**Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»
Національна бібліотека України імені В. І. Вернадського**

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 5 (травень)

Київ – 2021

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2021.– №5 (травень). – 304 с.

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

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

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

ЗМІСТ

«В Украине создадут университет для подготовки специалистов в области новых технологий. Обучение планируют начать уже через два года.

Лучшие студенты смогут получить работу после завершения обучения, заявил президент Владимир Зеленский во время совещания по подготовке концепции создания этого университета.

Концепцию должны разработать к июлю 2021, а к октябрю - принять закон об особенностях правового статуса этого учебного заведения.

Построить его планируют к сентябрю 2023 года. Первыми пройти обучение смогут 120 студентов, а в дальнейшем их количество будет увеличиваться.

Университет будет иметь шесть основных направлений: информационные технологии, кибербезопасность и искусственный интеллект; нанотехнологии; аэрокосмические технологии; новые энергетические технологии; биотехнологии и науки о здоровье; международные отношения и безопасность.

«Создание такой мощной современной образовательно-научной платформы позволит Украине готовить специалистов по чрезвычайно востребованных специальностей. Они станут тем двигателем, который будет двигать вперед украинскую науку и экономику, а также способствовать становлению нашей страны как IT-хаба Европы», - сказал Зеленский.

В вузе будут преподавать лучшие украинские и иностранные эксперты. 30% в учебном процессе будет занимать теория, 70% - практические занятия. Студенты смогут пройти стажировку на лучших отечественных предприятиях и в международных компаниях.

«Лучшие студенты будут получать высокие стипендии, а после завершения обучения - гарантированное трудоустройство в Украине. Также студенты и выпускники будут иметь возможность реализации в Украине собственных научных разработок», - отметил президент». ***(В Украине создадут университет современных технологий – подробности // Gazeta.ua (https://gazeta.ua/ru/articles/life/_v-ukraine-sozdadut-universitet-sovremennyh-tehnologij-podrobnosti/1032431). 18.05.2021).***

***

«Для защиты от кибератак общественники пользуются услугами российской компании DDoS-GUARD.

Информационныq ресурс общественного движения «Движение сопротивления капитуляции», который называют близким к пятому президенту Петру Порошенко, использует российские сервисы для защиты от DDoS-атак. В частности, такие данные приводит сервис 2ip, передает Klymenko Time.

Так, при вводе для проверки домена rok.org.ua, по которому расположен сайт организации, отображается информация о том, что ресурс находится на серверах Ростова-на-Дону. Однако проверка в данном случае касается домена ddos-guard.net. Это сайт российской компании, работа которой заключается, среди прочего, в защите ресурсов от DDoS-атак.

Похожие данные приводят сервисы Whois DomainTolls и CuteStat, однако у них городом расположения сервера указана Москва.

Примечательно, что «Движение сопротивления капитуляции» проявлял самую заметную активность в 2019 году – перед встречей президента Украины Владимира Зеленского, канцлера Германии Ангелы Меркель, президента Франции Эммануэля Макрона и президента РФ Владимира Путина в Париже. В частности, его представители собирались на митингах против "формулы Штайнмайера», которая предусмотрена Минскими соглашениями.

Следует отметить, что данное движение возглавляет Андрей Левус, который после непопадания в парламент (выдвигался от Европейской солидарности) создал данный проект…». ***(«Движение сопротивления капитуляции» пользуется услугами компаний из РФ ради кибербезопасности (фото) // Фокус (https://focus.ua/politics/482769-dvizhenie-soprotivleniya-kapitulyacii-polzuetsya-uslugami-kompaniy-iz-rf-radi-kiberbezopasnosti-foto). 17.05.2021).***

***

«В киберцентре UA30, недавно открытом при Государственной службе специальной связи и защиты информации Украины, состоялись первые учения по кибербезопасности. 30 представителей Госспецсвязи, Киберполиции и ситуационного центра обеспечения кибербезопасности СБУ приняли в них участие на протяжении трех дней.

Напомним, что киберцентр UA30, специалисты которого должны предотвращать виртуальные атаки на украинские объекты, был открыт при участии президента Владимира Зеленского 13 мая. В центре работает единственная в Украине команда реагирования на компьютерные чрезвычайные происшествия - CERT-UA (Computer Emergency Response Team of Ukraine).

