанавливать другое вредоносное ПО или предоставлять удаленный доступ к зараженной машине.

Как и другие трояны, описанные в этой статье, QakBot также вступил в партнерство с вирусом-вымогателем под названием ProLock, который обычно является финальной полезной нагрузкой атаки…

Все исполняемые вложения

Наконец, никогда не следует открывать вложения с расширениями.vbs,.js,.exe,.ps1,.jar,.bat,.com или.scr, поскольку все они могут использоваться для выполнения команд на компьютере.

Поскольку большинство почтовых сервисов, включая Office и Gmail, блокируют «исполняемые» вложения, распространители вредоносных программ будут отправлять их в архивах, защищенных паролем, и включать пароль в электронное письмо.

Этот метод позволяет исполняемому вложению обходить шлюзы безопасности электронной почты и достигать предполагаемого получателя.

К сожалению, Microsoft решила по умолчанию скрывать расширения файлов, что позволяет злоумышленникам обманом заставить пользователей запускать небезопасные файлы. В связи с этим BleepingComputer настоятельно рекомендует всем пользователям Windows включить отображение расширений файлов.

Если вы получили электронное письмо, содержащее один из этих типов исполняемых файлов, оно почти наверняка является вредоносным и должно быть немедленно удалено». ***(Lawrence Abrams. The most common malicious email attachments infecting Windows // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/the-most-common-malicious-email-attachments-infecting-windows/). 11.10.2020).***

***

«Исследователи кибербезопасности из Netlab обнаружили две новых бот-сети IoT под названием HEH и Ttint.

Netlab - это подразделение сетевых исследований китайского гиганта кибербезопасности Qihoo 360. Исследователи компании впервые обнаружили ботнет Ttint, нацеленный на маршрутизаторы Tenda, используя две уязвимости нулевого уровня.

Ttint распространяет троян для удаленного управления на основе кода вредоносной программы Mirai.

Mirai вызвала массовый хаос в 2016 году, когда поразила DNS-провайдера Dyn и повлияла на популярные сервисы, включая PayPal, Spotify, PlayStation Network, Xbox Live, Reddit, Amazon, GitHub и многие другие.

Netlab отмечает, что, хотя Mirai фокусируется на DDoS-атаках, таких как атака против Dyn, Ttint более сложна.

В дополнение к DDoS-атакам, Ttint поддерживает 12 функций удаленного управления, таких как прокси-сервер Socket5 для маршрутизаторов, вмешательство в DNS маршрутизатора, настройка iptables и выполнение пользовательских системных команд.

Ботнет также обходит обнаружение Mirai с помощью протокола WebSocket-over-TLS на уровне связи C2 и защищает себя, используя множество плавающих IP-адресов инфраструктуры.

На момент написания статьи две уязвимости нулевого дня, используемые Ttint, остаются не исправленными.

Кроме того, Netlab обнаружила еще один ботнет IoT. Он одноранговый, и исследователи назвали его HEH.

HEH написан на языке Go, и Netlab утверждает, что он использует проприетарный протокол P2P. Троян распространяется с помощью перебора Telnet на порты 23/2323 и влияет на многие архитектуры ЦП, включая x86 (32/64), ARM (32/64), MIPS (MIPS32 / MIPS-III) и PPC.

Ботнет состоит из трех модулей: модуля распространения, модуля локальной службы HTTP и модуля P2P.

В HEH девять команд, но как минимум три еще не реализованы, поскольку бот явно все еще находится в разработке:

В настоящее время наиболее полезными доступными функциями HEH являются выполнение команд оболочки, обновление списка одноранговых узлов и загрузка определенного файла, который будет использоваться в качестве данных ответа HTTP локальным сервером HTTP.

Интересно, что функция Атака в настоящее время пуста, однако вряд ли так и останется в будущем.

Оба ботнета демонстрируют растущее желание хакеров взломать устройства Интернета вещей. Неудивительно, что Интернет вещей стал такой целью, учитывая быстрое распространение подключенных устройств и их зачастую слабую безопасность». ***(Романов Роман. Исследователи кибербезопасности обнаружили две новых бот-сети в Интернете вещей // Internetua (https://internetua.com/issledovateli-kiberbezopasnosti-obnarujili-dve-novyh-bot-seti-v-internete-vesxei). 08.10.2020).***

***

«Facebook подробно рассказал о кибератаке с рекламным мошенничеством, которая продолжается с 2016 года, во время кражи учетных данных Facebook и файлов cookie браузера.

Facebook подробно описал масштабную китайскую кампанию по вредоносному ПО, которая на протяжении многих лет нацелена на его рекламную платформу и выкачивает 4 миллиона долларов из рекламных аккаунтов

пользователей. Кампания была рассмотрена группами безопасности социальных сетей после того, как она впервые стала активной.

Вредоносная программа, получившая название SilentFade (сокращение от «Тихий запуск рекламы в Facebook с использованием эксплойтов»), взламывала учетные записи Facebook и использовала их для продвижения вредоносной рекламы, кражи файлов cookie браузера и многого другого. Гигант социальных сетей заявил, что китайская кампания по вредоносному ПО началась в 2016 году, но впервые она была обнаружена в декабре 2018 года из-за подозрительного всплеска трафика на ряде конечных точек Facebook. После тщательного расследования Facebook прекратил кампанию и возбудил судебный иск против киберпреступников, стоящих за атакой в декабре 2019 года.

«Наше расследование выявило ряд интересных методов, используемых для компрометации людей с целью совершения рекламного мошенничества», - заявили Санчит Карве и Дженнифер Ургилес из Facebook в анализе, представленном в четверг на конференции Virus Bulletin 2020. «Злоумышленники в основном проводили вредоносные рекламные кампании, часто в форме рекламы фармацевтических таблеток и спама с фальшивыми одобрениями знаменитостей».

Facebook заявил, что SilentFade не был загружен или установлен с помощью Facebook или каких-либо его продуктов. Вместо этого он обычно был связан с потенциально нежелательными программами (ПНП). ПНП - это программы, которые пользователь может счесть нежелательными; они могут использовать реализацию, которая может поставить под угрозу конфиденциальность или ослабить безопасность пользователя. В данном случае, по мнению исследователей, вредоносное ПО распространялось через пиратские копии популярного программного обеспечения (например, программное обеспечение для графического дизайна Coreldraw Graphics для векторных иллюстраций и макетов страниц, как показано ниже).

После установки SilentFade украл учетные данные Facebook и файлы cookie из различных хранилищ учетных данных браузера, включая Internet Explorer, Chromium и Firefox.

«Файлы cookie более ценны, чем пароли, потому что они содержат токены сеанса, которые являются токенами после аутентификации», - говорят исследователи. «Такое использование скомпрометированных учетных данных может привести к обнаружению учетных записей, защищенных двухфакторной аутентификацией, которую SilentFade не может обойти».

По словам исследователей, сама вредоносная программа состоит из трех-четырех компонентов, причем основной компонент-загрузчик включен в пакеты PUP. Этот компонент загрузчика является либо отдельным вредоносным компонентом, либо службой Windows (установленной как «AdService» или «HNService»). Он отвечает за постоянство при перезагрузках и за удаление 32-разрядных и 64-разрядных версий динамических библиотек (DLL) в каталоге приложений Chrome, которые обычно называются winhttp.dll и запускают атаки с перехватом DLL.

«Все прокси DLL отправляют запросы к настоящему файлу winhttp.dll, но отправляют запросы на facebook.com через процесс Chrome, избегая обнаружения

вредоносных программ на основе динамического поведения, имитируя безобидные сетевые запросы», - заявили исследователи.

После кражи учетных данных вредоносная программа извлекает метаданные об учетной записи Facebook (такие как платежная информация и общая сумма, ранее потраченная на рекламу в Facebook), используя API-интерфейс Facebook Graph, который является законной функцией Facebook, позволяющей пользователям читать и записывать данные и из социальной сети Facebook. Затем эти данные отправляются обратно на серверы C2 вредоносного ПО (в виде зашифрованного большого двоичного объекта JSON через настраиваемые заголовки HTTP).

SilentFade имеет различные тактики устойчивости и уклонения от обнаружения, включая код для обнаружения виртуальных машин (проверка поля описания всех доступных драйверов дисплея на «Виртуальный» или «ВМ») и прекращения выполнения при обнаружении. Он также отключает уведомления Facebook от скомпрометированных учетных записей, которые потенциально могут предупредить жертву о подозрительной активности.

Кроме того, с помощью уникальной тактики защиты от обнаружения сервер C2 хранит данные и регистрирует IP-адрес входящего запроса с целью определения местоположения. «Это имело решающее значение, поскольку злоумышленники намеренно использовали украденные учетные данные из того же или соседнего города на зараженной машине, чтобы создать впечатление, будто первоначальный владелец учетной записи путешествовал по их городу», - заявили исследователи.

Хотя учетные данные пользователей Facebook ценны, пользователи с учетными записями, привязанными к кредитным картам (например, для бизнес-счетов), также дали киберпреступникам возможность использовать эти платежные карты для продвижения вредоносной рекламы в Facebook.

Однако «следует отметить, что данные платежной информации (такие как номера банковских счетов и кредитных карт) никогда не были доступны злоумышленникам, поскольку Facebook не делает их видимыми через веб-сайт для настольных компьютеров или Graph API», - заявили исследователи.

В рамках расследования SilentFade Facebook также обнаружил другие китайские вредоносные кампании, в том числе получившие название StressPaint, FacebookRobot и Scranos. Facebook предупредил, что некоторые из этих вредоносных атак оставались активными еще в июне…». ***(Lindsey O'Donnell. Years-Long 'SilentFade' Attack Drained Facebook Victims of $4M // Threatpost (https://threatpost.com/silentfade-attack-facebook/159780/). 02.10.2020).***

***

«Спир-фишинговые атаки, нацеленные на VIP-персон и других лиц, показывают ключевые изменения в вредоносном ПО и, вероятно, связаны с текущим конфликтом с Арменией.

Новая итерация PoetRAT программ - шпионы, спортивные улучшения эксплуатационной безопасности, эффективность коды и запутывание, делают раунды в Азербайджане, ориентированная на государственный сектор и другие

организации, ключевые как страны конфликта с Арменией из- за спорными территориями усиливаются.

Исследователи Cisco Talos обнаружили, что исследователи аналитики угроз наблюдали несколько новых атак с использованием вредоносного ПО, которые демонстрируют «изменение возможностей исполнителя» и «зрелость в направлении повышения операционной безопасности», при этом сохраняя тактику целевого фишинга, чтобы побудить пользователей загрузить вредоносные документы в сообщении в блоге, опубликованном во вторник.

PoetRAT ворвался на сцену в апреле в качестве регионального бэкдора, который действовал как острие копья для более широкой системы шпионажа. В этом случае оператор развернул дополнительные инструменты постэксплуатации в целевых системах, в том числе инструмент dog.exe, который отслеживает пути к жестким дискам для эксфильтрации информации через учетную запись электронной почты или протокол передачи файлов (FTP), в зависимости от по комплектации. Другой инструмент, Bewmac, позволяет злоумышленнику записывать камеру жертвы. Исследователи также столкнулись с другими инструментами, включая кейлоггер, средство для кражи учетных данных браузера, платформу с открытым исходным кодом для повышения привилегий (WinPwnage) и инструмент тестирования на проникновение и сетевого сканирования с открытым исходным кодом (Nmap).

На этот раз, по словам исследователей Уоррена Мерсера и Пола Раскагереса, для установки PoetRAT в двух отдельных файлах на машинах жертв в атаках используются документы Microsoft Word, предположительно принадлежащие правительству Азербайджана - вместе с государственным гербом Азербайджана в верхних углах. и Витор Вентура.

«Эти документы Word по-прежнему содержат вредоносные макросы, которые, в свою очередь, загружают дополнительные полезные данные, когда злоумышленник настраивает свои сайты на конкретной жертве», - пишут они. Однако, по словам исследователей, вредоносный документ, включенный в электронные письма с целевым фишингом, удаляет PoetRAT с некоторыми заметными изменениями во вредоносном ПО.

Различия между предыдущей и последней кампаниями включают изменение языка программирования, используемого для вредоносного ПО, с Python на скрипт Lua. В предыдущих кампаниях интерпретатор Python устанавливался вместе с основной полезной нагрузкой. Исследователи объяснили, что это изменение повышает эффективность кода и уменьшает размер файла вредоносного ПО - даже если оно само по себе сохраняет несложность, как было продемонстрировано в более ранних кампаниях, отметили исследователи.

«Предыдущие версии PoetRAT развертывали интерпретатор Python для выполнения включенного исходного кода, что приводило к гораздо большему размеру файла по сравнению с переключением последней версии на сценарий Lua», - сказали они. «Код легко разбирается - ничего сложного, но наш анализ показал нам, что кампании эффективны».

Исследователи отметили, что в последней кампании также есть несколько новых тактик, позволяющих избежать обнаружения. К ним относятся новый

протокол эксфильтрации для сокрытия действий злоумышленников, а также «дополнительная обфускация, позволяющая избежать обнаружения на основе строк или сигнатур», включая алгоритм сжатия Base64 и LZMA, отметили исследователи.

По их словам, разработчики также улучшили операционную безопасность (OpSec), выполнив разведку скомпрометированных систем и изменив протокол, используемый для загрузки и выгрузки файлов с FTP на HTTP.

Жертвы и конфликт

В число жертв кампании входят высокопоставленные лица Азербайджана и организации в государственном секторе, при этом злоумышленники демонстрируют доступ к конфиденциальной информации, такой как дипломатические паспорта, принадлежащие некоторым гражданам страны.

Исследователи Cisco Talos впервые обнаружили PoetRAT в апреле в ходе атак на энергетические компании в Азербайджане, которые включали инструменты постэксплуатации для регистрации нажатий клавиш, записи видео с веб-камер и кражи учетных данных браузера. Операторы вредоносных программ также нацелены на других жертв в государственном и частном секторах Азербайджана, а также на системы SCADA.

Согласно сообщению, исследователи считают, что причиной новых атак, скорее всего, является растущий конфликт между Азербайджаном и Арменией.

«Поскольку геополитическая напряженность в Азербайджане с соседними странами растет, это, без сомнения, этап шпионажа с последствиями для национальной безопасности, осуществляемый злоумышленником, проявляющим особый интерес к различным правительственным ведомствам Азербайджана», - писали они.

Вредоносная программа получила свое название от различных ссылок на сонеты английского драматурга Уильяма Шекспира, которые были включены в макросы, встроенные во вредоносные документы Word, которые были частью первоначальной кампании. Литературные отсылки, найденные в макросах на этот раз - из романа русского писателя Федора Достоевского «Братья Карамазовы», также могут быть завуалированной ссылкой на текущий конфликт. И Азербайджан, и Армения когда-то входили в состав бывшего Советского Союза, и Россия имеет тесные связи с обеими странами, а также является военным союзником Армении». ***(Elizabeth Montalbano. PoetRAT Resurfaces in Attacks in Azerbaijan Amid Escalating Conflict // Threatpost (https://threatpost.com/poetrat-resurfaces-azerbaijan-conflict/159917/). 07.10.2020).***

***

«Недавно обнаруженная программа-вымогатель поражает компании по всему миру, включая глобальную логистическую компанию GEFCO.

Недавно обнаруженное семейство программ-вымогателей под названием Egregor было замечено в «дикой природе», использовавшее тактику перекачивания корпоративной информации и угрозы ее разглашения «СМИ» перед шифрованием всех файлов.

Эгрегор - это оккультный термин, предназначенный для обозначения коллективной энергии или силы группы людей, особенно когда люди объединены

для достижения общей цели - по поводу банды вымогателей. Согласно анализу Appgate, код, похоже, является побочным продуктом программы- вымогателя Sekhmet (названной в честь египетской богини исцеления) - ссылка, которая также была отмечена другими исследователями.

«Мы обнаружили сходство в программах-вымогателях Sekhmet и Egregor, таких как методы обфускации, функции, вызовы API и строки, такие как% Greetings2target% и% sekhmet_data%, меняющиеся на% egregor_data%», - сказал Threatpost Густаво Палазоло, исследователь безопасности в Appgate. «Кроме того, записка о выкупе также довольно похожа».

Что касается других технических деталей, то, согласно исследованию фирмы, объявленному в пятницу, «проанализированный нами образец имеет множество методов антианализа, таких как обфускация кода и упакованные полезные данные». «Кроме того, на одном из этапов выполнения полезная нагрузка Egregor может быть расшифрована только в том случае, если правильный ключ указан в командной строке процесса, что означает, что файл нельзя проанализировать ни вручную, ни с помощью песочницы, если точно такой же командная строка, которую злоумышленники использовали для запуска программы-вымогателя, не предоставляется».

Кроме того, «мы обнаружили, что Egregor может получать дополнительные параметры через командную строку, такие как «nomimikatz», «killrdp», «norename» и другие», - сказал Палазоло. «В настоящий момент наша команда все еще занимается реорганизацией вредоносного ПО, чтобы получить полную картину. Кроме того, мы продолжим отслеживать любые возможные варианты, возникающие из этого семейства».

В целом, по его словам, он имеет тот же уровень сложности, что и другие семейства программ-вымогателей, однако Egregor реализует большое количество методов антианализа, таких как обфускация кода и шифрование полезной нагрузки.

Хотя исследователи Appgate не знают, как долго Эгрегор находится в обращении, его первое публичное появление Эгрегора было 18 сентября в Твиттере после того, как его заметили @ demonslay335 и @PolarToffee.

Исследователи Appgate также обнаружили, что записка с требованием выкупа требует выплаты в течение трех дней - в противном случае конфиденциальные данные будут утечкой. В отличие от обычной тактики двойного вымогательства, используемой семейством программ-вымогателей, таких как NetWalker, операторы Egregor угрожают распространять украденное через «средства массовой информации», чтобы партнеры и клиенты компании-жертвы знали, что компания подверглась нападению.

В этой части записки о выкупе, предоставленной Threatpost, говорится: «Что это означает? Значит, скоро СМИ, ваши партнеры и клиенты УЗНАЮТ о вашей ПРОБЛЕМЕ».

Но пока никаких событий в СМИ не произошло. «Единственное свидетельство, которое у нас есть, - это глубокий веб-сайт, на котором публикуются подробности об атакованных компаниях. Мы не обнаружили никаких других новостей или информации о данных, переданных каким-либо СМИ», - сказал Палазоло.

И действительно, в ходе анализа был обнаружен сайт Egregor news с самовывозом, размещенный в глубокой сети, который преступная группа использует для утечки украденных данных.

«На момент написания этой рекомендации в их «зале стыда» числилось как минимум 13 различных компаний, включая глобальную логистическую компанию GEFCO, которая подверглась кибератаке на прошлой неделе», - говорится в сообщении компании.

В записке с требованием выкупа Egregor также говорится, что помимо расшифровки всех файлов в случае, если компания заплатит выкуп, операторы предоставят рекомендации по обеспечению безопасности сети компании, «помогая» им избежать повторного взлома, «действуя как своего рода черный - эта команда по тестированию на проникновение», - говорится в исследовании Appgate.

В примечании говорится: «(В случае оплаты)... Вы ПОЛУЧИТЕ ПОЛНОЕ РАСШИФРОВАНИЕ ваших машин в сети, ПОЛНЫЙ СПИСОК ФАЙЛОВ загруженных данных, подтверждение УДАЛЕНИЯ загруженных данных с наших серверов, РЕКОМЕНДАЦИИ по защите периметра вашей сети».

«Рекомендации по безопасности привлекли наше внимание, поскольку это что-то необычное для преступной группы, они пытаются сыграть хороших парней, предполагая, что они попытаются защитить вашу сеть», - сказал Палазоло.

Пока нет информации о первоначальном векторе заражения вредоносным ПО, но программы-вымогатели, похоже, имеют равные возможности с точки зрения своих целей: образцы затрагивают корпорации во Франции, Германии, Италии, Японии, Мексике, Саудовской Аравии и США. исследователь.

Что касается размера выкупа, то операторы криминального ПО заставляют жертв прыгать через обруч.

«К сожалению, в записке о выкупе или на веб-сайте Egregor нет подробностей о [сумме выкупа]», - сказал Threatpost исследователь. «Чтобы получить платежные реквизиты, жертве необходимо перейти по ссылке в глубокой сети, которую предоставил Эгрегор, и получить инструкции от злоумышленника через чат в реальном времени, чего мы не выполняли». ***(Tara Seals. Egregor Ransomware Threatens 'Mass-Media' Release of Corporate Data // Threatpost (https://threatpost.com/egregor-ransomware-mass-media-corporate-data/159816/). 02.10.2020).***

***

«Вариант ботнета Mirai под названием Ttint добавил возможности шпионажа в дополнение к его функциям отказа в обслуживании.

Два бывших маршрутизатора нулевого дня Tenda закрепляют распространение ботнета Ttint на базе Mirai. В дополнение к атакам типа «отказ в обслуживании» (DoS) этот вариант также поддерживает троянские программы удаленного доступа (RAT) и шпионское ПО.

Согласно 360Netlab, ботнет необычен в нескольких отношениях. С одной стороны, на фронте RAT исследователи заявили, что он реализует 12 функций удаленного доступа, которые сочетаются с пользовательскими командами сервера управления и контроля (C2) для выполнения таких задач, как настройка прокси

Socket5 для устройств маршрутизатора, вмешательство в DNS маршрутизатора., установка iptables и выполнение пользовательских системных команд.

Кроме того, Ttint также использует зашифрованные каналы для связи с C2, в частности, с использованием протокола WebSocket over TLS (WSS). Исследователи заявили, что это позволяет избежать обнаружения трафика, обеспечивая при этом дополнительную безопасность.

И наконец, похоже, что инфраструктура мигрирует. 360Netlab сначала заметила злоумышленников, использующих IP-адрес облачной службы Google, прежде чем переключиться на хостинг-провайдера в Гонконге.

Нулевые дни

Маршрутизаторы Tenda доступны в крупных магазинах и используются в домах и небольших офисах. Первая уязвимость, используемая для распространения образцов Ttint (CVE-2018-14558), эксплуатируется по крайней мере с ноября прошлого года; но это не было раскрыто до июля. Теперь доступно обновление прошивки для решения этой проблемы.

Ошибка представляет собой критическую уязвимость, связанную с внедрением команд, рейтинг которой составляет 9,8 из 10 по шкале серьезности уязвимости CvSS. Он позволяет злоумышленникам выполнять произвольные команды ОС с помощью созданного запроса goform / setUsbUnload. Это возникает потому, что функция formsetUsbUnload выполняет функцию dosystemCmd с ненадежным вводом.

В конце августа в ходе кампании обнаружилась вторая критическая уязвимость маршрутизатора Tenda (CVE-2020-10987). Он также имеет рейтинг 9,8 из 10 и был первоначально раскрыт в июле независимыми экспертами по оценке безопасности после того, как с января пытался получить патч от Tenda. Он смог использовать ошибку, чтобы вызвать состояние DoS.

Ошибка возникает из-за того, что конечная точка goform / setUsbUnload Tenda AC15 AC1900 версии 15.03.05.19 позволяет удаленным злоумышленникам выполнять произвольные системные команды через параметр POST deviceName в соответствии с описанием CVE.

360Netlab также пытался предупредить Tenda о проблемах с ошибкой, на этот раз для использования при заражении ботнетами.

«28 августа 2020 года мы сообщили детали второй 0-дневной уязвимости и PoC [доказательство концепции] производителю маршрутизаторов Tenda по электронной почте, но производитель еще не ответил», - заявили исследователи.

Threatpost обратился к производителю за дополнительной информацией.

Ttint RAT

Ttint как вредоносное ПО может выполнять 10 типичных инструкций DDoS-атак Mirai (включая несколько векторов атак), а также 12 инструкций RAT и 22 настраиваемые команды C2, которые работают вместе.

«Вообще говоря, на уровне хоста поведение Ttint относительно простое», - утверждают исследователи. «При запуске он удаляет свои собственные файлы, манипулирует сторожевым таймером и предотвращает перезапуск устройства, он работает как единый экземпляр, привязав порт; затем изменяет имя процесса, чтобы ввести пользователя в заблуждение… наконец, он устанавливает соединение

с расшифрованным C2, сообщает информацию об устройстве, ожидает, пока C2 выдаст инструкции, и выполняет соответствующие атаки или пользовательские функции».

По словам исследователей, одной из наиболее заметных функций RAT является команда для привязки определенного порта, выданная C2 для включения прокси-службы Socket5. Это позволяет злоумышленникам получить удаленный доступ к интрасети маршрутизатора и перемещаться по сети.

«Как правило, Ttint объединяет несколько настраиваемых функций для достижения конкретных целей атаки», - пояснили исследователи. «Возьмите две соседние команды, которые мы захватили, первая команда - iptables -I INPUT -p tcp –dport 51599 -j ACCEPT, чтобы разрешить доступ к порту 51599 затронутого устройства. Следующая команда - включить функцию прокси Socket5 на порту 51599 затронутого устройства. Комбинация двух команд позволила злоумышленнику использовать прокси Socket5».

Другая команда указывает вредоносной программе вмешиваться в DNS маршрутизатора, изменяя файл resolv.conf, что позволяет ему перехватить доступ к сети любого из пользователей маршрутизатора. Это, в свою очередь, позволяет злоумышленникам отслеживать или красть конфиденциальную информацию.

Между тем, настроив iptables, операторы могут осуществлять переадресацию трафика и преобразование целевых адресов, что может раскрыть внутренние сетевые службы и привести к раскрытию информации. И, реализовав обратную оболочку через сокет, автор Ttint может использовать оболочку затронутого устройства маршрутизации как локальную оболочку.

И, наконец, пользовательские команды также позволяют вредоносному ПО самообновляться и самоуничтожаться.

По словам исследователей, информация C2 образца Ttint Bot зашифрована и хранится в таблице с конфигурационной информацией в формате Mirai, защищенной ключом XOR.

«Когда бот работает, он расшифровывает, чтобы получить адрес C2,… а затем безопасно связывается с C2 через WebSocket по протоколу TLS», - утверждают исследователи. «Когда Ttint C2 отвечает боту с кодом ответа 101, это означает, что рукопожатие протокола завершено, и затем бот может общаться, используя протокол WebSocket».

В последнее время наблюдается возрождение вредоносных программ на основе Mirai, способных создавать большие бот-сети за счет эксплуатации плохо защищенных устройств IoT. Это способствовало значительному увеличению количества распределенных атак типа «отказ в обслуживании» (DDoS) в первой половине года по сравнению с тем же периодом прошлого года. Однако добавление RAT и команд C2 знаменует собой изменение для мира Mirai.

«Две функции нулевого дня, 12 функций удаленного доступа для маршрутизатора, протокол зашифрованного трафика и перемещаемый IP-адрес инфраструктуры», - написала компания в недавнем блоге. «Этот ботнет не кажется очень типичным игроком». ***(Tara Seals. Tenda Router Zero-Days Emerge in Spyware Botnet Campaign // Threatpost (https://threatpost.com/tenda-router-zero-days-spyware-botnet/159834/). 05.10.2020).***

***

«Вариант вредоносного ПО для криптоджекинга основан на типичном подходе группы TeamTNT с несколькими новыми - и сложными - дополнениями.

Исследователи обнаружили последний гамбит вредоносного ПО для криптоджекинга от TeamTNT, получивший название Black-T. Этот вариант основан на типичном для группы подходе с несколькими новыми и сложными дополнениями.

TeamTNT известна тем, что нацелена на учетные данные Amazon Web Services (AWS), чтобы проникнуть в облако и использовать его для добычи криптовалюты Monero. Но, по словам исследователей из подразделения 42 сети Palo Alto Network, с помощью Black-T группа добавила дополнительные возможности к своей тактике, методам и процедурам (TTP). К ним относятся добавление сложных сетевых сканеров; нацеливание на инструменты майнинга XMR конкурентов в сети; и использование скребков паролей.

Что TeamTNT планирует делать с сохраненными паролями и дополнительными возможностями, пока неясно, но разработка сигнализирует, что группа не планирует замедляться в ближайшее время.

В августе исследователи определили TeamTNT как первую группу криптоджекинга, специально нацеленную на AWS. Благодаря все более изощренным TTП киберпреступная банда, похоже, набирает обороты. Буквально в прошлом месяце было обнаружено, что TeamTNT использует общий инструмент облачного мониторинга с открытым исходным кодом под названием Weave Scope, чтобы проникнуть в облако и выполнять команды без нарушения работы сервера.

По словам исследователей, Black-T представляет собой заметный скачок вперед в совершенстве операции.

После развертывания Black-T первым делом необходимо отключить любые другие вредоносные программы, конкурирующие за вычислительную мощность, в том числе Kinsing, Kswapd0, ntpd miner, redis-backup miner, auditd miner, Migration miner, Crux worm и Crux worm miner. По иронии судьбы, тот факт, что TeamTNT идентифицировал этих конкурентов в своем вредоносном ПО, дает специалистам по безопасности критически важное предупреждение, чтобы они были в поисках потенциальных угроз со стороны этих групп, сказал Unit 42.

Этот вид киберджекинга не нов, но, похоже, он набирает обороты.

«Битва за облачные ресурсы будет продолжаться и в будущем», - сказал Натаниэль Квист, старший исследователь угроз подразделения 42. «В прошлом группы злоумышленников, такие как Рок и Паша, сражались за ресурсы. TeamTNT сегодня борется с вредоносным ПО Kinsing и червем Crux. Я считаю, что эта битва за ресурсы усилится, и группы злоумышленников будут искать другие возможности использования облачных ресурсов. Мы видим это сейчас, когда TeamTNT собирает пароли и учетные данные AWS в попытке расширить и поддерживать присутствие в облаке».

После того, как он устраняет конкуренцию, Black-T устанавливает masscan, libpcap для прослушивания различных ресурсов в сети, включая pnscan, zgrab,

Docker и jq (последний является гибким JSON-процессором командной строки, согласно Unit 42).

«TeamTNT вкладывает больше ресурсов в операции сканирования, вероятно, с целью выявления и взлома большего количества облачных систем», - добавил Квист. «Zmap - известное решение для сканирования с открытым исходным кодом, и с созданием zgrab, инструмента GoLang, написанного для zmap, оно пытается извлечь выгоду из дополнительных преимуществ языка программирования Go, таких как увеличение скорости и производительности. Вполне вероятно, что участники TeamTNT пытаются улучшить свои возможности сканирования, чтобы сделать их более быстрыми, точными и менее ресурсоемкими».

Затем Black-T загружает различные файлы: бета-версия для создания нового каталога; инструменты паролей mimipy и mimipenquin; и программное обеспечение для майнинга XMR под названием bd.

«Включение инструментов паролей из памяти следует рассматривать как эволюцию тактики, - сказал Квист. «TeamTNT уже интегрировала сбор и эксфильтрацию учетных данных AWS из скомпрометированных облачных систем, что обеспечивает возможности после эксплуатации. Добавляя возможности извлечения паролей из памяти, участники TeamTNT увеличивают свои шансы на сохранение устойчивости в облачных средах».

Использование TeamTNT таких червей, как masscan или pnscan, не новость, но Unit 42 заметил, что Black-T добавляет новый порт сканирования. Исследователи задаются вопросом, сигнализирует ли это о том, что группа также выяснила, как нацеливаться на устройства Android.

По словам Квиста, поскольку удаленная работа и экономия средств продолжают приводить к переносу вычислений в облако, обязательно появятся новые группы, такие как TeamTNT, готовые воспользоваться преимуществами. Он добавил, что администраторы должны предпринять шаги для обеспечения того, чтобы API-интерфейсы Docker и демонов, а также любые другие конфиденциальные сетевые сервисы не были доступны, чтобы можно было защитить облако от следующей эволюции облачных криптоджекеров». ***(Becky Bracken. Black-T Malware Emerges From Cryptojacker Group TeamTNT // Threatpost (https://threatpost.com/blackt-cryptojacker-teamtnt/159853/). 05.10.2020).***

***

«Впервые ботнет IPStorm был замечен специалистами компании Anomali в июне 2019 года, и тогда он атаковал только Windows-машины. В то время в ботнет входили примерно 3000 зараженных систем, но уже тогда исследователи обнаружили несколько уникальных и интересных особенностей, характерных исключительно для IPStorm. Например, полное название малвари — InterPlanetary Storm, — происходит от InterPlanetary File System (IPFS), P2P-протокола, который малварь использовала для связи с зараженными системами и передачи команд.

Кроме того, IPStorm оказался написан на языке Go, и хотя сейчас малварью на этом языке никого не удивить, в 2019 году подобное было распространено не так

широко, что делало IPStorm довольно экзотичным и интересным образцом вредоносного ПО.

Интересно, что в отчете Anomali от 2019 года не объяснялось, как распространяется малварь. Тогда некоторые исследователи надеялись, что IPStorm окажется чьим-то экспериментом с IPFS и не получит полноценного развития. Увы, этим надеждам не суждено было сбыться.

В свежих отчетах, опубликованных экспертами Bitdefender и Barracuda, сказано, что были обнаружены новые версии IPStorm, способные заражать устройства под управлением Android, macOS и Linux. Также эксперты разобрались в способах распространения ботнета, опровергнув теорию о том, что был лишь чей-то эксперимент. Хуже того, количество зараженных машин увеличилось уже до 13 500 хостов.

По данным исследователей, ботнет атакует и заражает Android-девайсы, сканируя интернет в поисках устройств с открытым портом ADB (Android Debug Bridge). В свою очередь, устройства под управлением Linux и macOS компрометируют через словарные атаки на SSH, то есть злоумышленники просто подбирают имя пользователя и пароль.

После того как IPStorm проникает на устройства, малварь проверяет наличие honeypot-софта, закрепляется в системе, а затем ликвидирует ряд процессов, которые могут представлять угрозу для ее работы.

Хотя ботнет активен уже больше года, исследователи до сих пор не выяснили, какова конечная цель операторов IPStorm. Дело в том, что IPStorm устанавливает реверс-шелл на всех зараженных устройствах, но затем оставляет системы в покое. В теории этим бэкдором можно злоупотребить множеством способов, но пока операторы IPStorm вообще его не используют, хотя могли бы устанавливать на зараженные устройства майнеры, использовать их как прокси, организовывать DDoS-атаки, или попросту продавать доступ к зараженным системам». ***(Мария Нефёдова. Ботнет IPStorm стал атаковать устройства на Android, macOS и Linux // Xakep (https://xakep.ru/2020/10/01/ipstorm/). 01.10.2020).***

***

«Жертвы операторов вымогательского ПО не сообщают об атаках в полицию, что затрудняет определение уровня преступности и осложняет борьбу с причастными к ним группировкам.

В отчете Европола Internet Organised Crime Threat Assessment 2020 (Оценка угрозы организованной преступности в интернете 2020) подробно описаны ключевые формы киберпреступности, которые представляют угрозу для бизнеса в настоящее время.

Программы-вымогатели остаются одной из основных проблем, особенно с учетом того, что подобные группировки все чаще демонстрируют высокий уровень навыков и изощренности. Во многих случаях вымогатели не просто шифруют данные с помощью вредоносного ПО и требуют сотни тысяч или миллионов долларов в биткойнах, но они также угрожают утечкой украденных конфиденциальных корпоративных файлов или персональной информации жертв, если их требования не будут выполнены.

Хотя программы-вымогатели являются одной из самых известных форм кибератак, уведомлений о данных преступлениях поступает очень мало, поскольку многие организации не обращаются в правоохранительные органы после того, как стали жертвами. Несколько правоохранительных органов по всей Европе и вовсе заявили, что слышали о случаях вымогательства только из сообщений в местных СМИ.

Обращение в полицию с просьбой о возбуждении уголовного дела «обычно не является приоритетом» для потерпевших, которые больше озабочены поддержанием бизнеса и снижением ущерба их репутации. Для некоторых идея привлечения правоохранительных органов вовсе может рассматриваться как риск для их репутации.

В связи с этим некоторые предприятия предпочитают сотрудничать с «частными охранными фирмами» для расследования атак или переговоров о выплате выкупа. Компании делают это с целью скрыть доказательства атаки от общественности. Многие компании по-прежнему рассматривают уплату выкупа как самый быстрый и простой способ восстановления работы систем.

«Прибегая к услугам подобных фирм, жертвы не подают официальную жалобу, тем самым снижая осведомленность правоохранительных органов о реальном количестве атак программ-вымогателей», — говорится в отчете Европола.

Но не только компании не сообщают об атаках программ-вымогателей, пытаясь избежать огласки. Некоторые жертвы просто не думают, что правоохранительные органы могут чем-то помочь». ***(Жертвы вымогательского ПО боятся сообщать полиции об атаках из-за рисков // SecurityLab.ru (https://www.securitylab.ru/news/512771.php). 06.10.2020).***

***

«Специалисты из компании Sonatype обнаружили четыре пакета JavaScript npm с вредоносным кодом, который похищал данные пользователей и загружал информацию на общедоступную страницу GitHub. Были обнаружены следующие пакеты: electorn (255 загрузок), lodashs (78 загрузок), loadyaml (48 загрузок) и loadyml (37 загрузок).

Все четыре пакета были разработаны одним и тем же пользователем, использующим псевдоним simplelive12, и загружены на портал npm в августе нынешнего года. Два пакета (lodashs, loadyml) были удалены автором вскоре после публикации, однако они уже успели заразить устройства некоторых пользователей. Остальные пакеты (electorn и loadyaml) были удалены ИБ-экспертами из Sonatype.

Для того чтобы жертва установила вредоносные пакеты, их разработчик использовал технику тайпсквоттинга. Все четыре пакета имели неправильные названия более популярных пакетов, и полагались на то, что пользователи совершат ошибку при их поиске.

Злоумышленник обманом пытается заставить пользователя допустить опечатку и установить вредоносный пакет в своей среде вместо того, который он изначально намеревались загрузить. Например, разработчик запрашивает пакет «electron», но случайно записывает его как «electorn».

Как только жертва по ошибке скачивала и устанавливала один из четырех вредоносных пакетов, обнаруженный внутри вредоносный код собирал IP-адрес разработчика, информацию о стране проживания, городе, логине, пути к домашнему каталогу и модели процессора. Похищенная информация публиковалась в качестве нового комментария в разделе «Проблемы» репозитория на GitHub». ***(На портале npm обнаружено четыре пакета с вредоносным кодом // SecurityLab.ru (https://www.securitylab.ru/news/512754.php). 05.10.2020).***

***

«С портала npm были удалены три JavaScript-пакета (plutov-slack-client, nodetest199 и nodetest1010), содержащие вредоносный код.

По словам команды кибербезопасности npm, библиотеки открывали оболочки на компьютерах разработчиков, импортировавших пакеты в свои проекты. Оболочки могут работать как на операционных системах Windows, так и в Unix-подобных операционных системах, таких как Linux, FreeBSD, OpenBSD и пр.

Первый пакет был загружен на портал npm в мае 2018 года, а два других — в сентябре. Каждый пакет был скачан несколько сотен раз с момента загрузки на портал.

«Любой компьютер, на котором установлен или запущен один из упомянутых пакетов, следует считать полностью скомпрометированным. Все секреты и пароли, хранящиеся на этом компьютере, должны быть немедленно перемещены на другой компьютер», — заявили эксперты.

Пользователям необходимо удалить пакет, но, поскольку полный контроль над компьютером мог быть перехвачен злоумышленником, нет никакой гарантии, что устранение пакета приведет к удалению всего вредоносного программного обеспечения, возникшего в результате его установки». ***(Три вредоносных пакета npm могут полностью скомпрометировать компьютер // SecurityLab.ru (https://www.securitylab.ru/news/513146.php). 19.10.2020).***

***

«Министерство обороны США и министерство внутренней безопасности США рассказали о вредоносном ПО, которое используется неназванной группировкой для осуществления кибератак. Как сообщили источники ресурса CyberScoop, преступники атакуют организации в Индии, Казахстане, Кыргызстане, Малайзии, России и Украине.

Вредоносная программа, которую военное киберкомандование окрестило SlothfulMedia, представляет собой средство для кражи информации, способное осуществлять кейлоггинг и изменять файлы. Агентства разместили образец вредоносного ПО в репозитории на VirusTotal.

Вредонос используется в успешных текущих кампаниях, однако ведомства не сообщили, какая группировка ответственна за их проведение. В отчете также не упоминаются конкретные цели преступников.

Киберкомандование впервые начало разоблачать поддерживаемые государством хакерские кампании в 2018 году. Ранее ведомство сообщало о хакерских операциях со стороны иностранных правительств, включая операции из

Северной Кореи, России, Ирана и Китая. Связанные с правительством Китая хакеры ранее атаковали малайзийские и индийские организации, в то время как российские хакеры проводили операции кибершпионажа против целей в Украине, Казахстане и Кыргызстане.

Как сообщили ведомства, вредоносная программа загружает два файла на устройстве жертвы. Один из них представляет собой троян для удаленного доступа, который способен делать снимки экрана, изменять файлы на системах, завершать процессы и запускать произвольные команды. Троян, обозначенный как mediaplayer.exe, также, по-видимому, взаимодействует с C&C-сервером злоумышленников с помощью HTTP-over-TCP.

Второй файл имеет случайное пятизначное имя и удаляет загрузчик, как только RAT получит персистенство на системе. Персистенство достигается за счет создания службы с именем Task Frame, которая обеспечивает загрузку RAT после перезагрузки системы». ***(Власти США разоблачили текущие хакерские кампании в России, Украине, Индии и Малайзии // SecurityLab.ru (https://www.securitylab.ru/news/512724.php). 03.10.2020).***

***

«…Бразильцев предупреждают о новом оверлейном вредоносном ПО, нацеленном на пользователей Windows с целью выкачивания финансовых данных жертв и опустошения их банковских счетов. Исследователи говорят, что вредоносному ПО, получившему название Vizom, не хватает изощренности, что компенсирует его творческое злоупотребление экосистемой Windows.

Trusteer, бостонское исследовательское подразделение IBM Security, сообщило, что новый код активно используется в кампаниях, ориентированных на пользователей онлайн-банков в Бразилии. По его словам, оверлейное вредоносное ПО широко распространено в Латинской Америке и является одним из основных нарушителей в последнее десятилетие.

Vizom похож на другие оверлейные штаммы вредоносных программ в том, что его вектор атаки осуществляется через вредоносный спам и фишинговые кампании, которые доставляются в почтовые ящики потенциальных жертв.

«Обычно Vizom доставляется в виде спама, когда Vizom загружается невольным пользователем, он попадает в каталог [Windows] AppData и запускает процесс заражения», - пишет Чен Нахман, исследователь угроз безопасности в Trusteer.

Он объяснил, что вредоносная программа называется «Визом», потому что она использует некоторый законный компьютерный код, используемый браузером Chromium Vivaldi, и двоичные файлы из популярного программного обеспечения для видеоконференцсвязи, название которого исследователи не смогли идентифицировать.

Сначала дроппер загружает исполняемый файл, а затем распаковывает программное обеспечение для видеоконференцсвязи и полезную нагрузку DLL вредоносного ПО, объяснил Нахман в опубликованной в понедельник разбивке цепочки заражения вредоносным ПО.

«Что нам показалось интересным в Vizom, так это способ его заражения и развертывания на пользовательских устройствах. Он использует `` захват DLL '', чтобы проникнуть в легитимные каталоги на машинах под управлением Windows, замаскированных под легитимное, популярное программное обеспечение для видеоконференций, и обманывает внутреннюю логику операционной системы, загружая вредоносные библиотеки динамических ссылок (DLL) до того, как она загрузит легитимные которые принадлежат этому адресному пространству. Он использует аналогичную тактику для проведения атаки», - написал Нахман.

После заражения Vizom использует описанный выше метод для совмещения с Windows различными способами, например, предварительно загружая вредоносные файлы из различных каталогов ОС во время выполнения вредоносной программы.

Шаг на сторону антивируса

«В данном случае имя вредоносной DLL было взято из популярного программного обеспечения для видеоконференцсвязи:« Cmmlib.dll ». Чтобы убедиться, что вредоносный код запускается из «Cmmlib.dll», автор вредоносной программы скопировал реальный список экспорта этой легитимной DLL, но постарался изменить его, чтобы все функции были направлены на один и тот же адрес - адресное пространство вредоносного кода.," он написал.

Точно так же, чтобы проскользнуть мимо средств защиты конечных точек, законный браузер Vivaldi переносится в целевую систему вместе с вредоносными библиотеками DLL, которые также используются для проведения атаки, согласно отчету.

Сохранение вредоносного ПО поддерживается за счет изменения «ярлыков браузера, чтобы все они вели к его собственным исполняемым файлам и продолжали работать в фоновом режиме, независимо от того, какой браузер пытался запустить пользователь».

Теперь, когда жертва запускает свой браузер, вредоносная программа Vizom загружается и маскируется под процесс браузера Vivaldi, чтобы увеличить вероятность того, что ее не обнаружат.

«Поскольку так много людей перешло на работу из дома, и почти все используют видеоконференцсвязь... Vizom использует двоичные файлы популярного программного обеспечения для видеоконференцсвязи, чтобы прокладывать себе путь в новые устройства», - написал он.

«Vizom использует файлы еще одного легального программного обеспечения, на этот раз интернет-браузера Vivaldi, который помогает скрыть активность вредоносного ПО и избежать обнаружения средствами управления операционной системы и антивирусного программного обеспечения», - добавил он.

Вредитель после заражения

После заражения вредоносная программа отслеживает активность браузера, связывается с сервером управления и контроля (C2) злоумышленников, улавливает нажатия клавиш и развертывает свой оверлейный экран над веб-сайтом банка, который злоумышленники предварительно выбрали.

«После того, как Vizom полностью запускается на зараженном устройстве, он, как и другие оверлейные вредоносные программы, отслеживает онлайн-

просмотр пользователей в ожидании совпадения со своим целевым списком», - написал исследователь. «Поскольку Vizom не перехватывает браузер, как обычно это делают другие, более сложные вредоносные программы, он отслеживает активность, сравнивая заголовок окна, к которому пользователь обращается, с ключевыми целевыми строками, которые интересуют злоумышленника. Это сравнение происходит постоянно в цикле».

Как только жертва посещает веб-сайт желаемого банка, злоумышленник получает предупреждение в реальном времени об открытом банковском сеансе. Vizom запускает злоумышленника, открывая сокет TCP и связывая сервер C2. Связь с сервером C2 представляет собой обратную оболочку, которую зараженная машина использует для обратной связи с атакующим сервером, где порт прослушивателя получает соединение.

Фаза RAT

Затем злоумышленник использует троянский компонент своего вредоносного ПО для удаленного доступа, чтобы запустить оверлейный интерфейс и взять под контроль сеанс браузера. Исследователи заявили, что после этого жертв обманом заставляют предоставить личную идентифицирующую информацию (PII) и финансовую информацию, которая помогает злоумышленнику совершать мошеннические транзакции с банковского счета цели.

Фактические данные, похищенные у целей, собираются с помощью кейлоггера и затем отправляются на C2 злоумышленника. Следует отметить, что, по словам Нахмана, Vizom «генерирует HTML-файл из зашифрованных строк, а затем открывает его в браузере Vivaldi в режиме приложения». По его словам, это не типично для подобных оверлейных вредоносных программ и позволяет запускать приложение на одной веб-странице без типичного пользовательского интерфейса браузера, не позволяя зараженной жертве выполнять действия на экране.

«Vizom фокусируется на крупных бразильских банках, однако известно, что та же тактика используется против пользователей по всей Южной Америке и уже наблюдалась в отношении банков в Европе», - предупредил он». ***(Tom Spring. Overlay Malware Targets Windows Users with a DLL Hijack Twist // Threatpost (https://threatpost.com/overlay-malware-dll-hijack/160288/). 19.10.2020).***

***

«Эксперты «Лаборатории Касперского» сообщают, что шпионский вредонос GravityRAT, который используется для проведения целевых атак как минимум с 2015 года, теперь представляет собой мультиплатформенный инструмент. Данная малварь ранее применялась в ходе кампании кибершпионажа, нацеленной на индийских военных, и изначально была разработана для Windows-устройств. Теперь же появились новые модули, направленные на операционные системы Android и macOS.

Исследователи обнаружили, что GravityRAT научился атаковать и Android, когда в 2019 году заметили вредоносный модуль в приложении для путешественников по Индии Travel Mate, исходный код которого выложен на Github. Злоумышленники взяли версию приложения, опубликованную на Github в

октябре 2018 года, добавили в нее вредоносный код и поменяли название на Travel Mate Pro.

Найденный образец отличался от типичной шпионской Android-малвари: для его внедрения было выбрано специфическое приложение, а вредоносный код не был похож на известную малварь такого типа. Поэтому специалисты решили сопоставить код с кодом программ, используемых для проведения известных кампаний кибершпионажа, и в итоге обнаружили более десяти вредоносных модулей, также относящихся к семейству GravityRAT.

Малварь распространяется под видом легитимных приложений (таких как защищенные облачные хранилища, файлообменники, браузеры, программы для создания резюме или медиаплееры) и в фишинговых ссылках на скачивание якобы защищенного мессенджера для обсуждения вакансии. Вредонос атакует устройства под управлением Windows, Android и MacOS.