«Киберцентр UA30 является частью нашей новой стратегии реформирования сферы кибербезопасности. Наша цель заключается в том, чтобы Украина в ближайшем времени стала полноправной участницей мировой экосистемы кибербезопасности, на высоком уровне обеспечивала защиту собственных государственных информационных ресурсов, критической инфраструктуры, и демонстрировала высокую готовность к противодействию киберугрозам, с которыми к сожалению мы встречаемся ежедневно и чувствуем ежедневно высокий риск для наших критических систем, - сказал Виктор Жора, заместитель главы Госспецсвязи по вопросам цифрового развития, цифровых трансформаций и цифровизации. - Важной составляющей реформы кибербезопасности является в том числе реформа образования в этой сфере и обучение специалистов. Ведь усилия команды реагирования на компьютерные чрезвычайные происшествия и усилия других субъектов обеспечения кибербезопасности будут напрасными без надлежащего уровня подготовки всех специалистов по кибербезопасности, министерств, ведомств, областных госадминистраций, объектов критической инфраструктуры. Поэтому мы в рамках киберцентра UA30 создали уникальный для Украины тренинговый киберцентр, в котором специалисты имеют возможность отрабатывать реальные сценарии кибератак, икать правильные подходы для защиты от подобных атак и обмениваться передовыми мировыми практиками».

По словам замглавы Госспецсвязи, всего в мире насчитывается 20 подобных центров, 6 из них - в США. Что касается самого тренинга, то в ходе его три синие команды защитников, в состав которых входили сотрудники ключевых украинских учреждений по кибербезопасности, занимались охотой на угрозы и другими конкретными задачами, о которых участники узнали только во время учений. Синие команды изучили, как работают злоумышленники, когда красная команда организаторов учений запускала фиктивные атаки на заранее определенную ИТ-инфраструктуру. Украинские ИТ-эксперты узнали, какие индикаторы остаются после атак злоумышленников и как они передвигаются между сетевыми системами.

«Подобных учений может быть много, но уникальной чертой данных учений было то, что они позволяют наглядно увидеть, каким образом, какими инструментами, методами пользуются злоумышленники для реализации своих кибератак. И, таким образом, зная их способность, службам противодействия будет намного легче, быстрее и эффективнее реагировать на них, - сказала Мерле Майгре, эксперт проекта EU4DigitalUA, специалист по кибербезопасности эстонской Академии электронного управления. - Необходимо отметить, что в качестве нападающей стороны выступали профессионалы - специалисты эстонского специализированного агентства CyberEx, которое специализируется на киберзащите. Поэтому они были в состоянии реализовать наиболее интересные и мощные сценарии атак, направляя их на государственные инфраструктурные элементы, обычные хакерские атаки и специализированные, которые могут выполняться в скрытом ключе. Поэтому реализация множественных сценариев угроз, то на чем профилированы эстонские специалисты, и чем они могли эффективно поделиться с украинским коллегами. Это было чрезвычайно полезно с профессиональной точки зрения. Удовольствие и польза дает самый положительный результат».

«Европейский Союз твердо поддерживает Украину, в частности путем расширения ее способности противостоять киберугрозам, - заявил Реми Дюфло, заместитель главы представительства ЕС в Украине, на церемонии награждения участников учений. - Целью этих учений является повышение устойчивости и опыта украинских органов кибербезопасности для предотвращения и ликвидации атак. Это часть более широкой поддержки Украины со стороны ЕС. Цифровая трансформация и электронное управление является одним из самых успешных украинских реформ. Их также нужно защищать».

Виктор Жора подчеркнул, что в Госспецсвязи нацелены на то, чтобы развивать успех проведения тренингов. Уже имеется предварительная договоренность с коллегами из министерств и ведомств, где имеется бешеный спрос, и планируется до конца года в тренинговом центре киберцентра UA30 обучить до полутысячи специалистов». ***(Герман Богапов. В киберцентре UA30 состоялись первые учения по кибербезопасности // Internetua (http://internetua.com/v-kibercentre-ua30-sostoyalis-pervye-ucseniya-po-kiberbezopasnosti). 19.05.2021).***

***

«Министерство цифровой трансформации провело масштабное мероприятие Diia Summit 2.0, куда пригласили руководство страны.

Бочка меда

На конференции руководители страны заявили о полном переходе на цифру с отказом от бумажных технологий. Из последних нововведений в “Дії” - изменение места регистрации онлайн, налоговая в несколько кликов, электронные петиции, е-подпись в смартфоне, автоматическая регистрация СПД и т.д. - более 10 новых электронных услуг. Обновления уже доступны на портале и в приложении.