Функциональность GravityRAT в большинстве случаев остается прежней, типичной для шпионского ПО. Так, вредонос передает на управляющий сервер данные об устройстве, список контактов, электронные адреса, данные журнала звонков и SMS-сообщения. Некоторые трояны также искали в памяти устройства файлы с расширениями .jpg, .jpeg, .log,.png, .txt,.pdf,.xml, .doc, .xls, .xlsx, .ppt, .pptx, .docx и.opus, а затем тоже отправляли их на командные серверы.

«Мы видим, что злоумышленники, стоящие за кампанией GravityRAT, активно инвестируют в его разработку. Они хитроумными методами избегают обнаружения и добавляют модули для разных операционных систем, что предсказывает нам рост числа атак этого зловреда в Азиатско-Тихоокеанском регионе в будущем. На развитие инструмента также влияет распространённый в среде злоумышленников тренд не разрабатывать новое ПО, а совершенствовать уже имеющееся», — комментирует Татьяна Шишкова, эксперт по безопасности «Лаборатории Касперского». ***(Мария Нефёдова. У малвари GravityRAT появились версии для Android и macOS // Xakep (https://xakep.ru/2020/10/20/gravityrat/). 20.10.2020).***

***

«Эксперты компании Bitdefender подробно рассказали о работе P2P-ботнета Interplanetary Storm (он же IPStorm), который использует зараженные устройства в качестве прокси.

По данным исследователей, в состав ботнета входят более 9000 хостов (по другим данным число зараженных девайсов и вовсе превышает 13 500), подавляющее большинство которых работают под управлением Android, а еще около одного процента под управлением Linux и Darwin. По данным исследователей, это различные маршрутизаторы, NAS, UHD-ресиверы, многофункциональные платы (к примеру, Raspberry Pi) и прочие IoT-девайсы. В основном зараженные устройства находятся в Гонконге, Южной Корее и на Тайване.

Исследователи пишут, что о предназначении ботнета можно догадаться по специализированным узлам, входящим в управляющую инфраструктуру малвари:

- прокси-сервер, который пингует другие узлы, чтобы подтвердить их доступность;
- программа проверки прокси, которая подключается к прокси-серверу бота;
- менеджер, который отдается команды для сканирования и брутфорса;
- бэкэнд-интерфейс, отвечающий за хостинг Web API;
- узел, использующий криптографические ключи для аутентификации других устройств и подписания авторизованных сообщений;
- узел, используемый для разработки.

Суммарно это гарантирует проверку доступности узлов, подключение к прокси, хостинг Web API, подписание авторизованных сообщений и даже тестирование малвари на этапе разработки, рассказывают исследователи.

«Все это наводит на мысль, что ботнет используется в качестве прокси-сети, вероятно, предлагаемой в качестве сервиса анонимизации», — гласит отчет Bitdefender.

Заражение Interplanetary Storm происходит через сканирование SSH и подбор слабых паролей. Сама малварь написана на языке Go, причем в отчете подчеркивается, что ее основные функции были написаны с нуля, а не заимствованы у других ботнетов, как это часто бывает. Суммарно исследователи обнаружили более 100 изменений в коде вредоноса, то есть разработка Interplanetary Storm идет полным ходом.

В код вредоноса интегрированы имплементации опенсорсных протоколов NTP, UPnP и SOCKS5, а также библиотека lib2p для реализации peer-to-peer функциональности. Также малварь использует сетевой стек на основе lib2p для взаимодействия с IPFS.

«По сравнению с другими вредоносными программами, написанными на Go, которые мы анализировали в прошлом, IPStorm примечателен комплексным дизайном взаимодействия модулей и тем, как он использует конструкты libp2p. Совершенно очевидно, что злоумышленник, стоящий за этим ботнетом, хорошо владеет Go», — резюмируют эксперты». ***(Мария Нефёдова. Прокси-ботнет Interplanetary Storm насчитывает более 9000 устройств // Хакер (https://xakep.ru/2020/10/19/interplanetary-storm/). 19.10.2020).***

***

«В области кибербезопасности термин Offensive Security Tools (OST) относится к программным приложениям, библиотекам и эксплоитам, которые обладают атакующими способностями и были выпущены либо для бесплатного скачивания, либо по лицензии с открытым исходным кодом. OST-проекты обычно разрабатываются для демонстрации концепции эксплоита для новой уязвимости, для демонстрации новой/старой техники взлома или в виде утилит для тестирования на проникновение, предоставляемых сообществу.

Подобные инструменты помогают ИБ-экспертам изучить и подготовить системы и сети к потенциальным атакам. Однако те же инструменты помогают злоумышленникам сократить расходы на разработку собственного ПО.

Исследователь безопасности Пол Литвак (Paul Litvak) из компании Intezer Labs проанализировал 129 OST с открытым исходным кодом, а также проверил

образцы вредоносных программ и отчеты о кибербезопасности с целью выяснить, насколько широко распространены проекты OST среди хакерских группировок.

Результаты были собраны на интерактивной карте.

Как обнаружил Литвак, OST широко применяются среди самых разных киберпреступников — от известных APT-группировок (DarkHotel и пр.), до операторов вредоносного ПО (TrickBot и пр.).

«Наиболее распространенными проектами были библиотеки внедрения памяти (ReflectiveDllInjection и MemoryModule) и инструменты для удаленного доступа (Empire, Powersploit и Quasar)», — отметил эксперт.

Среди инструментов для перемещения по сети лидировал Mimikatz, а для обхода контроля учетных записей пользователей чаще всего использовалась библиотека UACME.

Единственными проектами, которые не пользовались популярностью, были инструменты с функциями кражи учетных данных. Как полагает Литвак, преступники предпочитают аналогичные инструменты, предоставляемые на подпольных хакерских форумах.

Специалист также отметил, что OST-инструменты со сложными функции также редко использовались злоумышленниками, даже если их атакующие возможности были очевидны. Литвак рекомендует разработчикам OST-проектов воспользоваться данной информацией и усложнить свой код, чтобы отбить у преступников желание использовать проект». ***(Хакеры часто используют в атаках инструменты с открытым исходным кодом // SecurityLab.ru (https://www.securitylab.ru/news/512980.php). 13.10.2020).***

***

«Как сообщают специалисты проекта DFIR Report, атака с использованием вымогательского ПО Ryuk занимает 29 часов – начиная от отправки жертве электронного письма и заканчивая полной компрометацией среды и шифрованием систем.

Впервые об атаках Ryuk стало известно в 2018 году. Тогда предполагалось, что вымогательская программа – дело рук северокорейских хакеров из-за его сходства с вымогательской программой Hermes. Однако затем специалисты связали Ryuk с российскими хакерами.

В течение двух последних лет Ryuk использовался в огромном количестве кибератак на серьезные организации, в том числе на медицинские учреждения во время пандемии коронавируса. В случае с атаками, изученными специалистами DFIR Report, все начинается с вредоносного письма с ссылкой на загрузчик Bazar/Kegtap, внедряющийся во множество процессов и проводящий разведку зараженной системы с помощью утилит Windows, таких как nltest и net group, и стороннего инструмента AdFind.

Затем в течение дня вредонос не проявляет никакой активности, после чего снова проводит разведку с помощью тех же инструментов и Rubeus. Полученные данные отправляются на подконтрольный злоумышленникам сервер, а атакующие начинают боковое перемещение по сети.

Для компрометации дополнительных систем в сети злоумышленники используют различные методы, в том числе WMI, удаленное выполнение служб PowerShell и компонент Cobalt Strike, загружаемый по SMB. Далее этот компонент использовался как поворотный момент.

Затем в среде устанавливаются дополнительные компоненты, и с помощью PowerShell отключается Защитник Windows. Через минуту после передачи по SMB выполняется Ryuk и начинается шифрования (серверы с резервными копиями шифруются в первую очередь).

Согласно отчету DFIR Report с подробным описанием всех этапов атаки, Ryuk также передается остальным хостам в сети через SMB, а затем выполняется через RDP-соединение с контроллера домена.

«В общей сложности кампания длилась 29 часов – от первоначального запуска Bazar до выполнения вымогательского ПО», – отмечается в отчете DFIR Report.

После шифрования вымогатель потребовал выкуп в размере порядка 600 биткойнов (около $6 млн). Впрочем, операторы Ryuk готовы торговаться». ***(Весь цикл атаки вымогательского ПО Ryuk длится 29 часов // SecurityLab.ru (https://www.securitylab.ru/news/512965.php). 13.10.2020).***

***

«Не секрет, що в Play Store ховається незліченна кількість шкідливих додатків. Останнім часом на Play Store прокотилася хвиля шкідливого "рекламного ПЗ". Якщо у вас є будь-яке з цих додатків для Android, у ваших інтересах видалити їх якомога швидше. За словами розробника антивіруса Avast, це 21 останнє додаток, яке необхідно негайно видалити через наявність шкідливого коду в них.

По-перше, більшість цих додатків для Android на перший погляд не здаються шкідливими або дуже підозрілими. Якщо ви не оціните їх належним чином, ви повірите, що вони чисті. Тим не менш, експерти з кібербезпеки Avast, як завжди, просканували Play Store на наявність вірусів і виявили, що в цих додатках згадується реклама YouTube, яка просуває зовсім інші функції, ніж ті, які користувачі фактично отримали при завантаженні цих ігор.

Повний список додатків, які потрібно видалити:

Shoot Them
Crush Car
Rolling Scroll
Helicopter Attack – New
Assassin Legend – 2020 New
Helicopter Shoot
Rugby Pass
Flying Skateboard
Iron it
Shooting Run
Plant Monster
Find Hidden
Find 5 Differences – 2020 New

Rotate Shape
Jump Jump
Find the Differences – Puzzle Game
Sway Man
Desert Against
Money Destroyer
Cream Trip – New
Props Rescue…» ***(Google Play заполонили програми-віруси, повний список небезпечних програм // Знай.ua (https://techno.znaj.ua/346747-google-play-zapolonili-programi-virusi-povniy-spisok-nebezpechnih-program). 27.10.2020).***

***

«Французская компания Sopra Steria, предоставляющая корпоративные ИТ-услуги, подтвердила сегодня, что они подверглись атаке программы-вымогателя Ryuk.

Sopra Steria - европейская компания в области информационных технологий, в которой работает 46 000 сотрудников в 25 странах мира. Компания предоставляет широкий спектр ИТ-услуг, включая консалтинг, системную интеграцию и разработку программного обеспечения.

21 октября Sopra Steria заявила, что подверглась кибератаке, но не предоставила никаких дополнительных подробностей.

«Вечером 20 октября была обнаружена кибератака в IT-сети Sopra Steria.

Были приняты меры безопасности для сдерживания рисков».

Французским СМИ и BleepingComputer тогда сообщили, что компания подверглась атаке вымогателя Ryuk после того, как ранее была заражена либо TrickBot, либо BazarLoader.

Обе вредоносные программы создаются одной и той же хакерской группой и обеспечивают удаленный доступ к злоумышленникам, стоящим за Ryuk Ransomware. Этот доступ позволяет злоумышленникам дополнительно взломать сеть и в конечном итоге развернуть программу-вымогатель на всех устройствах компании.

Сегодня Sopra Steria опубликовала заявление, подтверждающее, что они были затронуты программой-вымогателем Ryuk. В ходе расследования было установлено, что злоумышленники скомпрометировали их сеть на выходных, а затем 20 октября развернули программу-вымогатель.

«Вирус был идентифицирован: это новая версия вымогателя Ryuk, ранее неизвестная поставщикам антивирусного программного обеспечения и службам безопасности».

«Следственные группы Sopra Steria немедленно предоставили компетентным органам всю необходимую информацию. Группа смогла быстро сделать сигнатуру вируса этой новой версии доступной для всех поставщиков антивирусного программного обеспечения, чтобы они могли обновить свое антивирусное программное обеспечение».

«Кроме того, также было установлено, что кибератака была начата всего за несколько дней до ее обнаружения», - подтвердил Сопра Стерия в заявлении, отправленном BleepingComputer.

Sopra Steria также заявляет, что их расследование не указывает на утечку каких-либо данных о клиентах в это время.

Компания начала восстанавливать устройства и ожидает, что это займет несколько недель, прежде чем компания станет полностью работоспособной». ***(Lawrence Abrams. Sopra Steria confirms being hit by Ryuk ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/sopra-steria-confirms-being-hit-by-ryuk-ransomware-attack/). 26.10.2020).***

***

«На этой неделе Emotet перешел на новый шаблон, который представляет собой сообщение Microsoft Office, в котором говорится, что Microsoft Word необходимо обновить, чтобы добавить новую функцию.

Emotet - это вредоносная программа, которая распространяется через электронные письма, содержащие документы Word с вредоносными макросами. При открытии этих документов их содержимое будет пытаться обманом заставить пользователя включить макросы, чтобы вредоносная программа Emotet была загружена и установлена на компьютер.

После установки вредоносного ПО Emotet будет использовать компьютер для рассылки спама и, в конечном итоге, установки другого вредоносного ПО, которое может привести к атаке программ-вымогателей в сети жертвы.

Новый шаблон вредоносного документа

Спам-кампании Emotet используют различные приманки, чтобы заставить получателей открыть вложение, например, выдавать себя за счета-фактуры, уведомления об отправке, резюме или заказы на покупку или даже информацию о COVID-19, как показано ниже.

К этим спам-сообщениям прикреплены вредоносные вложения Word (.doc) или ссылки для их загрузки.

При открытии этих вложений пользователю будет предложено «Включить контент», чтобы запускались вредоносные макросы для установки вредоносного ПО Emotet на компьютер жертвы.

Чтобы обманом заставить пользователей включить макросы, Emotet использует различные дизайны или шаблоны документов, которые отображают предупреждение для пользователя.

На этой неделе Emotet перешел на новый шаблон, который представляет собой сообщение Microsoft Office, в котором говорится, что Microsoft Word необходимо обновить, чтобы добавить новую функцию…

Чтобы обновить Microsoft Word, в документе пользователю предлагается нажать кнопку «Разрешить редактирование», а затем кнопку «Включить содержимое», что вызовет выполнение вредоносных макросов…

Почему необходимо распознавать вложения Emotet?

Emotet сегодня считается самым распространенным вредоносным ПО, нацеленным на пользователей. Это особенно опасно, так как устанавливает на

компьютер жертвы другие инфекции, такие как вредоносные программы Trickbot и QBot.

После установки TrickBot и QBot будут пытаться украсть сохраненные пароли, банковскую информацию и другую различную информацию, но также часто приводят к атакам программ- вымогателей Conti (TrickBot) или ProLock (QBot).

В связи с этим важно, чтобы все пользователи электронной почты распознавали вредоносные шаблоны документов, используемые Emotet, чтобы вы случайно не заразились. ***(Lawrence Abrams. Emotet malware now wants you to upgrade Microsoft Word // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/emotet-malware-now-wants-you-to-upgrade-microsoft-word/). 24.10.2020).***

***

«Новый троян удаленного доступа Abaddon может быть первым, кто использует Discord в качестве полноценного сервера управления и контроля, который указывает вредоносной программе, какие задачи выполнять на зараженном компьютере. Хуже того, для этого вредоносного ПО разрабатывается функция вымогателя.

Злоумышленники, использующие Discord для злонамеренной деятельности, не новость.

В прошлом мы сообщали о том, как злоумышленники используют Discord для удаления украденных данных или создают вредоносное ПО, которое модифицирует клиент Discord для кражи учетных данных и другой информации.

RAT использует Discord как полноценный C2-сервер

Однако новый троян удаленного доступа Abaddon (RAT), обнаруженный MalwareHunterTeam, может стать первым вредоносным ПО, которое использует Discord в качестве полноценного сервера управления и контроля.

Сервер управления и контроля (C2) - это удаленный хост, с которого вредоносное ПО получает команды для выполнения на зараженном компьютере.

При запуске Abaddon автоматически украдет следующие данные с зараженного ПК:

Файлы cookie Chrome, сохраненные кредитные карты и учетные данные.

Учетные данные Steam и список установленных игр

Жетоны Discord и информация MFA.

Списки файлов

Системная информация, такая как страна, IP-адрес и информация об оборудовании.

Затем Abaddon подключится к серверу управления и контроля Discord, чтобы проверить наличие новых команд для выполнения…

Эти команды сообщают вредоносной программе о необходимости выполнения одной из следующих задач:

Украсть файл или целые каталоги с компьютера

Получите список дисков

Откройте обратную оболочку, которая позволяет злоумышленнику выполнять команды на зараженном ПК.

Запустить программу-вымогатель, находящуюся в разработке (подробнее об этом позже).

Отправьте обратно всю собранную информацию и очистите существующий сбор данных.

Вредоносная программа будет подключаться к C2 каждые десять секунд для выполнения новых задач.

Используя сервер Discord C2, злоумышленник может постоянно отслеживать свою коллекцию зараженных компьютеров на предмет новых данных и выполнять дальнейшие команды или вредоносное ПО на компьютере.

Разработка базовой программы-вымогателя

Одна из задач, которую может выполнить вредоносное ПО, - зашифровать компьютер с помощью базовой программы-вымогателя и расшифровать файлы после уплаты выкупа.

Эта функция в настоящее время находится в разработке, так как ее шаблон записки с требованием выкупа содержит заполнитель, поскольку разработчик работает над этой функцией.

Поскольку программы-вымогатели являются чрезвычайно прибыльными, неудивительно, что в будущем эта функция будет реализована». ***(Lawrence Abrams. New RAT malware gets commands via Discord, has ransomware feature // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-rat-malware-gets-commands-via-discord-has-ransomware-feature/). 23.10.2020).***

***

«В результате расследования в сети муниципальных жертв атак были обнаружены кастомный бэкдор RAT и троян Emotet.

Согласно отчету, Национальная гвардия была призвана помочь остановить серию правительственных атак с использованием программ-вымогателей в Луизиане.

По словам консультанта по кибербезопасности, беседовавшего с Reuters, местные правительственные учреждения по всему штату Пеликан подверглись атакам с применением программ-вымогателей, "свидетельствующие о том, что замешана сложная хакерская группа".

В документе сообщается, что судебно-медицинское расследование атак выявило троян удаленного доступа (RAT), скрытый в затронутых сетях, который часто является визитной карточкой группы расширенных постоянных угроз (APT), которая, как известно, является крылом правительства Северной Кореи. Тем не менее, исходный код бэкдора «KimJongRat» частично утек, что может позволить кибератакам скопировать его, что ставит под сомнение эту атрибуцию.

Источники сообщили, что троян Emotet также был обнаружен в сетях жертв, которые могут загружать другие вредоносные программы и самораспространяться по сетям. Агентство кибербезопасности и безопасности инфраструктуры США (CISA) в начале этого месяца выпустило предупреждение о том, что правительствам штатов и местным властям необходимо укрепить свои системы

против вредоносного ПО на фоне резкого роста фишинговых атак Emotet на муниципалитеты с июля.

«Это увеличение сделало Emotet одной из самых распространенных постоянных угроз», - говорится в предупреждении CISA.

Источники сообщили, что атаки привели к блокировке сетей в нескольких правительственных учреждениях на севере Луизианы после того, как сотрудники с помощью электронной почты были настроены на открытие вложения и запуск цепочки заражения. Кроме того, злоумышленники использовали учетные записи электронной почты жертв для рассылки вредоносных программ другим сотрудникам под видом законных сообщений.

Однако, согласно отчету, эта кибератака была остановлена «на ранних стадиях до того, как был нанесен значительный ущерб».

Неясно, какое семейство вымогателей использовалось в атаках. Национальная гвардия Луизианы отказалась комментировать инциденты.

Это не первый раз, когда Луизиана вызывает Национальную гвардию для борьбы с кибератаками. В июле 2019 года губернатор Луизианы объявил чрезвычайное положение в штате после того, как программа-вымогатель поразила как минимум три школьных округа - Монро-Сити, Морхаус и Сабин. Объявление чрезвычайного положения позволило координировать действия экспертов по кибербезопасности из Национальной гвардии, полиции штата Луизиана и Управления технологических служб.

Атаки программ-вымогателей продолжают расти во всех секторах. Только в этом месяце Software AG была поражена вымогателем Clop; Французский ИТ-гигант Sopra Steria пострадал от Ryuk; и в одном из округов Грузии была обнаружена атака на базу данных регистрации избирателей». ***(Tara Seals. Louisiana Calls Out National Guard to Fight Ransomware Surge // Threatpost (https://threatpost.com/louisiana-national-guard-ransomware/160508/). 23.10.2020).***

***

«Специалисты компании G DATA опубликовали отчет о новой малвари T-RAT, которую распространяют всего за 45 долларов США. Основной особенностью вредоноса является то, что T-RAT позволяет контролировать зараженные системы через Telegram-канал, а не через веб-панель администрирования, как это бывает обычно.

Создатели малвари уверяют, что это обеспечивает более быстрый и легкий доступ к зараженным компьютерам из любого места, и позволяет оперативно похищать данные. Впрочем, также T-RAT можно контролировать более традиционными методами, посредством RDP и VNC.

Telegram-канал T-RAT поддерживает 98 команд, которые позволяют извлекать из браузера пароли и файлы cookie, перемещаться по файловой системе жертвы и искать конфиденциальные данные, развертывать кейлоггер, тайно записывать звук через микрофон устройства, делать скриншоты рабочего стола жертвы, снимки через веб-камеру и перехватывать содержимое буфера обмена.

Кроме того, владельцы T-RAT могут использовать специальный механизм для захвата данных из буфера обмена, который подменяет строки, похожие на

адреса криптовалютных и электронных кошельков, на адреса злоумышленников. Это позволяет успешно перехватывать транзакции Qiwi, WMR, WMZ, WME, WMX, Яндекс.Деньги, Payeer, CC, BTC, BTCG, Ripple, Dogecoin и Tron.

Также малварь способна работать с командами терминала (CMD и PowerShell), блокировать жертве доступ к определенным сайтам (например, сайтам антивирусов и технической поддержки), ликвидировать конкретные процессы (отключать защитное и отладочное ПО) и даже деактивировать Панель задач и Диспетчер задач.

Эксперты G DATA пишут, что T-RAT — лишь одно из многих семейств малвари, которые оснащены возможностью управления через Telegram, и это не первый RAT, работающий по такой модели. Так, похожей функциональностью обладают: RATAttack (ориентирован на Windows), HeroRAT (нацелен на Android), TeleRAT (используются в основном против пользователей из Ирана, нацелен на Android), IRRAT (нацелен на Android), RAT-via-Telegram (доступен на GitHub, ориентирован на пользователей Windows) и Telegram-RAT (доступен на GitHub, нацелен на пользователей Windows).

«Новые образцы T-RAT регулярно загружают на VirusTotal. Я предполагаю, что он активно распространяется, хотя прямых доказательств этого у меня нет», — рассказывает эксперт компании Карстен Хан» ***(Karsten Hahn). (Мария Нефёдова. Новую малварь T-RAT можно контролировать через Telegram // Xakep (https://xakep.ru/2020/10/23/t-rat/). 23.10.2020).***

***

«Исследователи из компании Imperva выяснили (1, 2), что ботнет KashmirBlack, активный с конца 2019 года, заразил сотни тысяч сайтов, работающих на базе популярных CMS, в том числе WordPress, Joomla, PrestaShop, Magneto, Drupal, vBulletin, osCommerce, OpenCart и Yeager.

Как правило, ботнет использует серверы зараженных ресурсов для добычи криптовалюты, перенаправляет легитимный трафик на спам-сайты, задействует взломанные сайты для атак на другие ресурсы и поддержания своей активности, а порой и вовсе устраивает дефейсы.

Специалисты пишут, что изначально KashmirBlack был небольшим ботнетом, однако за прошедшие месяцы он разросся и превратился угрозу, способную атаковать тысячи сайтов в день. Наиболее радикальные изменения в работе малвари произошли в мае 2020 года, когда ботнет расширил управляющую инфраструктуру и свой арсенал эксплоитов. Так, исследователи пишут, что в настоящее время KashmirBlack управляется одним C&C-сервером, но использует более 60 серверов (в основном взломанные ресурсы) в своей инфраструктуре.

«KashmirBlack взаимодействует с сотнями ботов, каждый из которых обменивается данными с управляющим сервером, чтобы получить список новых целей, выполнить брутфорс-атаку, установить бэкдоры и работать над расширением ботнета», — гласит отчет компании.

Основной способ распространения KashmirBlack — сканирование интернета в поисках сайтов, которые работают под управлением устаревшего ПО. Затем малварь задействует эксплоиты для различных известных уязвимостей, чтобы

взломать уязвимый сайт и захватить его сервер. По данным Imperva, ботнет активно злоупотребляет 16 уязвимостями:

удаленное выполнение кода PHPUnit (CVE-2017-9841);

уязвимость загрузки файла jQuery (CVE-2018-9206);

инъекции команд в ELFinder (CVE-2019-9194);

уязвимость удаленной загрузки файлов в Joomla;

Magento Local File Inclusion (CVE-2015-2067);

уязвимость загрузки веб-форм в Magento;

проблема загрузки произвольного файла в CMS Plupload;

уязвимость в Yeager CMS (CVE-2015-7571);

множественные уязвимости, включая загрузку файлов и RCE во многих плагинах для различных платформ;

уязвимость WordPress TimThumb RFI (CVE-2011-4106);

RCE-уязвимость Uploadify;

RCE-уязвимость в виджете vBulletin (CVE-2019-16759);

RCE-уязвимость в WordPress install.php;

брутфорс-атака на WordPress xmlrpc.php;

RCE в ряде плагинов для WordPress(полный список здесь);

RCE в ряде тем для WordPress (полный список здесь);

уязвимость загрузки файла в Webdav.

Исследователи Imperva отмечают, что, по их мнению, данный ботнет — это дело рук хакера, известного под псевдонимом Exect1337, который входит в индонезийскую хакерскую группу PhantomGhost». ***(Мария Нефёдова. Ботнет KashmirBlack стоит за атаками на популярные CMS, включая WordPress, Joomla и Drupal // Xakep (https://xakep.ru/2020/10/27/kashmirblack/). 27.10.2020).***

***

«Специалисты компании FireEye рассказали о ряде вредоносных кампаний по распространению вымогательского ПО, в рамках которых использовалось новые загрузчики KEGTAP (также известный как BEERBOT), SINGLEMALT (также известный как STILLBOT) и WINEKEY (также известный как CORKBOT). В некоторых случаях развертывание вымогателей происходило в течение 24 часов после взлома.

Хотя данные семейства вредоносов взаимодействуют с одним и тем же C&C-сервером и имеют общие функциональные особенности, сходство в коде между ними минимально. Операторы, осуществляющие вредоносные кампании, активно нацелены на больницы, пенсионные сообщества и медицинские центры даже в разгар глобального кризиса в области здравоохранения.

В рамках кампаний по распространению KEGTAP, SINGLEMALT и WINEKEY были разосланы письма частным лицам в организациях из различных отраслей и географических регионов. Письма содержали ссылку на документ Google Docs со встроенной ссылкой на URL-адрес, содержащий полезную нагрузку вредоносного ПО. Преступники маскируют письма, используя обычные корпоративные темы, включая сообщения о жалобах, увольнениях, бонусах, контрактах, графиках работы или опросах.

Ранние кампании осуществлялись через Sendgrid и включали встроенные ссылки на URL-адреса Sendgrid, которые перенаправляли пользователей к документам Google. При нажатии на ссылки загружались двоичные файлы вредоносных программ с именами файлов, замаскированных под документы. Ранее двоичные файлы вредоносных программ размещались в скомпрометированной инфраструктуре, однако злоумышленники вскоре перешли на размещение своего вредоносного ПО на легитимных web-сервисах, включая Google Drive, Basecamp, Slack, Trello, Yougile и JetBrains.

После запуска загрузчика и бэкдора на системе жертвы, злоумышленники загружали POWERTRICK и/или маяки Cobalt Strike. В дополнение к использованию общих постэксплуатационных фреймворков, таких как Cobalt Strike, Metasploit и EMPIRE, эксперты наблюдали использование других бэкдоров, включая ANCHOR, который, предположительно, находится под контролем TrickBot.

Загрузчики могут поддерживать персистентность посредством перезагрузки, используя по крайней мере четыре различных метода, включая создание запланированной задачи, добавление себя в папку автозагрузки в качестве ярлыка, создание запланированного задания Microsoft BITS с помощью /setnotifycmdline и добавление себя в значение Userinit в разделе реестра HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.

По крайней мере в одном случае злоумышленники поддерживали доступ к среде жертвы, используя украденные учетные данные для доступа к корпоративной инфраструктуре VPN, настроенной на требование только однофакторной аутентификации. Преступники использовали похищенные учетные данные, полученные с помощью MimiKatz, для повышения привилегий.

Подходы, используемые для выполнения разведки сети в этих инцидентах, различались, однако значительная часть наблюдаемой разведывательной деятельности была связана с перечислением Activity Directory с использованием общедоступных утилит, таких как BLOODHOUND, SHARPHOUND или ADFind, а также выполнения PowerShell-команд с использованием маяков Cobalt Strike.

Перемещение по сети чаще всего выполнялось с использованием действительных учетных данных обычных пользователей и администраторов в сочетании с маяками Cobalt Strike, RDP и SMB или с использованием тех же бэкдоров, которые используются для закрепления в сетях жертв.

Эксперты также зафиксировали инциденты, связанные с KEGTAP, которые включали развертывание вымогателя Ryuk после взлома. Также наблюдались случаи, когда установка бэкдора ANCHOR предшествовала развертыванию Conti или Maze». ***(Хакеры вооружились новыми загрузчиками для установки вымогателей // SecurityLab.ru (https://www.securitylab.ru/news/513516.php). 29.10.2020).***

***

«Огромную роль в кибератаках играют эксплоиты – они позволяют хакерам осуществлять действия, которые в ином случае были бы невозможны. Однако, поскольку эксплоиты используются во многих семействах

вредоносного ПО, вся «слава» достается создателям вредоносных программ, а разработчики эксплоитов остаются в тени. В связи с этим специалисты компании Check Point Эяль Иткин (Eyal Itkin) и Итай Коэн (Itay Cohen) решили провести исследование, посвященное авторам эксплоитов.

Исследователи разработали методологию и техники отслеживания разработчиков по «почерку», то есть, по оставляемым ими цифровым отпечаткам (так называемый фингерпринтинг). С ее помощью им уже удалось найти связь между 16 эксплоитами и их разработчиками, известными как Volodya (он же BuggiCorp) и PlayBit (он же luxor2008). Об уникальных отпечатках, позволивших им вычислить Volodya, исследователи рассказали еще в начале текущего месяца. Теперь же они опубликовали подробности о том, как им удалось выйти на его коллегу PlayBit.

Специалисты заинтересовались PlayBit после того, как наткнулись на публикацию в блоге «Лаборатории Касперского» о том, что известная киберпреступная группировка Sodinokibi (другое название REvil) вооружилась эксплоитом для уязвимости CVE-2018-8453 в Windows. Поскольку изначально эксплоит использовался группировкой FruityArmor, исследователи пришли к выводу, что его разработчиком является кто-то третий.

Как показал анализ эксплоита, в нем использовался совсем другой шаблон, чем в эксплоитах авторства Volodya, а значит, Volodya не является его создателем. Поскольку разработчик реализовал в своем творении новые функции, это дало исследователям дополнительный набор артефактов для анализа его «почерка». Собрав воедино все артефакты, специалисты создали цифровой отпечаток и отправились на охоту за другими созданными разработчиком эксплоитами.

В общей сложности исследователи обнаружили пять эксплоитов авторства PlayBit. Все они предназначены для уязвимостей нулевого дня в Windows, позволяющих атакующему повышать свои привилегии на системе жертвы. Речь идет о CVE-2013-3660 (используется вредоносными программами Dyre и Ramnit), CVE-2015-0057 (Dyre и Evotob), CVE-2015-1701 (Locky), CVE-2016-7255 (LockCrypt) и CVE-2018-8453 (REvil/Sodinokibi, Maze и Neshta).

Проанализировав эксплоиты, исследователи обнаружили в них общие черты. К примеру, как и Volodya, PlayBit использовал для их создания один простой шаблон. Кроме того, он «обернул» свои эксплоиты в оболочку, позволяющую им проверять возможность эксплуатации уязвимостей на отдельно взятом компьютере, и использовал обфускацию для сокрытия полезных функций эксплоитов. В отличие от эксплоитов Volodya, творения PlayBit пытаются узнать об атакуемой системе как можно больше – точную версию ОС, номер сборки Windows и пакет обновлений, а также определяют, является ли компьютер сервером». ***(Эксперты вычислили автора популярных эксплоитов по почерку // SecurityLab.ru (https://www.securitylab.ru/news/513389.php). 27.10.2020).***

***

«Два члени консольної хакерської і піратської організації, відомої як Team Xecuter, були заарештовані і звинувачені в шахрайстві, одного з яких звуть Гері Баузер. Громадянин Франції Макс Луарн і Баузер, родом з Канади, але заарештований в Домініканській Республіці, нібито очолювали групу, яка виробляє лінійку інструментів для злому заблокованого ігрового обладнання.

Team Xecuter - це команда хакерів, відома насамперед своїми зломами Nintendo, включаючи USB-пристрій під назвою SX Pro, який дозволяє Nintendo Switch запускати піратські ігри.

Nintendo добре обізнана з групою, оскільки ще в травні вона подала проти неї два судові позови з основним наміром закрити сторонніх роздрібних продавців, які перепродують продукти Team Xecuter через мережу. Nintendo також має свою суперечливу історію, що включає агресивні судові розгляди щодо несанкціонованого використання її інтелектуальної власності. В останні роки Nintendo пішла на пошуки так званих ROM-сайтів, на яких розміщені скопійовані файли ігор, а також інших сайтів та інтернет-магазинів, які використовують піратський контент і пов'язані з ним апаратні інструменти.

Міністерство юстиції пішло ще далі. "Ці обвинувачені нібито були лідерами сумнозвісного міжнародного злочинного угруповання, яке протягом багатьох років отримувало незаконний прибуток за рахунок крадіжки технологій відеоігор американських компаній", - йдеться в заяві Брайана К.Реббітта, виконуючого обов'язки помічника генерального прокурора Кримінального управління Міністерства юстиції. "Ці арешти показують, що департамент буде притягувати до відповідальності хакерів, які прагнуть привласнити і використовувати інтелектуальну власність американських компаній для отримання фінансової вигоди, незалежно від того, де вони можуть перебувати".

Обом чоловікам загрожує суворе тюремне ув'язнення, якщо вони будуть засуджені, включаючи 20 років за кожне звинувачення в змові з метою здійснення шахрайства з використанням електронних засобів, шахрайства з використанням електронних засобів і змови з метою відмивання грошей, С до п'яти років за деякі з менш значних звинувачень. Дата судового розгляду не встановлена…» ***(Николай Олефиренко. Хакерам "світить" реальний тюремний термін за злом консолі Nintendo Switch // Знай.ua (https://techno.znaj.ua/341758-hakeram-svitit-realniy-tyuremniy-termin-za-zlom-konsoli-nintendo-switch). 05.10.2020).***

***

«Сегодня в США, Португалии, Испании и Великобритании нескольким членам QQAAZZ, международной киберпреступной группировки, были предъявлены обвинения в предоставлении услуг по отмыванию денег для нескольких известных вредоносных программ, включая Dridex, Trickbot и GozNym.

По оценкам правоохранительных органов, начиная с 2016 года QQAAZZ отмыл или, по крайней мере, попытался отмыть десятки миллионов, украденных у жертв киберпреступлений.

«QQAAZZ рекламировал свои услуги как« глобальную услугу по отказу от банков »на русскоязычных онлайн-форумах киберпреступников, где киберпреступники собираются, чтобы предлагать или искать специальные навыки или услуги, необходимые для участия в различных киберпреступных действиях», - заявило сегодня Министерство юстиции.

«Преступные группировки, стоящие за некоторыми из самых вредоносных семейств вредоносных программ в мире (например, Dridex, Trickbot, GozNym и т. Д.), Входят в число тех киберпреступных групп, которые воспользовались услугами QQAAZZ».

20 членов QQAAZZ были арестованы в результате серии обысков более 40 домов в Латвии, Болгарии, Великобритании, Испании и Италии.

Это стало результатом международной правоохранительной операции с участием 16 стран, координируемой Европолом и получившей название Operation 2BaGoldMule.

В рамках этой операции в Болгарии была арестована обширная операция по добыче биткойнов, связанная с QQAAZZ.

Согласно обнародованным сегодня обвинительным актам [1, 2], преступная группировка предлагала свои «услуги по обналичиванию» в форме «глобальной услуги по предоставлению соучастников банка» известным российским бандам киберпреступников на русскоязычных форумах киберпреступников (например, Проверено и Мазафака).

Они общались со своими «клиентами» посредством обмена мгновенными сообщениями, давая им указание отправить украденные средства на банковские счета, находящиеся под контролем QQAAZZ и открытые с помощью денежных мулов с использованием поддельных и законных польских и болгарских удостоверений личности.

Члены QQAAZZ также включали десятки подставных компаний, которые использовались для открытия других банковских счетов, которые позже использовались для приема и отмывания средств, украденных киберпреступниками с помощью вредоносного ПО.

В общей сложности во время операции по отмыванию денег были использованы «сотни корпоративных и личных банковских счетов в финансовых учреждениях по всему миру».

Часть денег была также «конвертирована в криптовалюту с помощью« акробатических »сервисов, предназначенных для сокрытия первоначального источника средств».

QQAAZZ вернул часть отмытых средств своим клиентам, занимающимся киберпреступностью, после того, как выручил до 50% от общего остатка полученных украденных средств.

Хотя в США были идентифицированы десятки жертв, деньги которых были украдены и отмыты QQAAZZ, их общее количество и их личности неизвестны,

учитывая масштаб операции по отмыванию денег и множество киберпреступных банд, которые она обслуживала.

«Киберпреступники постоянно изучают новые возможности для злоупотреблений технологий и финансовых механизмов для обкрадывания миллионов пользователей в настоящее время из любой точки мира,» Edvardas Шилерис, руководитель Европейского центра киберпреступности Европола, сказал.

«Сегодняшняя операция показывает, как посредством надлежащей международной координации правоохранительных органов мы можем повернуть стол против этих преступников и привлечь их к ответственности». ***(Sergiu Gatlan. QQAAZZ group charged for laundering money stolen by malware gangs // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/qqaazz-group-charged-for-laundering-money-stolen-by-malware-gangs/). 15.10.2020).***

***

«Издание ZDNet сообщает, что в начале октября 2020 года Германии в Румынии прошли полицейские рейды на офисы компаний, связанных с разработкой так называемой легальной спайвари FinFisher.

Согласно заявлению прокуратуры Мюнхена, рейды были проведены на 15 объектах недвижимости (сюда входят как офисные помещения, так и частные апартаменты) в окрестностях Мюнхена, а также у румынской компании, связанной с разработкой FinFisher.

Эти рейды – часть расследования, начатого еще летом прошлого года после жалобы, поданной представителями портала Netzpolitik. Эту жалобу также подписали такие правозащитные группы, как Society for Freedom Rights, Репортеры без границ и Европейский центр по конституционным правам и правам человека. Они утверждали, что малварь FinFisher устанавливалась на устройства активистов, политических диссидентов и граждан в странах с репрессивными режимами, а также в странах, которым FinFisher было запрещено продавать свое ПО.

Тогда разработчики FinFisher отвергли эти обвинения и подали в суд на Netzpolitik, заставив его редакцию удалить оригинальную статью, однако расследование дела все равно было продолжено. В прокуратуре Мюнхена подтвердили журналистам ZDNet, что недавние рейды были частью этого судебного процесса, в рамках которого власти Германии собирают доказательства утверждений, изложенных в жалобе.

Нужно сказать, что немецкое информационное агентство Tagesschau, которое первым сообщило о прошедших рейдах, вообще утверждает, что FinFisher использовала спутниковые компании в других странах мира, чтобы обойти строгие ограничения на экспорт своего программного обеспечения.

Напомню, что спайварь FinFisher (она же FinSpy) по слухам активно применяется для политической слежки за журналистами и диссидентами в самых разных странах мира. В 2011 программу слил в WikiLeaks Джулиан Ассанж, после чего та стала достоянием анонимусов и подверглась пристальному изучению со стороны специалистов по информационной безопасности и прочих заинтересованных лиц.

FinFisher может перехватывать переписку жертвы в социальных сетях, отслеживать почтовые сообщения, работать кейлоггером, предоставлять доступ к хранящимся на инфицированной машине файлам, а также записывать видео и аудио с помощью встроенного микрофона и камеры. Существуют сборки продуктов FinFisher под Windows, macOS и Linux. Кроме того, за прошедшие годы были созданы мобильные версии спайвари практически для всех существующих сегодня платформ: Android, iOS, BlackBerry, Symbian и Windows Mobile.

Среди известных клиентов FinFisher: федеральная полиция Германии и полиция Берлина. Но также инструменты компании не раз обнаруживали на устройствах оппозиционеров и журналистов в таких странах, как Эфиопия, Бахрейн, Египет и Турция, то есть в странах, куда экспорт подобной спайвари запрещен». ***(Мария Нефёдова. Немецкие власти провели обыски в офисах FinFisher // Xakep (https://xakep.ru/2020/10/14/finfisher-raids/). 14.10.2020).***

***

Технічні аспекти кібербезпеки

«Специалисты компании Guardicore изучили пульты дистанционного управления XR11, работающий с приставкой Xfinity X1, и разработали атаку WarezTheRemote. Исследователи пришли к выводу, что из пультов можно сделать скрытые шпионские устройства и следить за пользователями.

Пульты XR11предоставляются американским телекоммуникационным гигантом Comcast клиентам платформы Xfinity. В общей сложности на сегодня было продано более 18 000 000 таких устройств. Такие пульты позволяют пользователям переключать каналы, искать программы и выполнять другие действия с помощью голосовых команд.

Первая фаза атаки WarezTheRemote связана с тем, что злоумышленник передает на устройство вредоносную прошивку. Дело в том, что устройство использует радиочастоту, а не инфракрасный порт для связи с приставкой. Поскольку радиочастота имеет большую дальность действия, хакер может организовать такую атаку со значительного расстояния.

Хотя коммуникации между пультом и приставкой зашифрованы, прошивка пульта работает некорректно и не может гарантировать, что на зашифрованные запросы принимаются только зашифрованные ответы, то есть злоумышленник имеет возможность отправлять пульту вредоносные ответы в формате простого текста.

Также исследователи рассказывают, что пульт ДУ проверяет наличие обновлений прошивки раз в 24 часа, опрашивая спаренную с ним приставку. Как оказалось, атакующий без труда мог выдать себя за приставку, воспользоваться уязвимостью, связанной с шифрованием, а затем сообщить удаленному устройству, что доступно обновление (образы прошивок не были подписаны).

Более того, специалисты не только нашли способ передать пульту вредоносную прошивку, но также осуществили DoS-атаку на саму приставку,

чтобы гарантировать, что та не помешает атаке на пульт (загрузка прошивки занимает примерно полчаса, и данный процесс может быть нарушен).

В итоге, исследователи перепрошили XR11 с помощью WarezTheRemote и получили возможность удаленно активировать микрофон устройства. Передача звука осуществлялась с помощью радиочастоты, что позволяло атакующему шпионить за пользователем, ведь пульт улавливает голос жертвы на расстояния до 15 футов (около 5 метров).

В отчете специалистов подчеркивается, что для проведения атаки не требуется дорогостоящее оборудование. Так, для WarezTheRemote понадобятся только RF-ресивер и антенна на 16 dBi, чья суммарная стоимость составляет несколько сотен долларов. Эти устройства позволят провести атаку с расстояния примерно 65 футов (около 20 метров). При этом в Guardicore уверены, что атака может сработать даже на больших расстояниях, если использовать более мощную аппаратуру.

Исследователи уведомили Comcast о найденных проблемах еще в апреле текущего года, и 14 июля 2020 года компания начала выпускать исправления. Производитель сообщил, что в прошивке версии 1.1.4.0 все вышеописанные баги были устранены (включая баг, позволявший спровоцировать у приставки отказ в обслуживании), и обновленная версия начала распространяться на устройства 24 сентября». ***(Мария Нефёдова. Исследователи превратили умные пульты Comcast в подслушивающие устройства // Xakep (https://xakep.ru/2020/10/08/warezтheremote/). 08.10.2020).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Специалисты Positive Technologies выявили уязвимость в системе IBM Maximo Asset, которая применяется для управления ремонтом и техоблуживанием производственных активов в крупнейших фармацевтических, нефтегазовых, автомобилестроительных, аэрокосмических, железнодорожных компаниях, в аэропортах, в морских портах, на АЭС и в других сферах.

Уязвимость CVE-2020-4521, обнаруженная в версиях 7.6.0 и 7.6.1 системы, имеет высокий уровень опасности (8,8 баллов по шкале CVSS) и связана с небезопасной десериализацией в Java. Ошибка может позволить удаленному злоумышленнику выполнить произвольный код в системе. Для эксплуатации уязвимости атакующий должен отправить специально созданный нелегитимный запрос, будучи аутентифицированным в системе (достаточно минимальных привилегий).

Как и в случае с CVE-2020-4529 – другой уязвимостью в IBM Maximo, для эксплуатации CVE-2020-4521 атакующий может иметь низкие привилегии и уровень доступа рядового оператора – например, кладовщика, который удаленно

подключается к системе и заносит позиции в базу. Атакующий отправляет на сервер специально подготовленный Java-объект в сериализованном виде. Из-за небезопасного механизма десериализации этот объект можно восстановить на сервере из последовательности байтов и использовать в атаке. При успешной эксплуатации уязвимости злоумышленник получит возможность удаленного выполнения кода и полного контроля над веб-приложением IBM Maximo, что может быть использовано для доступа к корпоративной и технологической сетям предприятия. Возможность дальнейшего развития атаки зависит от конкретной конфигурации системы и наличия других уязвимостей.

Проблема затрагивает также специализированные отраслевые решения, реализованные на базе 7.6.0 и 7.6.1 версий системы: Maximo for Aviation, Maximo for Life Sciences, Maximo for Nuclear Power, Maximo for Oil and Gas, Maximo for Transportation, Maximo for Utilities, а также продукты SmartCloud Control Desk, IBM Control Desk и Tivoli Integration Composer.

Для устранения уязвимости необходимо обновить IBM Maximo Asset Management и связанные с этой системой решения и продукты до последних версий в соответствии с рекомендациями производителя». ***(В IBM Maximo исправлена уязвимость, позволявшая удаленно выполнить произвольный код // Компьютерное Обозрение (https://ko.com.ua/ibm_maximo_udalenno_vypolnit_proizvolnyj_kod_v_sisteme_134728). 02.10.2020).***

***

«Исследователь в области кибербезопасности Нильс Х (Niels H) обнаружил серьезную уязвимость в сопроцессоре Apple T2.

Что это такое Apple T2 пришел на смену T1 и начал устанавливаться в устройствах Apple с 2017 года. Это чип, основная функция которого — обеспечение безопасности пользовательских данных. На него завязаны процесс авторизации при помощи Touch ID, шифрование, пароли KeyChain и многое другое. T2 устанавливают в ноутбуках MacBook и компьютерах iMac. Apple уверяла, что этот чип в разы повысит безопасность пользовательской информации и защищенность компьютера от взлома, а в результате он и сам небезопасен.

Как это работает

Из-за общих корней с процессором Apple A10 T2 уязвим к взлому при помощи эксплойта Checkm8, использующегося для джейлбрейка iPhone. В результате хакер может получить полный доступ к устройству. Но для взлома чипа необходимо прямое подключение через USB-C. Хотя данные защищены шифрованием FileVault, хакеры могут перехватить пароли. Причем проблема не может быть устранена путем обновления программного обеспечения, поэтому устранить уязвимость нельзя. Чтобы защититься, вам остается только следить за устройствами, подключенными к компьютеру: не используйте подозрительные устройства с USB-C и не подпускайте незнакомых людей». ***(В чипе Apple T2 для iMac и MacBook нашли серьезную уязвимость: к чему это может привести и как уберечься // информационный портал "ua.today" (http://ua.today/news/technology_and_science/v_chipe_apple_t2_dlya_imac_i_macboo***

k_nashli_sereznuyu_uyazvimost_k_chemu_eto_mozhet_privesti_i_kak_uberechsya). 07.10.2020).

***

«Microsoft предупреждает, что киберпреступники начали использовать код эксплойта для уязвимости ZeroLogon в своих атаках. Предупреждение поступило после того, как компания заметила продолжающиеся атаки со стороны кибершпионажа MuddyWater (SeedWorm) во второй половине сентября.

На этот раз злоумышленником является TA505, злоумышленник, который неизбирательно относится к жертвам, которых он атакует, с историей, начинающейся с распространения банковского трояна Dridex в 2014 году.

На протяжении многих лет он участвовал в атаках с использованием самых разных вредоносных программ, от бэкдоров до программ-вымогателей.

В последнее время за вторжениями этой группы последовало развертывание программы-вымогателя Clop, как в прошлогодней атаке на Маастрихтский университет, в результате которой был уплачен выкуп в размере 30 биткойнов (около 220 000 долларов США).

Поддельные обновления и легальные инструменты

Microsoft утверждает, что TA505, которую она отслеживает как Chimborazo, развернула кампанию с поддельными обновлениями программного обеспечения, которые подключаются к инфраструктуре управления и контроля (C2) злоумышленника.