«Мы уже сделали диджитал-революцию. Если раньше, чтобы получить целыйы ряд разрешений, надо было платить взятки. Были такие случаи. Сейчас надо платить только за интернет. Раньше - это десять кабинетов, сейчас - один сайт. Раньше - 50 справок в очередях, сейчас - три-четыре клика в смартфоне. Раньше - недели и месяцы, сейчас - 10-20 минут, чтобы открыть ФЛП или ООО в режиме онлайн. И если в прошлом году бизнес онлайн открывали лишь 5% предпринимателей Украины, то сегодня - 50%! - заявил Владимир Зеленский. - Мы - первая страна в мире, где цифровые паспорта имеют такую же юридическую силу, как и бумажные. Ряд документов - в смартфоне, возможность зарегистрировать новорожденного ребенка - в смартфоне, возможность изменить место регистрации - в смартфоне. Все в смартфоне. В общем, запущен десятки онлайн-услуг. Портал и приложения Дія, которыми пользуются сегодня более 10 миллионов граждан Украины. Нашим главным приоритетом остается вопрос национальной безопасности. в этом контексте полная построение цифровой государства дает возможность всем органам и службам эффективно работать онлайн при любых обстоятельствах, в любом месте, в любое время».

Он сообщил, что 24 августа этого года Украина войдет в режим “paperless” - никаких бумаг для государственных органов.

“Мы сделаем все, чтобы государство без бумаги существовало не на бумаге”, - скаламбурил президент.

Ложка дегтя

И это все замечательно, но надо обеспечить непрерывность функционирования сервисов. Эксперты неоднократно отмечали, что при разработке “Дія” не делался упор на соблюдении критериев безопасности.

А совсем недавно, 30 апреля, вдруг перестали работать Дія, helsi.me, часть сервисов Prozorro, e-construction.gov.ua и множество других сервисов государства в смартфоне. Полдня водители не могли предъявить цифровые удостоверения полиции, кто-то не смог показать свой электронный паспорт на самолет, а многие - записаться к врачу.

Тогда Минцифры сообщило, что произошел технический сбой хостинг-провайдера DeNovo на платформе G-Cloud. Программный сбой произошел в технологическом стеке виртуализации.

Мы обратились за комментариями к Максиму Агееву, CEO De Novo, и вот что он сообщил по результатам проведенного анализа ситуации:

В дисковой подсистеме произошел сбой в работе нескольких дисков. Это "мерцающая неисправность", которую крайне сложно идентифицировать. Поэтому на поиск причины ушло несколько часов. Мне очень жаль, что никто никогда не

писал о том, что облачные сервисы De Novo работают уже девять лет, и этот инцидент, хоть и не приятный, но первый за многие годы.

По результатам: было проведено внутреннее расследование, по итогам был составлен полный отчет о хронологии событий, все заказчики проинформированы. Данные и приложения клиентов не пострадали. Мы увеличили размер компенсации в пять раз по сравнению с контрактными условиями. “Дия” объявила о создании двухсайтовой катастрофоустойчивой архитектуры. Очевидно, делать такую архитектуру надо было изначально, но такого рода события абсолютно неуникальны и в других странах, и у глобальных провайдеров.

Мы полностью вывели из эксплуатации партию подозрительных дисков, всё работает стабильно. При этом именно качество наших процессов позволило закрыть такого рода проблему за несколько часов, а не дней. Я более чем уверен, что многие комплексы, находящиеся во владении крупных заказчиков, лежали бы дня два, а то и больше, при таком уникальном типе сбоя.

Хочется, чтобы в будущем разработчики критически важных продуктов в первую, а не вторую или третью, очередь обращали внимание на безопасность и стрессоустойчивость, а не прикрывались красивыми словами.

А то в очередной раз Минцифры заявило: «Кроме того, во время Diia Summit 2.0 анонсировали проведение нового этапа багбаунти, ведь безопасность Дії - один из главных приоритетов Минцифры. Открытый конкурс начнется в июне и продлится 6 месяцев. Призовой фонд - 1000000 гривен. Каждый (независимо от опыта или квалификации) сможет присоединиться». ***(Герман Богапов. Облачный провайдер De Novo расследовал причины сбоя приложения "Дія" // Internetua (http://internetua.com/oblacsnyi-provaider-de-novo-rassledoval-pricsiny-sboya-prilojeniya-diya-). 18.05.2021).***

***

«Навчання у форматі гри проводили для підвищення стійкості та рівня спеціалізованих знань і досвіду українських державних органів з питань кібербезпеки. Організатором виступила естонська компанія CybExer Tehnologies OU в рамках проєкту EU4DigitalUA під керівництвом Естонської академії електронного урядування.