Целью вредоносных обновлений является предоставление хакерам повышенных привилегий (обход контроля учетных записей пользователей) в целевой системе и запуск вредоносных сценариев.

Для второй части TA505 использует Windows Script Host (WScript.Exe), который позволяет выполнять сценарии на различных языках программирования, включая VBScript, Python, Ruby, PHP, JavaScript и Perl.

Microsoft заявляет, что злоумышленники компилируют версию инструмента постэксплуатации Mimikatz, используя Microsoft Build Engine (MSBuild.Exe) n для создания приложений.

Полученная таким образом версия Mimikatz включает код эксплойта для уязвимости ZeroLogon (CVE-2020-1472). За последний месяц многочисленные исследователи выпустили экспериментальные эксплойты для устранения этой уязвимости.

В короткой беседе Microsoft описала классическую атаку с захватом домена, для которой ZeroLogon идеально подходит. Он предлагает прямой доступ к контроллеру домена, поэтому злоумышленнику больше не нужно тратить время на получение учетных данных администратора.

Поскольку TA505 занимается крупномасштабным бизнесом по вымогательству, организациям следует уделять приоритетное внимание применению исправлений безопасности для этой уязвимости, поскольку атаки, подобные тем, что описала Microsoft, могут происходить с большей частотой.

Доступны детали ZeroLogon

Обнаруженный Томом Тервоортом из Secura, ZeroLogon позволяет злоумышленникам в доменной сети увеличивать права до уровня администратора без необходимости аутентификации.

Тервоорт обнаружил, что он может принудительно установить соединение с контроллером домена через Netlogon Remote Protocol в незашифрованном состоянии (незащищенная связь RPC).

Затем, используя уязвимость в алгоритме шифрования Netlogon, можно подделать логин администратора домена. Техническая рецензия доступно из Секуры.

На данный момент Microsoft устранила эту уязвимость частично, предотвратив обмен данными с контроллером Windows Active Domain через незащищенный RPC. Это обновление доступно с 11 августа.

Однако 9 февраля новое обновление обеспечит такую же безопасную связь для всех устройств в сети.

Предупреждения выпущены

Сетевые администраторы получали неоднократные предупреждения о серьезности уязвимости ZeroLogon (максимальная критическая оценка 10/10) и призывали применить текущий патч.

С выпуском кода эксплойта (права администратора домена за секунды), выпущенного с середины сентября, злоумышленники быстро начали использовать его в своих атаках.

18 сентября Агентство США по кибербезопасности и безопасности инфраструктуры (CISA) потребовало от Федеральной гражданской исполнительной власти отнестись к устранению неисправности как к чрезвычайной ситуации.

Microsoft впервые забила тревогу 23 сентября, когда увидела, что ZeroLogon активно используется в атаках. Затем появилось предупреждение о том, что MuddyWater использует эксплойт.

Теперь им владеют киберпреступники, что является явным признаком того, что ZeroLogon находится на пути принятия широким кругом групп угроз, нацеленных на организации как в государственном, так и в частном секторе». ***(Ionut Ilascu. Ransomware gang now using critical Windows flaw in attacks // BleepingComputer.com(https://www.bleepingcomputer.com/news/security/ransomware-gang-now-using-critical-windows-flaw-in-attacks/). 09.10.2020).***

***

«Apple выплатила группе хакеров награду в размере почти 300 тыс. долларов за обнаружение 55 уязвимостей в системах компании.

Хакерская группа состоит из 5 человек: Сем Карри, Бретт Бауэрхаус, Бен Садегипур, Семиюэль Эрба и Таннер Барнс. Хакеры потратили 3 месяца на исследования кибербезопасности технокорпорации и обнаружили 55 уязвимостей в ее системах. Из них 11 с критической серьёзностью, 29 высокой степени, 13 среднего уровня и 2 низкой степени серьезности.

"В процессе наших исследований мы обнаружили множество уязвимостей в ключевых элементах инфраструктуры, используя которые киберпреступники могли полностью скомпрометировать приложения и получить полный доступ к данным

клиентов Apple и сотрудников компании, запустить червя, способного автоматически захватить учётную запись iCloud, получить доступ к исходному коду внутренних проектов Apple, полностью скомпрометировать программное обеспечение складов компании и дать доступ к управлению внутренними инструментами управления и конфиденциальным данным сотрудников корпорации." - написали хакеры в своем блоге.

Apple со своей стороны заявила, что все обнаруженные уязвимости были исправлены и повторно проверены, неисправности были устранены в течение 4-6 часов с момента из обнаружения. - сообщается в блоге компании». ***(Романов Роман. Apple выплатила награду хакерам 300 тыс. долларов за обнаружение критических уязвимостей в системах компании // Internetua (https://internetua.com/apple-vyplatila-nagradu-hakeram-300-tys-dollarov-za-obnarujenie-kriticseskih-uyazvimostei-v-sistemah-kompanii-). 10.10.2020).***

***

«В системе видеоконференцсвязи Cisco Webex, IP-камерах Cisco для видеонаблюдения серии 8000 и Identity Services Engine существуют три серьезных недостатка.

Cisco выпустила исправления для уязвимостей высокой степени серьезности, которыми страдают ее популярная система видеоконференцсвязи Webex, IP-камеры видеонаблюдения и продукт сетевого администрирования Identity Services Engine.

В целом Cisco в среду выявила три уязвимости высокой степени серьезности и 11 уязвимостей средней степени серьезности.

Самым серьезным из них является недостаток (CVE-2020-3544) в IP -камерах Cisco для видеонаблюдения серии 8000, который занимает 8,8 балла из 10 по шкале CVSS.

«Уязвимость в реализации протокола Cisco Discovery Protocol [CDP] для IP-камер Cisco Video Surveillance 8000 Series может позволить неаутентифицированному злоумышленнику, находящемуся рядом, выполнить произвольный код на уязвимом устройстве или вызвать перезагрузку устройства», - говорится в рекомендациях Cisco по безопасности.

CDP - это инструмент сетевого обнаружения, который помогает сетевым администраторам идентифицировать соседние устройства Cisco. Уязвимость возникает из-за отсутствия проверок при обработке IP-камерой пакета CDP.

Чтобы воспользоваться уязвимостью, злоумышленнику не требуется проходить проверку подлинности. Однако человек должен находиться в том же широковещательном домене, что и затронутое устройство - поскольку CDP является протоколом уровня 2, злоумышленники должны быть смежными с уровнем 2.

«Злоумышленник может воспользоваться этой уязвимостью, отправив вредоносный пакет [CDP] на уязвимое устройство», - утверждает Cisco. «Успешный эксплойт может позволить злоумышленнику выполнить код на уязвимой IP-камере или вызвать ее неожиданную перезагрузку, что приведет к отказу в обслуживании (DoS)».

Уязвимость затрагивает камеры, на которых установлена прошивка более ранней, чем версия 1.0.9-5, для которых включен CDP, сообщила Cisco. Следует отметить, что IP-камеры Cisco Video Surveillance серии 8000 больше не продаются с 24 июля; однако поддержка уязвимостей и безопасности не закончится до 24 июля 2023 г.

Ошибка Webex

Cisco также исправила серьезную ошибку, влияющую на ее платформу Webex. Эта проблема является серьезной, учитывая, что множество сотрудников обращается к системам видеоконференцсвязи во время пандемии, однако ее очень сложно использовать, поскольку злоумышленник должен быть как аутентифицирован (требуя действительных учетных данных в системе Windows), так и локально.

Уязвимость возникает из-за неправильной обработки путей к каталогам во время выполнения. Злоумышленник может воспользоваться этой уязвимостью, поместив вредоносный файл DLL в определенное место в целевой системе, который затем будет запускаться при запуске уязвимого приложения.

«Успешный эксплойт может позволить злоумышленнику выполнить произвольный код в целевой системе с привилегиями учетной записи другого пользователя», - утверждает Cisco.

Недостаток (CVE-2020-3535) влияет на Cisco Webex Teams для Windows версий 3.0.13464.0–3.0.16040.0; это не влияет на Webex Teams для Android, Mac, iPhone и iPad.

Недостаток служб идентификации

Последний недостаток высокой степени серьезности (CVE-2020-3467) существует в веб-интерфейсе управления Cisco Identity Services Engine (ISE), инструменте, который позволяет создавать и применять политики безопасности и доступа для оконечных устройств, подключенных к компании. маршрутизаторы и коммутаторы. Уязвимость позволяет удаленным злоумышленникам, прошедшим проверку подлинности (с действующими учетными данными администратора, доступными только для чтения), изменять части конфигурации на уязвимом устройстве.

Ошибка возникает из-за неправильного применения управления доступом на основе ролей (RBAC) в веб-интерфейсе управления.

«Злоумышленник может воспользоваться этой уязвимостью, отправив обработанный HTTP-запрос на уязвимое устройство», - утверждает Cisco. «Успешный эксплойт может позволить злоумышленнику изменить части конфигурации. Измененная конфигурация может либо разрешить неавторизованным устройствам подключаться к сети, либо запретить авторизованным устройствам доступ к сети». Cisco заявила, что ей неизвестны какие-либо публичные эксплойты для какой-либо из трех ошибок». ***(Lindsey O'Donnell. Cisco Fixes High-Severity Webex, Security Camera Flaws // Threatpost (https://threatpost.com/cisco-webex-security-camera-flaws/159969/). 08.10.2020).***

***

«ZDNet сообщает, что список вакансий Google пополнился рядом новых должностей. Дело в том, что в компании создают новую команду безопасности Android, которой будет поручено искать уязвимости в особо важных приложениях из Google Play Store.

По словам Себастьяна Порста (Sebastian Porst), менеджера по разработке ПО для Google Play Protect, продукты, на которых сосредоточится внимание новой команды специалистов, в частности, включают приложения для отслеживания контактов COVID-19, а также приложения, связанные с выборами.

По сути, специалисты Google продолжат то, чем сейчас занимаются независимые исследователи в рамках bug bounty программы Google Play Security Reward. Напомню, что эта инициатива поощряет поиск багов в сторонних приложениях из Google Play Store, а эксперты Google принимают отчеты об ошибках и выплачивают вознаграждения от имени владельцев приложений.

При этом существующая bug bounty программа ограничена приложениями, насчитывающими более 100 000 пользователей. Однако приложения, работающие с конфиденциальными данными, а также связанные с критически важными задачами, далеко не всегда соответствуют условиям Google Play Security Reward, а значит, вряд ли будут проверены охотниками за багами». ***(Мария Нефёдова. Google создаст специальную команду для поиска багов в особо важных приложениях // Xakep (https://xakep.ru/2020/10/02/special-android-security-team/). 02.10.2020).***

***

«Специалисты компании CyberArk Labs опубликовали отчет, согласно которому высокие привилегии антивирусного ПО делают его более уязвимыми. В итоге защитные решения могут использоваться для атак с манипуляциями с файлами, и малварь получать повышенные права в системе.

Ошибки такого рода были обнаружены в продуктах Kaspersky, McAfee, Symantec, Fortinet, Check Point, Trend Micro, Avira и Microsoft Defender. В настоящее время все проблемы уже устранены разработчиками, а присвоенные им идентификаторы можно увидеть ниже (решения Avast и F-Secure пока ожидают присвоения CVE)…

Главным из обнаруженных в антивирусах недостатков исследователи называют возможность удалять файлы из произвольных мест, что позволяет злоумышленнику стереть любой файл в системе. Также отмечается похожая уязвимость, связанная с повреждением файлов, которая позволяет удалить содержимое любого файла в системе.

Согласно отчету, проблемы в основном возникают из-за дефолтных списков DACL (Discretionary Access Control Lists) для папки C:\ProgramData в Windows, которая используется приложениями для хранения данных пользователей без дополнительных разрешений. Так как каждый пользователь имеет права на запись и удаление на базовом уровне каталога, растет вероятность злоупотребления повышением привилегий, когда непривилегированный процесс создает новую папку в ProgramData, к которой впоследствии может получить доступ привилегированный процесс.

Было замечено, что когда два разных процесса (один привилегированный, а другой запущенный от лица аутентифицированного локального пользователя) совместно используют один и тот же лог-файл, злоумышленник может использовать привилегированный процесс для удаления файла и создания символической ссылки, которая будет указывать на произвольный файл с вредоносным содержимым.

Также аналитики CyberArk Labs изучили возможность создания новой папки в C:\ProgramData перед выполнением привилегированного процесса. В частности, они обнаружили, что процесс установки антивируса McAfee запускается после создания папки McAfee, и в это время стандартный пользователь имеет полный контроль над каталогом, может получить повышенные привилегии и выполнить атаку с использованием символической ссылки.

Кроме того, исследователи сообщают, что продукты Trend Micro, Fortinet и так далее могли использоваться для помещения вредоносного DLL-файла в каталог приложения и последующего повышения привилегий». ***(Мария Нефёдова. Эксперты CyberArk Labs выявили баги в популярных антивирусах // Xakep (https://xakep.ru/2020/10/06/av-bugs/). 06.10.2020).***

***

«Microsoft выплатила ИБ-исследователям вознаграждения на сумму 374 300 долларов США в рамках конкурса Azure Sphere Security Research Challenge, который длился три месяца. В общей сложности экспертам удалось обнаружить 20 важных уязвимостей. Баги были исправлены с релизом обновлений 20.07, 20.08 и 20.09.

Всего в конкурсе приняли участие 70 исследователей из 21 страны мира. Они представили на суд компании 40 отчетов, 30 из которых привели к выпуску патчей, а 16 удостоились выплат по программе bug bounty (в общей сложности 374 300 долларов). Самое крупное выплаченное вознаграждение составило 48 000 долларов США, а наименьшее — 3 300 долларов США.

В рамках исследования компания Microsoft пригласила к участию ведущих мировых экспертов в области кибербезопасности, а также поставщиков решений для обеспечения безопасности, чтобы они попытались взломать продукты компании, используя виды атак, наиболее часто используемых злоумышленниками. Участникам конкурса был предоставлен комплект разработчика, прямая связь с командой обеспечения безопасности ОС, поддержка по электронной почте, а также публично доступный код ядра операционной системы.

Целью конкурса было сосредоточить внимание исследователей на том, что оказывает наибольшее влияние на безопасность клиентов. Поэтому экспертам было предоставлено шесть сценариев исследования с дополнительным вознаграждением до 20% сверх стандартного вознаграждения в рамках программы Azure Bounty (до 40 000 долларов), а также 100 000 долларов за два высокоприоритетных сценария.

Исследование проводилось в партнерстве с компаниями Avira, Baidu International Technology, Bitdefender, Bugcrowd, Cisco Systems Inc (Talos), ESET, FireEye, F-Secure Corporation, HackerOne, K7 Computing, McAfee, Palo Alto Networks и Zscaler.

Эксперты McAfee уже опубликовали детальный отчет о своих изысканиях, прочесть который можно в блоге компании. Исследователи заявили, что заработали 160 000 долларов, которые планируют пожертвовать на благотворительность. Так, им удалось получить root-доступ, объединив шесть ошибок, три из которых были признаны критическими. Также аналитики McAfee нашли ранее неизвестную уязвимость в ядре Linux.

Свои выводы уже представили и специалисты компании Cisco Talos. Они выявили более десятка проблем, включая выполнение произвольного кода, отказ в обслуживании (DoS), раскрытие информации и повышение привилегий». ***(Мария Нефёдова. Microsoft выплатила 374 000 долларов за уязвимости в Azure Sphere // Xakep (https://xakep.ru/2020/10/09/azure-sphere-security-research-challenge/). 09.10.2020).***

***

«Национальный центр кибербезопасности Великобритании (NCSC) сегодня выпустил предупреждение, в котором подчеркиваются риски, связанные с недавно устраненной уязвимостью удаленного выполнения кода (RCE) CVE2020-16952 в Microsoft SharePoint Server.

NCSC, подразделение кибербезопасности британской разведывательной службы GCHQ, призывает организации убедиться, что все продукты Microsoft SharePoint в их средах имеют исправления против CVE-2020-16952, чтобы блокировать попытки поглощения.

«NCSC настоятельно рекомендует организациям обратиться к руководству Microsoft, упомянутому в этом предупреждении, и обеспечить установку необходимых обновлений в уязвимых продуктах SharePoint», - говорится в предупреждении.

Доступен экспериментальный эксплойт

Об уязвимости серверного включения (SSI) сообщил специалист по информационной безопасности Стивен Сили из Qihoo 360 Vulcan Team, который обнаружил, что она затрагивает Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Foundation 2013 с пакетом обновления 1 и Microsoft SharePoint Server 2019.

Seeley также предоставляет экспериментальный эксплойт, предназначенный для демонстрации того, как эту уязвимость можно использовать для удаленного выполнения произвольного кода.

CVE-2020-16952 позволяет злоумышленникам удаленно выполнять код после успешной эксплуатации в контексте локального администратора.

Аутентификация также требуется для использования уязвимости, при этом прошедшему проверку подлинности злоумышленнику требуются права на создание страницы (разрешение SharePoint по умолчанию) - дополнительную информацию о внутренней работе CVE-2020-16952, предоставленную фирмой Rapid7, занимающейся кибербезопасностью, можно найти здесь.

«CVE-2020-16952 представляет более высокий риск для многопользовательских сред, т. Е. Нескольких организаций, использующих одну и ту же среду SharePoint и / или Active Directory», - считают исследователи Rapid7.

Для защиты от атак, направленных на использование этой уязвимости, ИТ-администраторам рекомендуется применить обновления безопасности SharePoint за октябрь 2020 г.

Подробную информацию о том, как защитить уязвимые экземпляры Microsoft SharePoint, можно найти в KB4486676 для SharePoint 2019, в KB4486677 для SharePoint 2016 и в рекомендации KB4486694 для SharePoint 2013.

Риски незащищенных уязвимостей Sharepoint

Хотя пока нет сообщений о том, что эта уязвимость используется в дикой природе, риск того, что это произойдет, велик, учитывая, что уже доступен экспериментальный эксплойт.

Модуль эксплойтов также разрабатывается для среды тестирования на проникновение Metasploit с открытым исходным кодом и уже успешно протестирован с SharePoint 2019 на Windows Server 2016.

После того, как Microsoft выпустила обновления безопасности CVE-2020-16952 для всех поддерживаемых продуктов SharePoint (SharePoint 2013, 2016 и 2019) в рамках октябрьского вторника исправлений 2020 года, Rapid7 использовала данные, собранные до 5 октября, и обнаружила примерно 15000 служб SharePoint на 443 / tcp. доступные услуги.

Было обнаружено, что большинство из этих экземпляров SharePoint, доступных из Интернета, работают с SharePoint 2010 и 2013, с примерно 5300 серверами SharePoint 2010 и примерно 6400 серверами SharePoint 2013…

Учитывая, что серверы SharePoint используются в корпоративных средах, они также являются чрезвычайно привлекательной целью для злоумышленников, стремящихся найти и атаковать важные цели.

NCSC заявляет, что «ранее было замечено большое количество случаев использования уязвимостей SharePoint, таких как CVE-2019-0604, против британских организаций».

Вместе с CVE-2015-1641 эти две уязвимости присутствуют в списке наиболее используемых уязвимостей с 2016 года, опубликованном в совместных рекомендациях Агентства по кибербезопасности и безопасности инфраструктуры США (CISA) и Федерального бюро расследований (FBI).

Оба они используются для удаления вредоносных программ, таких как China Chopper, Toshliph и UWarrior, в корпоративных сетях, где работают службы SharePoint, которые не обновлялись в течение многих лет…». ***(Sergiu Gatlan. UK urges orgs to patch severe CVE-2020-16952 SharePoint RCE bug // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/uk-urges-orgs-to-patch-severe-cve-2020-16952-sharepoint-rce-bug/). 16.10.2020).***

***

«Агентство национальной безопасности США (АНБ) предупреждает, что китайские хакеры, спонсируемые государством, используют 25 различных уязвимостей в атаках на организации и интересы США.

В одном совещательным опубликованном сегодня, АНБ сказал, что он знает о целенаправленных нападений со стороны китайских спонсируемых государством хакеров против системы безопасности Национального (СНБ), промышленной базы

Министерства обороны США (DIB) и Министерства обороны (MO) информационных сетей.

В рамках этих атак АНБ обнаружило, что двадцать пять публично раскрытых уязвимостей использовались для получения доступа к сетям, развертывания вредоносных мобильных приложений и распространения в системе, в то время как злоумышленники воруют конфиденциальные данные.

АНБ рекомендует всем организациям немедленно устанавливать исправления на уязвимые устройства для защиты от кибератак, которые приводят к краже данных, банковскому мошенничеству и атакам программ-вымогателей.

«Мы четко и ясно слышим, что может быть трудно определить приоритеты усилий по установке исправлений и смягчению последствий», - заявила директор по кибербезопасности АНБ Энн Нойбергер.

«Мы надеемся, что, подчеркнув уязвимости, которые Китай активно использует для взлома систем, профессионалы в области кибербезопасности получат действенную информацию, чтобы определить приоритеты усилий и защитить свои системы».

Уязвимости, используемые на разных этапах атаки

Агентство национальной безопасности разделило уязвимости на разные категории, чтобы проиллюстрировать, как они используются в кибератаках.

Используйте безопасный удаленный доступ: чтобы получить доступ к сетям, китайские злоумышленники используют семь различных уязвимостей, многие из которых также предоставляют учетные данные, которые можно использовать для дальнейшего распространения в сети.

CVE-2019-11510 - уязвимости Pulse Secure VPN, которые позволяют неаутентифицированному злоумышленнику получить доступ к учетным данным VPN.

CVE-2020-5902 - уязвимость прокси-сервера / балансировщика нагрузки F5 BIG-IP® 8, связанная с удаленным выполнением кода.

CVE-2019-19781 - уязвимость Citrix Application Delivery Controller (ADC) и обхода каталога шлюза, которая может привести к удаленному выполнению кода без учетных данных.

CVE-2020-8193 - Уязвимость Citrix ADC, Citrix Gateway, Citrix SDWAN WAN-OP позволяет получить доступ без проверки подлинности к определенным конечным точкам URL и раскрытие информации пользователям с низким уровнем привилегий

CVE-2020-8195 - Уязвимость Citrix ADC, Citrix Gateway, Citrix SDWAN WAN-OP позволяет получить доступ без аутентификации к определенным конечным точкам URL и раскрытие информации пользователям с низким уровнем привилегий

CVE-2020-8196 - Уязвимость Citrix ADC, Citrix Gateway, Citrix SDWAN WAN-OP обеспечивает неаутентифицированный доступ к определенным конечным точкам URL и раскрытие информации пользователям с низким уровнем привилегий

CVE-2019-0708 - уязвимость службы удаленного рабочего стола Windows BlueKeep позволяет пользователям, не прошедшим проверку подлинности, выполнять удаленное выполнение кода.

Использование управления мобильными устройствами (MDM) : компрометируя серверы MDM, злоумышленники могут выталкивать вредоносные мобильные приложения или изменять конфигурации устройств, которые отправляют трафик через прокси-серверы или узлы, контролируемые злоумышленником.

CVE-2020-15505 - уязвимость удаленного выполнения кода в системе управления мобильными устройствами MobileIron 13 (MDM).

Используйте Active Directory для бокового перемещения и доступа к учетным данным:

CVE-2020-1472 - критическая уязвимость 10/10 Windows ZeroLogon Netlogon, связанная с повышением привилегий, позволяет злоумышленникам быстро получить доступ к учетным данным администратора домена на контроллере домена. Оттуда они могут собирать конфиденциальные данные или развертывать вредоносное ПО, например программы-вымогатели.

CVE-2019-1040 - уязвимость Windows NTLM позволяет злоумышленникам снизить встроенную безопасность операционной системы Windows.

Использовать общедоступные серверы: злоумышленники используют эти уязвимости для обхода аутентификации на веб-серверах, почтовых серверах или DNS для удаленного выполнения команд во внутренней сети. В случае скомпрометированных веб-серверов злоумышленники могут использовать их для атак с целью нацеливания на будущих посетителей.

CVE-2020-1350 - Уязвимость SigRed DNS-сервера Windows позволяет злоумышленникам распространяться через сеть.

CVE-2018-6789 - уязвимость почтового сервера Exim позволяет удаленное выполнение кода без аутентификации.

CVE-2018-4939 - уязвимость Adobe ColdFusion 14, которая может привести к выполнению произвольного кода.

Использование внутренних серверов: эти уязвимости используются для латерального распространения по сети и получения доступа к внутренним серверам, где злоумышленники могут украсть ценные данные.

CVE-2020-0688 - уязвимость Microsoft Exchange, которая позволяет пользователям, проверку подлинности, выполнять удаленное выполнение кода.