17-19 травня правоохоронці у формі гри відпрацювали необхідні навички з формування безпечного кіберсередовища на технічному рівні. Окрім працівників Департаменту кіберполіції, участь у навчальних змаганнях також взяли команди Державного центру кіберзахисту Держспецзв’язку України та Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ.

Навчання складалося з теоретичної та практичної частини. Розпочали команди з ознайомлення з наявною інфраструктурою, а далі – безпосередньо виконували завдання з реагування на інциденти інформаційної безпеки, які були максимально наближені до реальних умов. За підсумками – працівники Департаменту кіберполіції одержали перемогу.

Актуальність проведення такого формату кібернавчань також полягає у перетинанні фахівців різнопрофільних структур та підрозділів, державного та приватного секторів задля досягнення спільної мети – забезпечення кібербезпеки.

Під час підбиття підсумків із промовою виступив начальник Департаменту кіберполіції Олександр Гринчак: «Проведення навчальних заходів, на кшталт сьогоднішніх, є вкрай важливими та необхідними в реаліях сьогодення. Навіть у формі гри, ми формуємо необхідні навички та напрацьовуємо алгоритми дій для прийняття у подальшому вірних та виважених управлінських рішень».

Олександр Гринчак подякував організаторам, міжнародним партнерам та вітчизняним колегам за сконсолідовані, професійні дії під час навчання. Він також зауважив, що Департамент кіберполіції готовий та відкритий до співпраці у сфері підтримки та вдосконалення безпеки у кіберпросторі». ***(Кіберполіцейські перемогли у міжвідомчих змаганнях з інформаційної безпеки // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpoliczejski-peremogly-u-mizhvidomchyx-zmagannyax-z-informaczijnoyi-bezpeky-5010/). 19.05.2021).***

***

«Наприкінці травня розпочнеться навчання ветеранів за програмою професійного розвитку у сфері кібербезпеки та реінтеграції для ветеранів АТО/ООС «Кіберзахисники».

Як розповідає кореспондентка Сусіпльного Ліля Гончарук, Це перша в Україні програма професійної підготовки та реінтеграції у сфері кібербезпеки для ветеранів з подальшою підтримкою ветеранів у відновленні та побудові кар'єри у сфері кібербезпек

Учасниками стануть ветерани, які пройшли конкурсний відбір і сформували першу групу слухачів.

На презентації навчання були присутні представники державних органів, що координують програму: Міністерства у справах ветеранів, Ради Національної безпеки та оборони; представники організаторів програми: Посольства США в Україні, CRDF Global, НТУУ «Київський політехнічний інститут імені Ігоря Сікорського», НУ «Києво-Могилянська академія».

Спікери розповіли про передумови запуску програми в Україні та ключові моменти навчального процесу. Навчання розпочнеться в онлайн-форматі 31 травня». ***(Тетяна Войтюк. Ветеранів АТО почнуть навчати кібербезпеці // АТ «НСТУ» (https://suspilne.media/134215-zno-z-matematiki-vidbudetsa-28-travna-so-vzati-z-sobou/). 24.05.2021).***

***

«Национальный депозитарий Украины (НДУ) получил грант для повышения уровня кибербезопасности общедоступных ресурсов НДУ business-critical уровня.

Как сообщает пресс-служба Нацдепозитария, это стало возможным благодаря сотрудничеству НДУ (Национального координационного центра кибербезопасности (НКЦК) при СНБО Совет национальной безопасности и

обороны. — Delo.ua) и Фондом гражданских исследований и развития Соединенных Штатов Америки (CRDF Global) (при поддержке Государственного департамента США).

В рамках реализации проекта планируется получение устройств и программных средств, реализующих надежную защиту от кибератак.

«Внедрение современных систем и модернизация средств защиты кибербезопасности инфраструктуры системы депозитарного учета вместе с соответствующей подготовкой персонала в сфере кибербезопасности является чрезвычайно важным для рынка и его участников и позволит обеспечить максимально высокий и эффективный уровень защиты информации в депозитарной системе Украины», — заявил председатель правления НДУ Миндаугас Бакас…». ***(Нацдепозитарий получил грант для усиления кибербезопасности // Delo.ua (https://delo.ua/business/nacdepozitarij-poluchil-grant-dlja-usilenija-kib-382258/). 24.05.2021).***

***

«С начала года в Украине не зафиксировано ни одного сообщения о несанкционированном вмешательстве в государственные реестры.