CVE-2015-4852 - Компонент WLS Security в Oracle WebLogic15 Server позволяет удаленным злоумышленникам выполнять произвольные команды через созданный сериализованный объект Java16.

CVE-2020-2555 - в продукте Oracle® Coherence промежуточного программного обеспечения Oracle Fusion® существует уязвимость. Этот легко эксплуатируемый

CVE-2019-3396 - в соединителе виджетов на серверах Atlassian Confluence присутствует уязвимость серверного внедрения шаблона, которая позволяет удаленным злоумышленникам выполнять удаленное выполнение кода и обход пути.

CVE-2019-11580 - злоумышленники, которые могут отправлять запросы к экземпляру Atlassian® Crowd или Crowd Data Center, могут использовать эту уязвимость для установки произвольных подключаемых модулей, разрешающих удаленное выполнение кода. Эта уязвимость использовалась в атаках вымогателей GandCrab в прошлом.

CVE-2020-10189 - уязвимость Zoho ManageEngine 18 Desktop Central делает возможным удаленное выполнение кода. Этот баг использовался в атаках на развертывание бэкдоров.

CVE-2019-18935 - Уязвимость в пользовательском интерфейсе Telerik 19 для ASP.NET AJAX может привести к удаленному выполнению кода. Было замечено, что он использовался хакерской группой под названием «Blue Mockingbird» для установки майнеров Monero на уязвимых серверах, но также мог использоваться и для горизонтального распространения.

Используйте рабочие станции пользователей для повышения локальных привилегий: когда злоумышленник получает доступ к рабочей станции, его конечной целью является получение учетных данных или прав администратора. Используя эти уязвимости, хакер может повысить свои привилегии до СИСТЕМНЫХ или административных.

CVE-2020-0601 - Уязвимость Windows CryptoAPI Spoofing, обнаруженная АНБ, позволяет злоумышленникам подделывать сертификаты для подписи кода, чтобы вредоносные исполняемые файлы выглядели подписанными законной доверенной компанией.

CVE-2019-0803 - В Windows® существует уязвимость, приводящая к несанкционированному получению прав, когда компонент Win32k не может должным образом обрабатывать объекты в памяти.

Использовать сетевые устройства: эта последняя группа уязвимостей позволяет злоумышленникам отслеживать и изменять сетевой трафик по мере его прохождения через устройство.

CVE-2017-6327 - Symantec 22 Messaging Gateway может столкнуться с проблемой удаленного выполнения кода.

CVE-2020-3118 - уязвимость Cisco "CDPwn" в реализации протокола Cisco Discovery для программного обеспечения Cisco IOS 23 XR делает возможным удаленное выполнение кода.

CVE-2020-8515 - устройства DrayTek Vigor 24 позволяют удаленное выполнение кода от имени пользователя root (без аутентификации) с помощью метасимволов оболочки

Поскольку было замечено, что хакеры, спонсируемые государством Китая, использовали комбинацию этих уязвимостей, всем администраторам настоятельно рекомендуется исправить их как можно скорее». ***(Sergiu Gatlan. NSA: Top 25 vulnerabilities actively abused by Chinese hackers // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/nsa-top-25-vulnerabilities-actively-abused-by-chinese-hackers/). 20.10.2020).***

***

«TikTok расширил свою политику раскрытия уязвимостей, включив в нее глобальную программу вознаграждения за ошибки в партнерстве с этической хакерской платформой HackerOne. Запуск программы bug-bounty сигнализирует о новом направлении для китайского приложения для обмена видео, которое сильно критиковали за сомнительные методы обеспечения безопасности.

Хакеры, обнаружившие критические уязвимости в платформе TikTok, могут получить от 6900 до 14800 долларов в соответствии с программой, что является первым случаем, когда TikTok пригласил сообщество общественной безопасности для анализа своей платформы на наличие уязвимостей.

«Это партнерство поможет нам получить представление от исследователей верхней безопасности в мире, академических ученых и независимых экспертов, чтобы лучше открывайте потенциальные угрозы и сделать средства защиты безопасности TikTok даже сильнее,» Луна В из глобальной команды безопасности TikTok сказала в четверг в блоге пост раскрыв партнерство.

Программа предлагает этичным хакерам представить широкий спектр уязвимостей в приложении, в том числе связанные с: XSS, CSRF, SSRF, SQL Injection, ROP или JOP; воспроизводимые сбои со следами стека; утечка или жестко закодированные конфиденциальные учетные данные; пригодные для использования, опасные API; атаки с перехватом управления потоком; утечки пользовательских данных; уязвимости аутентификации или авторизации; или доступ к внутренним ресурсам TikTok.

Полный список уязвимостей, на которые распространяется программа, доступен на целевой странице TikTok. По словам Ву, для отправки ошибок на оценку в рамках программы исследователи могут использовать онлайн-форму.

Вознаграждения программы основаны на серьезности согласно Стандарту оценки общих уязвимостей (CVSS), который используется повсеместно для оценки риска уязвимостей безопасности. В дополнение к наивысшим вознаграждениям за ошибки, получившие критические оценки, хакеры могут заработать от 1700 до 6900 долларов за уязвимости с рейтингом «высокий»; От 200 до 1700 долларов за ошибки с рейтингом «средний»; и от 50 до 200 долларов за ошибки с «низким» риском.

TikTok, принадлежащий китайской ByteDance, был запрещен в некоторых странах и был на пути к той же участи в Соединенных Штатах, в основном из-за его мер безопасности, связанных с предполагаемыми уютными отношениями ByteDance с коммунистическим правительством Китая, которые, по мнению экспертов, данные его 100 миллионов пользователей в США подвергаются риску. Приложение использовало различные тактики для сбора данных с устройств Android и iPhone без ведома пользователей, среди других сомнительных методов.

В преддверии запрета США, TikTok владелец ByteDance достиг соглашения о продаже значительных долей собственности на Oracle и Walmart, сделка, которая в настоящее время находится на рассмотрении. Oracle согласилась приобрести 12,5% акций китайской компании, а Walmart - 7,5%; вместе компании заплатят в общей сложности 12 миллиардов долларов за 20-процентную долю владения для покрытия операций TikTok в США.

Неясно, является ли эта сделка тем, что побуждает хранителей TikTok быть более прозрачными в отношении безопасности приложений, но расширенная программа вознаграждений за ошибки, вероятно, улучшит ее общую безопасность и, следовательно, ее положение в мире технической безопасности в целом, считают наблюдатели. Наряду с партнерством с HackerOne, TikTok также выпускает серию видеороликов, в которых сотрудники призывают пользователей соблюдать правила кибергигиены.

«Такие программы могут привлекать разнообразных талантливых исследователей, которые могут рассматривать приложения с уникальными перспективами и опытом, которые не обязательно могут быть доступны в группах внутренней безопасности», - сказал Тим Макки, главный стратег по безопасности CyRC в Synopsys. электронное письмо в Threatpost.

Он отметил, что шаг TikTok идет по пятам за тем, что Apple расширила свою ранее частную программу вознаграждения за ошибки в публичную сферу, что уже привело к раскрытию ряда ключевых уязвимостей для технологического гиганта.

Учитывая, что TikTok наиболее популярен среди подростков, которые, вероятно, не очень задумываются о том, как приложения, которые они используют, могут шпионить за ними, программа также «может значительно улучшить общую безопасность их взаимодействия с приложениями и управлять данными, которые они создали», - добавил Макки». ***(Elizabeth Montalbano. TikTok Launches Bug Bounty Program Amid Security SNAFUs // Threatpost (https://threatpost.com/tiktok-bug-bounty-security/160203/). 16.10.2020).***

***

«Компания Cisco Talos опубликовала подробную информацию о ряде DoS-уязвимостей, обнаруженных одним из ее исследователей в продукте промышленной автоматизации от Rockwell Automation.

Проблемы содержатся в адаптере Allen-Bradley Flex IO 1794-AENT/B. В общей сложности было выявлено пять опасных уязвимостей (CVE-2020-6084, CVE-2020-6085, CVE-2020-6086, CVE-2020-6087 и CVE-2020-6088), связанных с переполнением буфера. Они затрагивают версии адаптера 4.003 и старше.

Удаленный неавторизованный злоумышленник может проэксплуатировать уязвимости и вызвать состояние «отказа в обслуживании» путем отправки специально сформированных пакетов.

Специалисты сообщили об уязвимостях Rockwell Automation в феврале. Поставщик дважды просил отсрочить публикацию сведений об уязвимостях, но после третьего запроса Talos сообщила, что уязвимости будут раскрыты 12 октября независимо от того, будет ли выпущен патч.

Rockwell Automation выпустили рекомендации, включающие прием CIP-соединений только из надежных источников на порт 44818, использование сегментации сети и средств управления безопасностью для минимизации уязвимости затронутых устройств, а также использование межсетевых экранов, VPN и других средств управления сетевой инфраструктурой». ***(В промышленном адаптере от Rockwell Automation обнаружены DoS-уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/513105.php). 15.10.2020).***

***

«Эксперт компании Positive Technologies Никита Абрамов обнаружил 11 уязвимостей в программном обеспечении SonicWall Network Security Appliance (NSA). Самая опасная из них (CVE-2020-5135) является критической и содержится в службе HTTP/HTTPS, используемой для управления продуктами, а также для удаленного доступа SSL VPN. Эта же уязвимость независимо от эксперта была обнаружена специалистами Tripwire VERT.

Злоумышленник может проэксплуатировать данную уязвимость путем отправки неаутентифицированного HTTP-запроса с использованием специального обработчика протокола с целью вызвать состояние «отказа в обслуживании». Как отметили эксперты, существует возможность перенаправления потока выполнения через повреждение стека, что указывает на возможное выполнение произвольного кода.

Однако для осуществления атаки с выполнением кода злоумышленнику потребуется использовать утечку информации и провести некоторый анализ.

«Если кто-то потратит время на подготовку полезной RCE-нагрузки, он, скорее всего, сможет создать крупный ботнет с помощью червя», — пояснил эксперт.

Пока что не было зафиксировано никаких признаков эксплуатации уязвимости, но результаты поискового запроса Shodan выявили около 460 тыс. уязвимых устройств.

Уязвимость затрагивает версии SonicOS 6.5.4.7-79n и старше, SonicOS 6.5.1.11-4n и старше, SonicOS 6.0.5.3-93o и старше, SonicOSv 6.5.4.4-44v-21-794 и старше и SonicOS 7.0.0.0-1.

Остальные проблемы включают ряд DoS-уязвимостей (CVE-2020-5133, CVE-2020-5138 и CVE-2020-5139), уязвимость переполнения буфера (CVE-2020-5137), и другие менее опасные уязвимости. SonicWall выпустила обновления, устраняющие обнаруженные проблемы. Порталы SSL VPN могут быть отключены от Сети в качестве временного решения перед применением исправления». ***(DoS-уязвимость в SonicWall VPN может привести к удаленному выполнению кода // SecurityLab.ru (https://www.securitylab.ru/news/513117.php). 16.10.2020).***

***

«Google опубликовала обновления для своего браузера Chrome, которое устраняет доселе не закрытую уязвимость в библиотеке рендеринга шрифтов, FreeType.

Сергей Глазунов, эксперт по кибербезопасности из команды Google Project Zero, уведомил компанию об этом баге в прошлый понедельник. Данная ошибка получила обозначение CVE-2020-15999 и высокий рейтинг опасности. Её относят к ошибкам, повреждающим память переполнением буфера кучи (heap buffer overflow).

К четвергу было готово обновление Chrome: стабильная версия 86.0.4240.111 для Windows, Mac & Linux содержала исправления пяти ошибок, в том числе и

упоминавшейся выше. В числе остальных, три (CVE-2020-16000/16001/16002) имеют высокий и одна (CVE-2020-16003) — средний уровень риска.

В блоге, анонсирующем это обновление, один из участников команды разработчиков Google Chrome, Прудхвикумар Боммана (Prudhvikumar Bommana), не вдаваясь в подробности сообщил, что Google располагает сведениями о фактах использования CVE-2020-15999 в преступных целях.

Технический лидер коллектива Project Zero, Бен Хоукс (Ben Hawkes), допускает, что уязвимыми могут оказаться другие реализации FreeType. Он отсылает пользователей к исходникам патча, которые Глазунов выложил на странице проекта FreeType, и призывает их подготовить исправления для других потенциально уязвимых программ.

«Исправление также есть в сегодняшней стабильной версии FreeType 2.10.4», — заявил Хоукс в Твиттере.

С это последней, за прошедшие 12 месяцев Google всего устранила три незакрытых (zero-day) уязвимости в браузере Chrome, включая критический баг удалённого выполнения кода, CVE-2019-13720, закрытый в Хэллоуин, и ошибку путаницы с памятью, CVE-2020-6418, которая была исправлена в феврале». ***(Google закрыла активно используемую хакерами уязвимость в Chrome // Компьютерное Обозрение (https://ko.com.ua/google_zakryla_aktivno_ispolzuemuyu_hakerami_uyazvimost_v_chrome_135017). 26.10.2020).***

***

«Федералы опубликовали список 25 лучших эксплойтов, изобилующий такими громкими именами, как BlueKeep, Zerologon и другими известными уязвимостями безопасности.

Китайские кибератаки, спонсируемые государством, активно компрометируют цели в США, используя множество известных уязвимостей безопасности, в том числе уязвимость Pulse VPN, претендующая на сомнительный титул «наиболее популярной ошибки» для этих групп.

Это согласно Агентству национальной безопасности (АНБ), которое опубликовало «25 лучших» эксплойтов, которые чаще всего используются связанными с Китаем продвинутыми постоянными угрозами (APT), включая такие, как Cactus Pete, TA413, Vicious Panda. и Виннити.

В сентябре ФРС предупредили, что китайские злоумышленники за последние месяцы успешно скомпрометировали несколько предприятий государственного и частного секторов; АНБ сейчас доводит до ясности точку зрения о необходимости исправлений на фоне этого шквала повышенной активности.

«Многие из этих уязвимостей могут быть использованы для получения первоначального доступа к сетям жертвы за счет использования продуктов, которые непосредственно доступны из Интернета,» предупредил АНБ, в вторник консультативно. «После того, как кибер-актор установил присутствие в сети из-за одной из этих уязвимостей удаленной эксплуатации, он может использовать другие уязвимости для дальнейшего использования сети изнутри».

APT - китайские и другие - активизировали свои усилия по кибершпионажу после пандемии, а также в преддверии выборов в США в следующем месяце. Но Хлоя Мессдаги, вице-президент по стратегии в Point3 Security, отметила, что эти уязвимости способствуют продолжающемуся нарастанию атак.

«В прошлом году мы определенно увидели рост этой ситуации, и это продолжается», - сказала она. «Они пытаются собрать данные об интеллектуальной собственности. Китайские злоумышленники могут быть национальным государством, могут быть компанией или группой компаний, или просто группой злоумышленников, или отдельным лицом, пытающимся получить конфиденциальную информацию для использования и создания конкурентоспособных компаний... другими словами, для кражи и использования в собственных целях. усиление."

Pulse Secure, BlueKeep, Zerologon и другие

Множество хорошо известных и печально известных ошибок попали в топ-25 АНБ. Например, печально известная ошибка Pulse Secure VPN (CVE-2019-11510) является первым недостатком в списке.

Это ошибка произвольного чтения файлов, которая делает систему уязвимой для удаленных злоумышленников, не прошедших проверку подлинности. В апреле этого года Агентство по кибербезопасности и безопасности инфраструктуры (CISA) Министерства внутренней безопасности предупредило, что злоумышленники активно используют эту проблему для кражи паролей для проникновения в корпоративные сети. Фактически, это ошибка, которая лежит в основе фиаско программы-вымогателя Travelex, которая произошла в январе.

Компания Pulse Secure выпустила исправление в апреле 2019 года, но многие компании, столкнувшиеся с уязвимостью, до сих пор не применили его, предупреждает CISA.

Еще одна серьезная проблема для иностранных злоумышленников - это критический недостаток в устройствах прокси / балансировщика нагрузки F5 BIG-IP 8 (CVE-2020-5902). Эта ошибка удаленного выполнения кода (RCE) существует в пользовательском интерфейсе управления трафиком (TMUI) устройства, которое используется для настройки. Он позволяет полностью контролировать хост-машину при эксплуатации, обеспечивая перехват и перенаправление веб-трафика, расшифровку трафика, предназначенного для веб-серверов, и использование в качестве точки перехода в другие области сети.

В конце июня F5 выпустила срочное исправление ошибки, которая имеет оценку серьезности CVSS 10 из 10 «из-за отсутствия сложности, простоты вектора атаки и значительного влияния на конфиденциальность, целостность и доступность», - заявили исследователи. в то время. В июле при обыске Shodan были обнаружены тысячи устройств.

АНБ также отметило несколько уязвимостей в Citrix как китайские фавориты, в том числе CVE-2019-19781, обнаруженную в прошлый праздничный сезон. Ошибка существует в Citrix Application Delivery Controller (ADC) и Gateway, специализированном сетевом устройстве, предназначенном для повышения производительности и безопасности приложений, доставляемых через Интернет. Эксплойт может привести к RCE без учетных данных.

Когда она была впервые раскрыта в декабре, уязвимость не имела патча, и Citrix пришлось изо всех сил стараться выпустить исправления, но не раньше, чем появился открытый код эксплойта для проверки концепции (PoC), а также активные эксплойты и активность массового сканирования. для уязвимых продуктов Citrix.

Другие ошибки Citrix в списке включают CVE-2020-8193, CVE-2020-8195 и CVE-2020-8196.

Между тем, ошибки Microsoft широко представлены, в том числе ошибка BlueKeep RCE в службах удаленных рабочих столов (RDP), которая все еще находится под активной атакой через год после раскрытия. Ошибка, отслеживаемая как CVE-2019-0708, может быть использована неаутентифицированным злоумышленником, подключающимся к целевой системе с помощью RDP, для отправки специально созданных запросов и выполнения кода. По их словам, проблема с BlueKeep заключается в том, что исследователи считают его способным к червю, что может привести к катастрофе на уровне WannaCry.

Еще одна ошибка с именем в списке - Zerologon, уязвимость, связанная с повышением привилегий, которая позволяет неаутентифицированному злоумышленнику, имеющему сетевой доступ к контроллеру домена, полностью скомпрометировать все службы идентификации Active Directory. Он был исправлен в августе, но многие организации остаются уязвимыми, и DHS недавно выпустило ужасное предупреждение об ошибке на фоне цунами атак.

Самая первая ошибка, о которой в Microsoft сообщило АНБ, CVE-2020-0601, также одобряется китайскими участниками. Эта уязвимость подмены, исправленная в январе, существует в том, как Windows CryptoAPI (Crypt32.dll) проверяет сертификаты Elliptic Curve Cryptography (ECC). Злоумышленник может воспользоваться этой уязвимостью, используя поддельный сертификат для подписи кода для подписи вредоносного исполняемого файла, создавая впечатление, что файл был получен из надежного законного источника.

Всего через неделю после выпуска январского бюллетеня по безопасности Microsoft, выпущенного во вторник, посвященного исправлению ошибок, были опубликованы два эксплойта для проверки концепции (PoC).

Кроме того, существует громкая ошибка RCE ключа проверки Microsoft Exchange (CVE-2020-0688), которая возникает из-за того, что сервер не может правильно создать уникальные ключи во время установки.

Это было исправлено в рамках февральских обновлений Microsoft Patch Tuesday - и в марте администраторы были предупреждены о том, что неустановленные серверы используются неназванными APT-участниками. Но по состоянию на 30 сентября по крайней мере 61% серверов Exchange 2010, 2013, 2016 и 2019 все еще оставались уязвимыми для уязвимости.

Лучшее из остальных

В списке 25 лучших, подготовленном АНБ, содержится множество вопросов, включая почти повсеместную ошибку RCE (CVE-2019-1040), которая, когда была раскрыта в прошлом году, затронула все версии Windows. Это позволяет злоумышленнику-посреднику обойти защиту NTLM Message Integrity Check.

Вот список других недостатков:

CVE-2018-4939 в некоторых версиях Adobe ColdFusion.

CVE-2020-2555 в продукте Oracle Coherence в Oracle Fusion Middleware.

CVE-2019-3396 в макросе Widget Connector в Atlassian Confluence Server

CVE-2019-11580 в Atlassian Crowd или Crowd Data Center

CVE-2020-10189 в Zoho ManageEngine Desktop Central

CVE-2019-18935 в пользовательском интерфейсе Progress Telerik для ASP.NET AJAX.

CVE-2019-0803 в Windows, проблема повышения привилегий в компоненте Win32k

CVE-2020-3118 в реализации протокола обнаружения Cisco для программного обеспечения Cisco IOS XR

CVE-2020-8515 в устройствах DrayTek Vigor

В сообщении также рассматриваются три более старых ошибки: одна при передаче почты exim‘a (CVE-2018-6789); один в Symantec Messaging Gateway (CVE-2017-6327); и один в компоненте безопасности WLS в Oracle WebLogic Server (CVE-2015-4852).

«Мы четко и ясно слышим, что может быть сложно определить приоритеты усилий по установке исправлений и смягчению последствий», - заявила директор по кибербезопасности АНБ Энн Нойбергер в заявлении для СМИ. «Мы надеемся, что, подчеркнув уязвимости, которые Китай активно использует для взлома систем, профессионалы в области кибербезопасности получат действенную информацию, чтобы определить приоритеты усилий и защитить свои системы». ***(Tara Seals. Bug Parade: NSA Warns on Cresting China-Backed Cyberattacks // Threatpost (https://threatpost.com/bug-nsa-china-backed-cyberattacks/160421/). 21.10.2020).***

***

«Компания Oracle выпустила обновления безопасности Critical Patch Update (CPU), исправляющие 402 уязвимости в различных продуктах. В новом CPU также содержится информация о ранее выпущенных исправлениях, с которыми клиентам рекомендуется ознакомиться.

Более половины из 402 исправленных уязвимостей в продуктах Oracle можно использовать удаленно без аутентификации. Более 80 критических уязвимостей получили оценку в 9,8 балла по шкале CVSS. Две из них (CVE-2020-1953 в Healthcare Foundation и CVE-2020-14871 в Solaris) получили максимальные оценки в 10 баллов по шкале CVSS.

Больше всего исправлений получили следующие продукты Oracle: приложения для финансовых служб (53 исправления — 49 уязвимостей могут быть использованы удаленно неавторизованным злоумышленником); MySQL (53 исправления — 4 уязвимости могут быть использованы удаленно); коммуникации (52 исправления — 41 уязвимость может быть использована удаленно); и Fusion Middleware (46 исправлений — 36 уязвимостей, которые можно использовать удаленно без аутентификации).

Меньшее количество исправлений получили — приложения для розничной торговли (28 исправлений), E-Business Suite (27), Database Server (18), PeopleSoft (15), Enterprise Manager (11), коммуникационные приложения (9), строительство и

проектирование (9), Hyperion (9), Java SE (8), системы (8), виртуализация (7), приложения для страхования (6), Policy Automation (6) и приложения для гостиничного бизнеса (6).

Многие из исправлений также устраняют различные другие уязвимости, а некоторые — десятки проблем. Например, исправление для опасной уязвимости в текстовом компоненте сервера базы данных (CVE-2020-14734) также содержит исправления для 38 дополнительных CVE». ***(Oracle исправила в своих продуктах более 80 критических уязвимостей // SecurityLab.ru (https://www.securitylab.ru/news/513304.php). 23.10.2020).***

***

«Спустя всего один месяц после раскрытия трех опасных уязвимостей в решениях для управления парком мобильных устройств MobileIron киберпреступники всех мастей начали активно эксплуатировать их для взломов корпоративных серверов и даже для организации вторжений в корпоративные сети.

Злоумышленники атакуют MDM-серверы от производителя программного обеспечения MobileIron. Аббревиатура MDM (Mobile Device Management) расшифровывается как «управление мобильными устройствами». MDM-системы используются на предприятиях для управления мобильными устройствами работников и позволяют системным администраторам с одного центрального сервера развертывать на них сертификаты, приложения, списки для контроля доступа, а также стирать данные с украденных устройств. Для этого MDM-серверы должны все время быть online и доступны через интернет, чтобы смартфоны удаленных сотрудников могли отправлять данные предприятию и получать последние обновления.

Летом нынешнего года исследователь безопасности компании DEVCORE Оранж Цай (Orange Tsai) обнаружил в MDM-решениях MobileIron три опасные уязвимости, сообщил о них производителю, и в июле было выпущено исправление. Поначалу Цай не публиковал подробности об уязвимостях (CVE-2020-15507, CVE-2020-15506 и самая опасная из них CVE-2020-15505), чтобы дать компаниям время на их исправление. Однако многие предприятия проигнорировали опасность и так и не установили обновления, поэтому в сентябре исследователь выложил всю информацию по трем уязвимостям.

Вскоре после публикации другие исследователи безопасности воспользовались предоставленными Цаем данными, написали PoC-эксплоиты для CVE-2020-15505 и опубликовали на GitHub.

Атаки не заставили себя долго ждать. Первая волна была зафиксирована в нынешнем месяце специалистами компании RiskIQ. Хотя они не представили подробностей об атаках, это сделали их коллеги из BlackArrow. Согласно отчету специалистов от 13 октября, злоумышленники атакуют MDM-решения MobileIron и включают их в DDoS-ботнет Kaiten.

Однако это еще не самое страшное. По данным Агентства национальной безопасности США, CVE-2020-15505 входит в топ-25 уязвимостей, эксплуатируемых хакерами, работающими на китайское правительство. Как

сообщает АНБ, китайские киберпреступники используют ее для получения первоначального доступа к подключенным к интернету устройствам, с помощью которых затем проникают в корпоративные сети». ***(Хакеры активно атакуют корпоративные MDM-серверы MobileIron // SecurityLab.ru (https://www.securitylab.ru/news/513274.php). 22.10.2020).***

***

«Project Zero, команда Google по поиску ошибок 0day, сегодня раскрыла уязвимость нулевого дня для повышения привилегий (EoP), обнаруженную в ядре Windows и активно используемую в целевых атаках.

Недостаток - это переполнение буфера на основе пула, которое существует в драйвере криптографии ядра Windows (cng.sys) и в настоящее время отслеживается как CVE-2020-17087.

Имеется доказательство концепции эксплойта

По словам исследователей безопасности Project Zero Матеуша Юрчика и Сергея Глазунова, локальные злоумышленники могут использовать уязвимость ядра Windows для повышения привилегий (включая выход из песочницы).

«Ошибка находится в функции cng! CfgAdtpFormatPropertyBlock и вызвана проблемой усечения 16-битных целых чисел», - объясняют исследователи.

Project Zero также предоставляет экспериментальный эксплойт (PoC), который можно использовать для сбоя уязвимых устройств Windows даже при конфигурации системы по умолчанию.

PoC был «протестирован на последней версии Windows 10 1903 (64-разрядная версия), но считается, что уязвимость присутствует, по крайней мере, с Windows 7.»

Атаки, не связанные с выборами в США

По словам Бена Хокса, руководителя технической группы исследовательской группы Google Project Zero, продолжающиеся атаки, использующие CVE-2020-17087 в дикой природе, не нацелены на цели, связанные с выборами в США.

«В настоящее время мы ожидаем, что исправление для этой проблемы будет доступно 10 ноября», - сказал Бен Хоукс, технический руководитель исследовательской группы Google Project Zero.

«Мы подтвердили с директором группы анализа угроз Google Шейном Хантли, что это целенаправленная эксплуатация и не имеет отношения к каким-либо целям, связанным с выборами в США».

Несмотря на то, что ошибка была добавлена в систему отслеживания проблем Project Zero всего 8 дней назад, она была обнаружена всего через 7 дней, поскольку использовалась злоумышленниками в «дикой природе».

На прошлой неделе Google также исправил активно используемую уязвимость нулевого дня, обнаруженную исследователями Project Zero в веб-браузере Google Chrome.

«Project Zero обнаружил и сообщил об активно эксплуатируемом 0day в freetype, который использовался для нацеливания на Chrome», - сказал тогда Хоукс». ***(Sergiu Gatlan. Windows kernel zero-day vulnerability used in targeted attacks // Bleeping Computer®***

(https://www.bleepingcomputer.com/news/security/windows-kernel-zero-day-vulnerability-used-in-targeted-attacks/). 30.10.2020).

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Щороку у жовтні «Місяць поширення знань про кібербезпеку» нагадує нам усім про важливість захисту безпеки в Інтернеті. Компанія розказала про автоматично вбудований захист у облікові записи Google та в кожен свій продукт/сервіс.

Безпека продуктів керується трьома основними принципами: захист інформації користувачів, відповідальне ставлення до неї та надання контролю. Компанія постійно застосовує ці принципи на практиці і хоче поділитися найновішими засобами безпеки та захисту конфіденційності, про які Ви можете дізнатися в повністю оновленому Центрі безпеки. Це єдине джерело, де зібрана вся інформація про те, як сервіси захищають користувачів. Він стане доступним вже сьогодні в США та незабаром глобально.

Проактивний захист за допомогою добре помітних сповіщень про безпеку

Коли ваша безпека під загрозою, дуже важливо не пропустити цей момент. Протягом багатьох років корпорація розробляла нові способи для повідомлення людей про ці проблеми та допомогла значно покращити їхню безпеку. Наприклад, у 2015 році почали використовувати Android сповіщення, які повідомляли людям про критичні проблеми з їхніми обліковими записами Google, зокрема щодо підозри про злам. Ця зміна виявилась приблизно у 20 ефективнішою, ніж сповіщення електронною поштою.

Сьогодні представляють оновлене критичне сповіщення та новий спосіб його надання. Незабаром, коли буде виявлено будь-яку серйозну проблему безпеки облікового запису Google, Ви побачите сповіщення в додатку Google, яким Ви користуєтеся, що допоможе вирішити проблему. Нові сповіщення захищені від підробки, тому можна бути впевненими, що вони надходять від самої компанії. Спочатку зміна з’явиться для користувачів iOS.

Легко контролюйте роботу Google Асистента за допомогою режиму «Гість»

Щодня Google Асистент допомагає людям робити щось у своєму домі, незалежно від того, чи пропонує він новий рецепт, який може Вам сподобатися, чи нагадує про наступну зустріч. Але бувають випадки, коли Ви не хочете, щоб ваші взаємодії з Асистентом зберігалися у вашому обліковому записі Google. Ось чому найближчими тижнями буде представлено гостьовий режим – новий спосіб використання Google Асистента на домашніх пристроях. За допомогою простої голосової команди Ви можете ввімкнути гостьовий режим, і Ваші взаємодії з Асистентом, перебуваючи в цьому режимі, не зберігатимуться у Вашому обліковому записі. Ви можете будь-коли вимкнути гостьовий режим, щоб знову отримати повну, персоналізовану роботу з Google Асистентом. Крім того, у Вас

завжди є можливість повернутися назад і видалити те, що Ви сказали Асистенту, просто використовуючи ваш голос.

Також додали ще більше відповідей на поширені запитання щодо безпеки і конфіденційності, на які Асистент відповість миттєво. Насправді Google щомісяця відповідає на понад 3 млн запитань щодо конфіденційності та безпеки по всьому світу.

Безпека вбудована у всі продукти

Конфіденційність та безпека є основою в усьому, що компанія робить з перших днів існування. Команди працюють щодня, щоб зробити продукти Google безпечними, незалежно від того, що Ви робите: переглядаєте сайти, користуєтеся поштою або спілкуєтесь з родиною в Google Meet. Цього тижня було оголошено про роботу із захисту інформації за допомогою нових засобів безпеки для Google Workplace та про нову систему захисту паролів у Chrome, а також про прогрес Chrome у Privacy Sandbox, ініціативі з принципового покращення конфіденційності в Інтернеті.

Щоб полегшити контроль за конфіденційністю, незабаром Ви зможете одразу редагувати дані історії місцезнаходжень у Хронології, додаючи або редагуючи місця, які Ви відвідали, лише кількома натисканнями.

Google також продовжує працювати над створенням технологій, які можна використовувати для подальшого захисту конфіденційності у всіх своїх продуктах. Наприклад, цього року, в рамках Android 11 поєднали диференційовану конфіденційність та об'єднане навчання, щоб навчити моделі, які дозволяють передбачати наступне слово на клавіатурі Gboard. Федеративне навчання, техніка, винайдена в Google, дозволяє розробникам навчати моделі ШІ та робити продукти розумнішими. В Android 11 тепер будуть генерувати розумні відповіді, включаючи рекомендації щодо смайлів, у повідомленнях Android на основі системної інформації. Це означає, що дані ніколи не передаються Gboard або Google». ***(Грицина Вікторія. Google розказав, як дбає про безпеку користувачів в Інтернеті // Pingvin Pro (https://pingvin.pro/gadgets/news-gadgets/google-rozkazav-yak-dbaye-pro-bezpeku-korystuvachiv-v-interneti.html). 08.10.2020).***

***

«Компания Fortinet, мировой лидер в области глобальных интегрированных и автоматизированных решений для обеспечения кибербезопасности, сообщает о вхождении в список лидеров сентябрьского исследования Gartner 2020 Magic Quadrant, посвященного инфраструктуре WAN Edge. Компания получила еще более высокие, чем в прошлом году, оценки в категориях «Ability to Execute» (Способность Реализации) и «Further in Completeness of Vision» (Полнота Видения).

«Несколько лет назад, когда вся отрасль думала об SD-WAN как о разрозненном продукте, мы в Fortinet выбрали сетевой подход, основанный на безопасности, объединив сетевые возможности и безопасность, чтобы стать первым вендором, предлагающим защищенный SD-WAN. Мы рады быть среди лидеров исследования 2020 Magic Quadrant, посвященного инфраструктуре WAN Edge. По нашему мнению, это является еще одним убедительным доказательством

способности Fortinet обеспечивать клиентам лучший пользовательский опыт одновременно с целостной безопасностью. Мы верим, что продолжим революцию в отрасли, предлагая решения, базирующиеся на сетевом подходе, основанном на безопасности, и обеспечивая наиболее гибкую защиту через SASE» – Джон Мэддисон, первый вице-президент отдела маркетинга продуктов и решений компании Fortinet.

Fortinet предлагает самое гибкое в отрасли решение SD-WAN

Fortinet продолжает инновации в рамках Fortinet Secure SD-WAN, предлагая органично разработанное решение, объединяющее расширенную маршрутизацию, возможности самовосстановления SD-WAN и интуитивно понятную оркестровку с наиболее гибкими в отрасли опциями безопасности. Все это обеспечивается благодаря встроенному межсетевому экрану нового поколения или облачной безопасности SASE. Стремление Fortinet к инновациям в области SD-WAN также привело к созданию самого обширного и безопасного решения в отрасли, которое можно развернуть дома, в филиале, кампусе и в нескольких облаках. Fortinet Secure SD-WAN предлагает клиентам значительные преимущества, в том числе:

Улучшение пользовательского опыта. Клиенты Fortinet могут исследовать и бороться с нарушениями WAN в динамике и на всех уровнях с помощью комплексных возможностей самовосстановления SD-WAN, базирующихся на специализированных ASIC для повышения производительности. Обучение приложений при помощи AI и ML, наглядность и контроль для обеспечения их максимальной производительности.

Снижение затрат и сложности. Подход к построению сетей, основанный на безопасности, объединяет сети и безопасность в единое решение Secure SD-WAN с централизованной оркестровкой, и позволяет клиентам сократить точечные продукты и снизить сложность эксплуатации, достигая лучших показателей по совокупной стоимости владения (TCO).

Ранее в этом году компания Fortinet была также отмечена, как выбор клиентов 2020 Gartner Peer Insights, посвященного инфраструктуре WAN Edge. Данный знак отличия получен на основании отзывов и оценок пользователей-профессионалов, имеющих опыт приобретения, внедрения или использования Fortinet Secure SD-WAN.

Кроме того, компания Omdia назвала Fortinet самым быстрорастущим поставщиком SD-WAN, отметив 247% -ный рост доходов вендора от SD-WAN в годовом выражении, с 1 квартала 2019 года по 1 квартал 2020 года. Это дополнительное признание в очередной раз указывает на способность Fortinet поставлять одно из лучших решений SD-WAN на рынке.

Fortinet демонстрирует четкое видение будущего SD-WAN

Клиенты, которые выбирают Fortinet Secure SD-WAN, могут защитить свои инвестиции в будущем, расширив возможности использования решения с помощью облачных инноваций безопасности, обеспечивающих в текущих условиях разнообразия специфики работы гибкие решения SASE где угодно и когда угодно. Благодаря широчайшей доступности для мультиоблака, постоянные инновации в объединенной облачной оркестровке обеспечат сквозную видимость и контроль в любом месте. Fortinet был одним из первых поставщиков, продемонстрировавших

расширение SD-WAN в SD-Branch, и продолжает внедрять инновации, чтобы обеспечить более тесную интеграцию, безопасность и аналитику между LAN Edge и WAN Edge». ***(Fortinet вошла в число лидеров Gartner 2020 Magic Quadrant по инфраструктуре WAN Edge // AMC Ukraine (https://channel4it.com/publications/fortinet-voshla-v-chislo-liderov-gartner-2020-magic-quadrant-po-infrastrukture-wan-edge-.html). 12.10.2020).***

***

«Компания «Elcore Украина», официальный дистрибьютор Trend Micro, сообщила о том, что вендор представил первую в своём роде «умную» систему предотвращения вторжения (IPS) для промышленных сред, которая была разработана для защиты крупномасштабных сетей от критических атак и снижения уровня капитальных и операционных затрат.

Решение EdgeIPS Pro компании TXOne Networks было специально создано для крупных «умных» объектов производства в таких отраслях, как автомобилестроение и изготовление полупроводников, где применяются системы централизованного управления и высокоавтоматизированные заводы с несколькими производственными линиями. Данное решение станет частью обширного пакета продуктов Trend Micro для защиты этого сегмента, который охватывает все уровни сетевой инфраструктуры — от «облачного» периметра до корпоративных ИТ-систем, производственных операций на местах, систем оперативно-диспетчерского управления (ОДУ) и разных уровней систем управления.

Конвергенция ИТ и ОТ (информационных и операционных технологий) на «умных» предприятиях принесла огромные преимущества в плане производительности, но также повысила риски в сфере кибербезопасности, связанные с заражением вредоносным ПО и несанкционированным доступом к сети. Это может полностью остановить производство, поскольку на подобных объектах чаще всего развёрнута «плоская» сетевая архитектура, а сами они тесно взаимосвязаны, что делает их уязвимыми для атак. Владельцам производственных структур необходимо подходящее решение для обеспечения сетевой безопасности, которое поддерживает сегментацию сети и способно защитить их инфраструктуру, не мешая достигнуть основных бизнес-целей, то есть не снижая производительность систем.

Как отмечается, стандартные решения для обеспечения безопасности ИТ-сетей не так легко подстраиваются под требования ОТ, особенно когда речь идёт о поддержке промышленных сетевых протоколов. В то же время существующие системы безопасности промышленных сетей сталкиваются с трудностями в сфере централизованного управления, поскольку эти решения необходимо развёртывать и обслуживать индивидуально для сотен объектов и сетей, существующих в производственных цехах.

«Цифровой ландшафт постоянно изменяется, поэтому решающее значение для бизнеса имеет успешное объединение ИТ и ОТ, — отметил Акихико Омикава (Akihiko Omikawa), исполнительный вице-президент направления систем безопасности интернета вещей в Trend Micro и председатель совета директоров

TXOne Networks. — Включение EdgeIPS Pro в решение Smart Factory Security Solution станет важной вехой на пути к защите крупномасштабных промышленных сетей на производстве. Простота его развёртывания и управления удобны для ИТ-подразделений и позволят организациям защитить свои сети от критических угроз, продолжая работу в обычном режиме».

EdgeIPS Pro — это прозрачный промышленный интенционно-ориентированный массив IPS, созданный с использованием однопроходной технологии глубокой инспекции пакетов компании TXOne (TXODPI™). Решение обеспечивает возможность сегментации сети с помощью межсетевого экрана/IPS/фильтрации протоколов с максимально полной поддержкой промышленных сетевых протоколов. При этом для его работы нет необходимости изменять параметры конфигурации сетей существующих активов, что дополнительно снижает начальные затраты на развёртывание системы. Также EdgeIPS Pro обеспечивает эффективное централизованное управление крупномасштабными промышленными сетями с поддержкой аппаратного байпаса третьего поколения с 48 или 96 портами и отличается простым в развёртывании форм-фактором для монтажа в стойку.

«Отсутствие сегментации сетей, которая позволила бы защитить их от распространения вредоносных программ, является наиболее распространённой проблемой на уровне опорных сетей. Также это — настоящая проблема для сред промышленных систем управления, поскольку они требуют расширенной и глубокой поддержки промышленных сетевых протоколов, — отметил д-р Теренс Лю (Terence Liu), генеральный менеджер TXOne Networks. — Наше решение EdgeIPS Pro позволяет ИТ-специалистам организовать сегментацию сетей на производственных объектах в соответствии с их бизнес-процессами». ***(Trend Micro представила «умную» систему предотвращения вторжения для промышленных сред // Компьютерное Обозрение (https://ko.com.ua/trend_micro_vypuskaet_umnuyu_sistemu_predotvrashheniya_vtorzheniya_dlya_promyshlennyh_sred_134799). 07.10.2020).***

***

«Для противодействия участившимся в последние годы атакам на API-серверы, Cloudflare в четверг выпустила новый инструмент безопасности, API Shield. Он будет предоставлен бесплатно всем владельцам учётных записей Cloudflare, независимо от тарифного плана.

API это интерфейсы между разными приложениями, которые выполняют предопределённые действия в ответ на команды или запросы клиентов. Их интегрируют в самостоятельные приложения либо в веб-базированные системы для обслуживания удалённых клиентов (мобильных приложений, устройств, серверов, пользователей).

Второй вариант особенно удобен для хакерских атак (автоматические попытки авторизации, инъекции команд, перечисление пользовательских данных и многое другое) поскольку такие API-серверы по определению должны всё время находиться в онлайновом режиме и быть открытыми для запросов отовсюду.

Новый API Shield реализует так называемую политику «позитивной безопасности», то есть блокирует всё входящие подключения, не имеющие криптографического сертификата и ключа, который владелец API сгенерировал в панели управления API Shield и установил на всех утверждённых клиентах, будь то мобильные приложения, устройства IoT, веб-серверы или что другое.

«Мы начинаем с поддержки трафика [API] JSON и, основываясь на отзывах клиентов, рассмотрим возможность расширения схемы защиты на двоичные протоколы, такие как gRPC», — говорится в пресс-релизе Cloudflare.

Дальнейшие планы наращивания функциональности предусматривают добавление в API Shield возможности ограничения скорости, защиты от DDoS-атак, правил веб-приложений, специально разработанных для API, и аналитики API». ***(Бесплатный API Shield защитит от атак веб-базированные API // Компьютерное Обозрение (https://ko.com.ua/besplatnyj_api_shield_zashhitit_ot_atak_veb-bazirovannye_api_134732). 02.10.2020).***

***

«GitHub сообщила в среду о запуске сканера уязвимостей, который будет автоматически выявлять проблемы с безопасностью в размещённых на этой платформе программных проектах.

Это усовершенствование делает принадлежащую Microsoft платформу хостинга программного кода более конкурентоспособной и, в перспективе, будет способствовать улучшению безопасности всей экосистемы Open Source.

Новый сканер уязвимостей основан на инструменте под названием CodeQL, который GitHub получила в прошлом году в результате приобретения стартапа. CodeQL позволяет разработчикам создавать абстрактное описание проблемы безопасности, а затем сканировать свои программные проекты в поисках кода, отвечающего этому описанию. Инструмент выполняет сканирование без участия человека, что значительно ускоряет анализ крупных кодовых баз.

Сейчас сканирование ведётся по двум тысячам шаблонов CodeQL. Обнаруженные программой ошибки отображаются в интерфейсе GitHub, и разработчики могут получить представление о степени уязвимости своего кода до его публикации. Интеграция с несколькими инструментами автоматизации разработки, по информации Microsoft, позволит компаниям предотвратить добавление уязвимого кода во внутренние программные репозитории.

Со временем GitHub планирует расширить первоначальную функциональность сканера. Так, сообщается, что разработчики получат возможность добавлять в набор шаблонов сканирования CodeQL свои собственные запросы. Кроме того, интеграция сканера уязвимостей с дополнительными продуктами других компаний будет способствовать обнаружению более широкого круга проблем безопасности.

Вклад нового сканера в повышение безопасности кода на GitHub уже ощущается. В рамках бета-тестирования, предшествовавшего вчерашнему запуску, CodeQL выявил более 20 000 ошибок в 12 000 репозиториях кода. Участники бета-программы исправили 72% этих ошибок быстрее, чем в среднем по отрасли.

Сканирование уязвимостей является бесплатным для всех репозиториев с открытым исходным кодом, а также доступно как часть платной версии GitHub Enterprise, что позволяет предприятиям использовать эту функцию для поиска проблем безопасности в своих внутренних программных проектах». ***(На GitHub появился сканер уязвимостей кода // Компьютерное Обозрение (https://ko.com.ua/na_github_poyavilsya_skaner_uyazvimostej_koda_134720). 02.10.2020).***

***

«Израильская компания Illusive Networks, которая создает ПО в сфере кибербезопасности, привлекла $24 млн инвестиций…

В раунде инвестирования B1 приняли участие Spring Lake Equity Partners, Marker, New Enterprise Associates, Bessemer Venture Partners, Innovation Endeavors, Cisco, Citi и Microsoft, сообщает "ЛІГА.net".

Эти средства компания использует для увеличения объема продаж и развития маркетинга. Также средства потратят на усовершенствование продукта для защиты облачных рабочих нагрузок.

Illusive Networks разрабатывает продукт в сфере обманных технологий. Их технология состоит в том, чтобы фиксировать и удалять хакера из сети в момент использования им нарочно созданных системой ложных данных.

Deception Technology (или обманные технологии) – это использование ловушек и приманок в корпоративной сети для предотвращения ее взлома. Это может быть создание фальшивых сетевых папок, внешне идентичных оригиналам или фиксация источника вредоносной активности непосредственно в момент ее совершения. Согласно исследованию компании Enterprise Management Associates, использование этих технологий позволяет обнаруживать киберпреступников в 12 раз быстрее». ***(Израильские охотники за хакерами привлекли $24 млн инвестиций // Багнет (http://www.bagnet.org/news/tech/1293674/izrailskie-ohotniki-za-hakerami-privlekli-24-mln-investitsiy). 08.10.2020).***

***

«Africell, крупнейший американский оператор мобильной связи, насчитывающий более 12 миллионов клиентов в 4 африканских странах, внедрил ведущее отраслевое решения российской компании StormWall по защите сети по BGP для повышения безопасности своих сетей.

Решение обеспечивает надежную защиту ИТ-инфраструктуры Africell на территории Уганды, Демократической республики Конго, Гамбии и Сьерра-Леоне, где компания предоставляет доступ к сети интернет посредством технологий 3G, LTE и 5G и оценивается регуляторами как компания номер один по качеству обслуживания.

Решение по защите сети по BGP обеспечивает автоматическую защиту для атакуемых сетей, позволяя на ранней стадии обнаружить DDoS-атаку и провести переключение трафика на DDoS-фильтры до того, как атака приведет к недоступности сервиса. Решение помогает обеспечить стабильную работу ИТ-инфраструктуры и сети, защитив их от всех известных DDoS-атак на уровнях L3-L5

OSI. Данный способ защиты предназначен для интернет-провайдеров, дата-центров, хостинг-компаний, а также корпоративных клиентов с собственной автономной системой.

Юнес Чаабан, технический директор Africell, отметил: «Безопасность данных наших клиентов является главным приоритетом для Africell. Именно поэтому мы работаем с компанией StormWall, чтобы использовать самые передовые системы защиты, доступные сегодня. Благодаря большому опыту, StormWall может предложить идеальное решение для защиты наших сетей от DDoS-атак. StormWall помогает Africell удостовериться в том, что мы можем продолжать развивать наш бизнес, не опасаясь стать жертвой кибератаки».

Рамиль Хантимиров, CEO и со-основатель StormWall, сказал: «Africell является одним из ведущих телеком-операторов Африки. Объемы обрабатываемого им трафика огромные, поэтому защита от DDoS-атак - одна из ключевых задач компании. Для нас было очень важно завоевать доверие Africell и предоставить наше решение, обеспечив высокий уровень защиты ресурсов компании. Использование профессиональных решений позволяет эффективно противостоять киберпреступникам, и мы рады, что африканские компании осознают необходимость использования таких методов защиты»… ***(Владимир Бахур. Разработанные в России технологии защиты от DDoS-атак востребованы в Африке // CNews (https://safe.cnews.ru/news/line/2020-10-08_razrabotannye_v_rossii_tehnologii). 08.10.2020).***

***

«Google добавил улучшенную защиту от вредоносных программ для всех пользователей Google Chrome, которые также участвуют в программе Advanced Protection Program (APP) компании.

Программа расширенной защиты Google - это бесплатная услуга, направленная на защиту учетных записей пользователей, включая, помимо прочего, активистов, журналистов, руководителей бизнеса и политические группы, которые имеют более высокий риск стать объектом атак в Интернете.

APP блокирует несанкционированный доступ к учетным записям зарегистрированных пользователей, предлагает дополнительную защиту от вредоносных загрузок и защищает информацию пользователей.

Более того, программа предоставит пользователям, зарегистрированным в APP, улучшенную защиту от фишинговых атак на аккаунты Google, вредоносных приложений и попыток кражи данных.

Предупреждения в реальном времени

«В частности, когда Chrome обнаруживает потенциально подозрительную загрузку файла, пользователи будут видеть новое сообщение с вопросом, хотят ли они отправить файл в Google Advanced Protection для проверки на наличие вредоносных программ», - пояснил сегодня Google.

«Если они решат отправить его, Google Safe Browsing просканирует его в реальном времени и предупредит пользователя, если определит, что файл небезопасен».

Новая улучшенная защита от вредоносных программ и предупреждения включены по умолчанию для всех пользователей, участвующих в Программе расширенной защиты и также вошедших в Chrome.

Эта функция доступна с сегодняшнего дня для всех пользователей программы Advanced Protection Programme. Пользователи, которые еще не зарегистрированы, могут сделать это, используя встроенный ключ безопасности своего телефона или физический ключ безопасности, соответствующий требованиям FIDO, перейдя сюда.

После регистрации они должны будут использовать ключ безопасности, используемый в процессе регистрации, при входе в свои учетные записи на новых устройствах.

Благодаря этой дополнительной защите, даже если пользователь Google станет жертвой фишинговой кампании, злоумышленник, стоящий за ним, не сможет получить доступ к учетной записи жертвы без ключа безопасности.

Они также будут получать дополнительные предупреждения при установке приложений или загрузке файлов, которые выглядят подозрительно из-за более строгих настроек и проверок защиты приложений. а также из-за нескольких дополнительных функций безопасности учетной записи, которые по умолчанию включены для пользователей, зарегистрированных в приложении.

В 2019 году ни один зарегистрированный в приложении пользователь не совершил фишинг

Ранее в этом году Google объявил, что за последний год он отправил своим пользователям около 40 000 предупреждений о спонсируемых государством попытках фишинга или взлома вредоносных программ.

Выдача себя за журналиста и новостных агентств была одной из наиболее часто определяемых тактик фишинга, которые использовали поддерживаемые государством злоумышленники в 2019 году, сказал Тони Гидвани, в то время менеджер по безопасности в Группе анализа угроз Google (TAG).

«Мы еще не видели, чтобы люди успешно использовали фишинг, если бы они участвовали в программе Google Advanced Protection Program (APP), даже если они неоднократно становились мишенями», - пояснил Гидвани.

«APP обеспечивает самую надежную защиту от фишинга и взлома учетных записей и специально разработано для учетных записей с самым высоким уровнем риска». ***(Sergiu Gatlan. Google boosts malware protection for high-risk accounts // BleepingComputer.com (https://www.bleepingcomputer.com/news/security/google-boosts-malware-protection-for-high-risk-accounts/). 09.10.2020).***

***

«Cloudflare теперь позволяет платным клиентам создавать уведомления, которые предупреждают их, когда их сайты подвергаются DDoS-атаке.

Распределенная атака типа «отказ в обслуживании» (DDoS) - это когда злоумышленник наводняет веб-сервер или подключение к Интернету большим количеством запросов, чем он может обработать. Этот поток запросов приводит к тому, что служба становится недоступной, а компания или человек выходит из строя.

Cloudflare всегда предлагал защиту от DDoS-атак в качестве одного из своих основных предложений, но если владелец или администратор сайта не будет активно использовать свой сайт или инструменты мониторинга, они не будут знать, что их сервис подвергся атаке, пока не станет слишком поздно.

Вчера Cloudflare объявила, что все платные клиенты теперь могут настраивать оповещения, которые уведомляют их, когда сайт, которым они управляют, подвергается DDoS-атаке.

В зависимости от того, какой у вас платный аккаунт в Cloudflare, вы можете получать уведомления по электронной почте или PageDuty.

Также существуют различные типы DDoS, которые вы можете получить - HTTPS DDoS и атаки L3 / L4. Доступность каждого типа оповещения зависит от того, какую службу вы используете с Cloudflare…

К сожалению, Cloudflare не позволяет создать тестовое уведомление, чтобы узнать, как оно будет работать с пользовательскими системами уведомлений или текстами SMS.

Как создать DDoS-оповещение Cloudflare

Чтобы создать уведомление Cloudflare DDoS, выполните следующие действия:

Войдите в панель управления Cloudflare по адресу https://dash.cloudflare.com.

Вверху панели управления щелкните раздел «Уведомления».

В разделе «Уведомления» нажмите кнопку «Создать».

Выберите тип уведомления DDoS, для которого вы хотите создать оповещение. Для большинства клиентов, использующих Cloudflare для защиты веб-сайта, вы увидите только «Предупреждение об атаке HTTP DDoS». Когда закончите, нажмите на кнопку «Далее» кнопку.

На следующем экране дайте уведомлению имя и необязательное описание. Затем добавьте адреса электронной почты или другие методы уведомления, которые должно использовать предупреждение.

По завершении нажмите кнопку «Создать», чтобы завершить настройку уведомления.

После создания оповещения, когда Cloudflare обнаруживает, что ваш сайт или сервис подвергается DDoS-атаке, он отправляет уведомление». ***(Lawrence Abrams. Cloudflare can now send DDoS alerts for sites are under attack // BleepingComputer.com(https://www.bleepingcomputer.com/news/technology/cloudflare-can-now-send-ddos-alerts-for-sites-are-under-attack/). 06.10.2020).***

***

«Журналисты Bleeping Computer обратили внимание на интересную утилиту, недавно созданную ИБ-экспертом Флорианом Ротом (Florian Roth). Разработка получила название Raccine (Ransomware vaccine, то есть «Вакцина от вымогателей») и она автоматически ликвидирует любые процессы, пытающиеся удалить теневые копии в Windows с помощью vssadmin.exe.

Дело в том, что операторы шифровальщиков не хотят, чтобы их жертвы использовали эту функцию ОС для бесплатного восстановления своих файлов, поэтому практически любая вымогательская малварь первым делом удаляет все

теневые копии с зараженной машины. Так, один из способов их удаления, это использование команды vssadmin.exe: vssadmin delete shadows /all /quiet. Другой способ — использование команды resize, чтобы задать объем хранилища, который Windows выделяет для теневых копий. Эта команда также сотрет существующие снапшоты: vssadmin.exe resize shadowstorage /for=D: /on=D: /maxsize=401MB.

«Программы-вымогатели часто удаляют все теневые копии, используя vssadmin. Но что если бы мы могли просто перехватить этот запрос и остановить вызов процесса? Давайте попробуем создать простую вакцину», — пишет Рот на GitHub-странице проекта.

Raccine работает просто: регистрирует файл raccine.exe как дебаггер для vssadmin.exe через реестр Windows и ключ Image File Execution Options Windows. После регистрации при каждом запуске vssadmin.exe также запускается и Raccine, которая проверяет, не пытается ли vssadmin удалить теневые копии. Если утилита обнаруживает, что процесс использует vssadmin delete или vssadmin resize shadowstorage, она автоматически завершает его, тем самым мешая работе шифровальщика.

Журналисты Bleeping Computer отмечают, что некоторые современные вымогатели удаляют теневые копии с помощью других команд, включая:

Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
WMIC.exe shadowcopy delete /nointeractive

Увы, в таких случаях Raccine не сможет ничего поделать, но Рот обещает со временем расширить функциональность утилиты, чтобы она могла распознавать и такие способы. Также в будущем Рот планирует добавить некоторые программы в исключения Raccine, чтобы они не прекращали работу с сообщением об ошибке». ***(Мария Нефёдова. Утилита Raccine не дает шифровальщикам удалять теневые копии // Xakep (https://xakep.ru/2020/10/05/raccine/). 05.10.2020).***

***

«Организации European Network for Cyber Security (ENCS) и European Distribution System Operators' Association (E.DSO) выпустили требования по кибербезопасности для распределенной автоматизации (Distribution Automation, DA) устройств связи с объектом (Remote Terminal Units, RTU).

Это третье руководство в серии рекомендаций по безопасности для «умной» энергетической сети после того, как ENCS и E.DSO опубликовали требования безопасности для точек зарядки электромобилей и «умных» счетчиков. Данные требования являются важным инструментом в улучшении безопасности сбора и анализа данных для коммунальных предприятий по всей Европе, помогая построить более устойчивую сеть.

Требования предоставляют операторам европейских распределительных систем определенный набор практических соображений по приобретению защищенных RTU и являются значительным шагом вперед к требованиям отрасли. Требования разделены на несколько частей

DA-201-2019: Архитектура безопасности для распределенных систем автоматизации (или только для членов ENCS);

DA-301-2019: Требования безопасности при закупке RTU DA (общедоступные);

DA-401-2019: План тестирования безопасности для распределенной автоматизации устройств связи с объектом (общедоступный).

ENCS активно участвует в обеспечении безопасности распределенной автоматизации с 2015 года, когда она начала анализировать уязвимости в архитектурах и системах. Требования были разработаны для всех участников и сначала использовались компанией Enexis Netbeheer, позволив обеспечить безопасную систему распределенной автоматизации и более плавный процесс закупок, выполненный с минимальными дополнительными затратами. ENCS также разработала план тестирования для контроля выполнения требований безопасности стандартизированным способом. Стандартизация плана тестирования упрощает обмен результатами тестирования между операторами сети.

«До сих пор в Европе были разные требования по безопасности из-за разрозненного подхода. Однако эта работа, которую мы проводим с E.DSO, позволила выработать согласованный и синхронизированный набор требований, позволяющие производителям реализовать безопасность с минимальными затратами», — сообщил управляющий директор ENCS Аньос Нейк (Anjos Nijk)». ***(Представлены новые требования по кибербезопасности распределенной автоматизации // SecurityLab.ru (https://www.securitylab.ru/news/513057.php). 14.10.2020).***

***

«Максимальний рейтинг отримали вісім продуктів, в тому числі, і Windows Defender («Захисник Windows»)

Windows Defender разом з рядом інших антивірусів був названий кращим рішенням для ОС від Microsoft.

Про це повідомляється на сайті німецького агентства Av-Test.

Фахівці лабораторії провели тестування програм для виявлення вірусів і на основі декількох показників розкрили кращі з них. Максимальний рейтинг отримали вісім продуктів, в тому числі, і Windows Defender («Захисник Windows»).

Також в список кращих програм за версією експертів увійшли AhnLab, Avira, F-Secure, G Data, McAfee, NortonLifeLock і «Антивірус Касперського».

Кращі, за даними Av-Test, антивіруси отримали максимальну кількість балів - 18. З точки зору безпеки комп'ютера, впливу на продуктивність пристрою і зручність використання програми оцінили на шість балів. Решта присутніх в топі сервіси - Avast, AVG, Bitdefender і BullGuard - набрали по 17,5 бала і також були рекомендовані фахівцями лабораторії до установки на комп'ютери під управлінням Windows.

«Захисник Windows» є вбудованим в ОС від Microsoft антивірусом. У вересні експерти з кібербезпеки виявили в продукті лазівку для установки шкідливих програм. Зокрема, пролом в системі безпеки дозволяв використовувати командний рядок MpCmdRun.exe для інсталяції непідтверджених додатків». ***(Експерти назвали найкращий антивірус для Windows // Українські медійні системи***

(https://glavcom.ua/techno/hitech/eksperti-nazvali-naykrashchiy-antivirus-dlya-windows-713121.html). 23.10.2020).

***

«В понедельник компания Zoom значительно повысила безопасность своих пользователей, развернув сквозное шифрование для своей сети онлайн-встреч.

E2EE передает управление ключами для шифрования данных организаторам встреч. До развертывания E2EE шифрование выполнялось на серверах Zoom, и кто-то, имеющий доступ к этим серверам, мог перехватить данные.

Чтобы использовать новую функцию, клиенты должны включить конференции E2EE на уровне учетной записи и подписаться на E2EE для каждой встречи.

«Распространение ключей среди клиентов и децентрализация доверия дает пользователям повышенную уверенность в том, что их обмен данными с меньшей вероятностью будет перехвачен через взломанные ключи или инфраструктуру», - сказал TechNewsWorld Джек Маннино, генеральный директор nVisium, поставщика безопасности приложений из Херндона, штат Вирджиния.

«Без сквозного шифрования есть вероятность, что кто-то, имеющий доступ к платформе, сможет перехватить разговоры», - пояснил Дэн Надир, главный директор по продукту Theta Lake, компании по унифицированным коммуникациям в Санта-Барбаре, Калифорния.

«Это может быть недобросовестный сотрудник или кто-то, кто может взломать систему», - сказал он TechNewsWorld. «Полное сквозное шифрование устраняет эту потенциальную уязвимость».

Забывчивые серверы

Zoom объяснил в заявлении, что на типичных собраниях его облачные серверы собраний генерируют ключи шифрования для каждого собрания и распространяют их среди участников собрания, использующих клиенты Zoom, когда они присоединяются.

С новым E2EE от Zoom, продолжил он, организатор встречи генерирует ключи шифрования и использует криптографию с открытым ключом для распространения этих ключей другим участникам встречи, которые также увидят код безопасности лидера встречи, который они могут использовать для проверки безопасного соединения. Хост может прочитать этот код вслух, и все участники могут проверить, что их клиенты отображают один и тот же код.

Серверы Zoom становятся не обращающими внимания на реле и никогда не видят ключи шифрования, необходимые для расшифровки содержимого встречи, пояснил он. Зашифрованные данные, передаваемые через серверы Zoom, не поддаются расшифровке Zoom, поскольку серверы Zoom не имеют необходимого ключа дешифрования.

«Мы очень гордимся тем, что сегодня представили новое сквозное шифрование Zoom пользователям Zoom во всем мире», - сказал в своем заявлении директор по информационной безопасности Zoom Джейсон Ли.

«Эта функция очень востребована нашими клиентами, и мы очень рады воплотить ее в жизнь», - добавил он.

Обезвреживание бомбардировки зумом

При правильном использовании E2EE может затруднить прослушивание разговоров с использованием E2EE даже для самых обеспеченных в мире спецслужб, заметил Тод Бердсли, директор по исследованиям Rapid 7, поставщика решений для безопасности данных и аналитики в Бостоне.

«Вот почему это такой мощный механизм обеспечения конфиденциальности для тех людей, которым нужно беспокоиться о разведывательных организациях, - журналистов, которые защищают источники, информаторов, активистов гражданских прав и других», - сказал он TechNewsWorld.

«Преимущества для пользователей, особенно во времена COVID, существенны», - добавил Дирк Шрейдер, глобальный вице-президент New Net Technologies, поставщика программного обеспечения для ИТ-безопасности и соблюдения нормативных требований из Неаполя, штат Флорида.

«Это особенно верно для бесплатных пользователей», - сказал он TechNewsWorld. «Во всем мире многие школы и волонтерские организации используют Zoom, чтобы оставаться на связи, несмотря на обеспокоенность по поводу конфиденциальности и безопасности».

Одной из первых проблем, с которыми столкнулись пользователи платформы, была «Zoom Bombing», когда злоумышленники вторгались на собрания и нарушали их. «E2EE может остановить это», - отметил Крис Картер, генеральный директор Approyo, поставщика услуг SAP в Маскего, штат Висконсин.

«Никто не может попасть на конференцию до ее хозяина», - сказал он TechNewsWorld. «Любой, кто участвует в конференции E2EE, должен предоставить информацию о себе, и организатор должен одобрить его. Они не могут войти в качестве анонимного гостя»

Обеспокоенность по поводу преступности

Картер добавил, что использование функции Zoom E2EE требует компромиссов. «Если у вас включен E2EE, вы не сможете записывать встречи на серверы Zoom», - пояснил он. «Вы не можете вести частные чаты или комнаты для обсуждения».

Хотя E2EE предлагается как бесплатным, так и платным пользователям Zoom, компания изначально предлагала ограничить эту функцию платными пользователями из-за опасений, что технология может быть использована преступниками. Этот потенциал все еще существует.

«По мере того как сервисы платформы переходят на сквозное шифрование, это означает, что у поставщиков услуг и правоохранительных органов становится меньше возможностей для обнаружения преступников и людей, использующих сервис в злонамеренных целях», - сказал Уильям Диксон, глава отдела кибербезопасности Всемирного экономического центра Forum, международная организация государственно-частного сотрудничества со штаб-квартирой в Женеве, Швейцария.

Это означает, продолжил он, что людям приходится вводить новшества и развивать свои взгляды на выявление преступлений на этих платформах. «Технологические компании использовали различные методы для обнаружения вредоносной активности», - сказал он TechNewsWorld. «Они вкладывают значительные средства в анализ на уровне метаданных и пользовательскую аналитику, чтобы дать правоохранительным органам советы о потенциальной подозрительной деятельности».

Хотя добавление E2EE является благом для пользователей Zoom, компания также извлекает выгоду из этого шага. «Это выводит их на уровень безопасности, который обычно есть в Microsoft», - утверждает Картер.

«По сути, у Zoom не было выбора», - сказал Шрейдер. «Добавление шифрования E2EE к его услугам было обязательным после всех потрясений, которые он пережил».

Надир утверждал, что сквозное шифрование - залог успеха любой компании, которая хочет предложить серьезное решение практически для любого случая использования.

«Поскольку для коммуникационных платформ это очень важно, то отсутствие этого, безусловно, является конкурентным недостатком для любой технологии на рынке», - добавил он.

Система единого входа на Horizon

Новая функция шифрования доступна как для бесплатных, так и для платных пользователей, а также для настольных компьютеров Mac и ПК версии 5.4.0 программы Zoom, а также для версии приложения для Android и Zoom Rooms.

Он использует то же 256-битное шифрование AES-GCM, которое используется для защиты собраний, не связанных с E2EE.

Zoom называет это начальное развертывание E2EE «техническим превью». он надеется собрать отзывы клиентов об их опыте использования этой функции и призывает клиентов включить Feedback to Zoom в своих учетных записях и использовать его, чтобы комментировать новую функцию.

Zoom отметил, что это только начальная фаза E2EE для него. На следующем этапе будет улучшено управление идентификацией и единый вход.

«Управление идентификацией и поддержка единого входа упростят для корпоративных клиентов использование Zoom в качестве платформы для совместной работы. Это уменьшит трение для конечных пользователей», - сказал TechNewsWorld Джефф Поллард, вице-президент и главный аналитик Forrester Research.

«Эта функциональность дополняет и дополняет E2EE, - добавил Шрейдер.

«Неправильно используя украденную личность, злоумышленник может присоединиться к зашифрованному сеансу, выдавая себя за настоящую личность, для сбора информации в реальном времени», - пояснил он. «Эти методы не уникальны для Zoom, они общие для всех видов услуг».

«Тем не менее, - продолжил он, - Zoom добавляет, что это означает, что компания серьезно относится к безопасности и конфиденциальности и хочет закрыть все пробелы». ***(John P. Mello Jr. Zoom Beefs Up User Security With End-To-***

End Encryption // TechNewsWorld (https://www.technewsworld.com/story/86900.html). 28.10.2020).

***

«Исследователи из организации Ponemon Institute провели опрос 603 специалистов по информационной безопасности в США по поводу использования межсетевых экранов. Респондентам предлагалось оценить эффективность межсетевых экранов в блокировании программ-вымогателей и ряда других существующих угроз.

Опрос охватывал как межсетевые экраны с отслеживанием состояния, которые проверяют входящий и исходящий сетевой трафик, так и межсетевые экраны, объединяющие анализ угроз, предотвращение вторжений, контроль доступа к приложениям и другие функции.

Как показали результаты опроса, организации очень недовольны своими нынешними межсетевыми экранами. Более половины (53%) респондентов заявили, что они либо отказываются от данных технологий, либо сокращают их зависимость и ищут другие варианты.

6 из 10 опрошенных руководителей системы безопасности считают, что у устаревших межсетевых экранов нет необходимых возможностей для защиты важных приложений и систем от атак. Они считают устаревшие межсетевые экраны малоэффективными для создания среды с нулевым доверием, а 76% потребовалось слишком много времени для защиты новых приложений или изменения конфигурации с помощью устаревших устройств.

57% опрошенным потребовалось от трех недель до месяца, чтобы изменить конфигурацию межсетевого экрана с учетом обновленного или нового приложения». ***(Большинство ИБ-специалистов отказываются от межсетевых экранов // SecurityLab.ru (https://www.securitylab.ru/news/513421.php). 29.10.2020).***

***

«Исследователи из Университета Карнеги-Меллона пришли к выводу, что нейронные сети, обученные для изучения подходов злоумышленников к брутфорсу паролей, могут использоваться для обеспечения минимальной безопасности паролей без использования огромных «черных списков» и громоздких комбинаций букв, цифр и специальных символов.

Используя модель нейронной сети исследователи провели анализ ряда различных рекомендаций по созданию паролей, от восьмизначных с использованием одного класса (букв, например) до шестнадцадизначных паролей с использованием четырех классов (строчных букв, прописных букв, цифр и символов). Как показали результаты исследования, использование всего лишь 12 символов одного класса и соблюдение рекомендаций нейронной сети позволило создать трудные для взлома пароли, которых должно хватить для большинства случаев использования.

По словам экспертов, требование сочетать разные регистры, числа и символы не является обязательным.

«Раньше было намного меньше трех- и четырехклассных паролей, которые оказывались доступны в Сети. Злоумышленникам было труднее разработать способы эффективного угадывания подобных паролей. Теперь, когда произошло много утечек таких паролей, гораздо проще обучить алгоритм их угадывать», — пояснили исследователи.

Исследование направлено на поиск наилучшего баланса между удобством использования и безопасностью паролей. Нейронная сеть моделирует поведение злоумышленников с целью определить, о каких комбинациях можно легко догадаться с помощью существующих методов.

По словам специалистов, сочетание минимальной длины пароля и соответствие стандарту надежности нейронных сетей может помочь компаниям гарантировать, что их сотрудники создают трудные для взлома пароли». ***(Нейросети помогут пользователям выбирать более надежные пароли // SecurityLab.ru (https://www.securitylab.ru/news/513398.php). 27.10.2020).***

***

«Ветеран рынка кибербезопасности, McAfee, на организованной им виртуальной конференции MPOWER Digital анонсировал новые продукты и расширенные возможности предлагаемых сервисов.

Главным событием стал релиз новой платформы MVISION Cloud Native Application Protection Platform (MVISION CNAPP). Она предназначена для комплексной защиты данных, защиты от угроз, обеспечения управления и соответствия для жизненных циклов облачных приложений.

Анонсированная как первая в отрасли интегрированная архитектура безопасности экосистемы облачных приложений, MVISION CNAPP включает в себя Cloud Security Posture Management — для публичной облачной инфраструктуры и Cloud Workload Protection — для защиты хостов и рабочих нагрузок, включая виртуальные машины, контейнеры и бессерверные вычисления.

В духе популярного в кибербезопасности тренда MVISION CNAPP позволяет строить политики, базирующиеся на концепции «нулевого доверия» с отслеживанием поведенческих аномалий для исключения ложных срабатываний.

Одна из ключевых функций этой платформы делает возможным «глубокое обнаружение» всех облачных ресурсов с определения их приоритетов по степени риска. Другая важная функция предохраняет от «дрейфа» конфигурации и осуществляет аудит уязвимости виртуальных машин, контейнеров и бессерверных сред.

Совместимость с MITRE ATT&CK Framework открывает для пользователей MVISION CNAPP доступ к глобальной базе информации о тактике и методах киберпреступников. Для обеспечения бесперебойности бизнеса новый сервис поддерживает автоматизацию средств непрерывного контроля соответствия и управления.

Фирма McAfee также ознакомила участников конференции с новой функциональностью фреймворка MVISION Unified Cloud Edge (MVISION UCE), который, по её заявлению, реализует уникальный подход к защите от фишинговых и вымогательских (ransomware) угроз.

В числе усовершенствований сервиса, способствующих снижению затрат и сложности, связанных с корпоративной безопасностью, при обеспечении максимальной облачной гибкости, были анонсированы интеграция технологии изоляции удалённого браузера (RBI) со средствами защиты в реальном времени; унифицированные предотвращение потери данных и управление инцидентами на разных устройствах, в сетях, в Интернете и в облаке.

MVISION CNAPP в настоящее время предлагается в бета-статусе, широкая доступность сервиса запланирована на март 2021 года. Новые функции в MVISION UCE появятся в ноябре, за исключением RBI, которая в ближайшие месяцы будет проходить бета-тестирование». ***(McAfee представила новую платформу защиты приложений // Компьютерное Обозрение (https://ko.com.ua/mcafee_predstavila_novuyu_platformu_zashhity_prilozhenij_135078). 30.10.2020).***

***