Как передает корреспондент Укринформа, об этом во время форума «Украина 30. Земля» сообщила заместитель министра юстиции Ольга Онищук.

По ее словам, обеспечение незыблемости имущественных и корпоративных прав на бизнес и недвижимость - основной приоритет государства.

«Эффективная защита прав собственников, а особенно хозяев и пользователей земельных участков, - это наше прошлое, настоящее и будущее. За последние 20 месяцев сделано много для того, чтобы приблизить регистрационные услуги к международным стандартам, чтобы они были безопасными, удобными и более понятными и для граждан, и для бизнес-сообщества», - отметила Онищук.

По ее словам, Министерство юстиции применяет действия по предотвращению любых рейдерских атак, в частности через государственные реестры. Благодаря принятым мерам в прошлом году удалось полностью обезопасить два основных реестра недвижимости и бизнеса от кибератак. Как подтверждение - в течение почти 5 месяцев с начала года в Украине не зафиксировали ни одного сообщения о несанкционированном вмешательстве в госреестры. Тогда как в прошлом году 40% жалоб на незаконные регистрационные действия были связаны именно с такими незаконными операциями.

«Мы очистили систему государственной регистрации от недобросовестных кадров. И не только благодаря тому, что в 2019 году аннулировали доступ к госреестрам коммунальным предприятиям (бывшим так называемым "аккредитованным субъектам"). Речь идет о настоящей "генеральной уборке" в рядах государственных регистраторов, нотариусов путем проведения специальных проверок и аннулирования свидетельств на предоставление права нотариальной деятельности нотариусам, которые нарушали закон. И сейчас дерзких нарушителей, которые осмеливаются совершать незаконные регистрационные действия, практически нет», - заверила Ольга Онищук.

Она также напомнила о деятельности открытого в декабре 2019 года Офиса противодействия рейдерству. Сейчас он осуществляет профессиональную экспертизу регистрационных действий, правомерность которых оспаривается.

«Есть инструмент мгновенного реагирования, который позволяет министру в течение одних суток отменять незаконные регистрационные действия при наличии очевидных грубых нарушений закона госрегистратором или нотариусом», - сказала она.

Теперь специалисты Минюста работают в двух направлениях: законодательном и техническом. В частности, ко второму чтению готовится законопроект №3774, который, помимо прочего, содержит антирейдерские предохранители для аграрного бизнеса. К примеру, вводится норма, согласно которой правовые действия относительно прекращения аренды земель сельскохозяйственного назначения будут признаваться "значительными", такими, которые могут быть заключены только с согласия общего собрания участников - то есть, с согласия собственника бизнеса.

«Чрезвычайно важным будет и введение единого цикла нотариального удостоверения договора отчуждения корпоративных прав и одновременной государственной регистрации прав на бизнес в результате заключения такого правового действия. Эта норма предусмотрена законопроектом о реформе нотариата, который в ближайшее время правительство внесет на рассмотрение парламента. И именно нотариат станет гарантом правовой чистоты заключения сделок при отчуждении земельных участков. Таким образом, нотариат осуществит самую большую миссию в открытии рынка земли», - убеждена Онищук.

Заместитель министра также рассказала о перспективах введения «технических щитов» в государственных реестрах.

«Важно выстроить систему госреестров таким образом, чтобы регистраторы и нотариусы не имели возможности проводить незаконные действия, а технические щиты блокировали любые попытки такого вмешательства. Сейчас готовим так называемые «островки безопасности», первые из которых уже до конца июня введем в систему государственных реестров», - подытожила Ольга Онищук…». ***(Государство защитило основные имущественные реестры от кибератак – Минюст // Укринформ (https://www.ukrinform.ru/rubric-economy/3251725-gosudarstvo-zasitilo-osnovnye-imusestvennye-reestry-ot-kiberatak-minust.html). 24.05.2021).***

***

«Кібербезпеку в держсекторі марно обговорювати у відриві від реальних завдань, які можна вирішити, адже всі ключові заходи залишаться в руках держави. Корисний івент має відповідати трьом важливим вимогам: рішення посильних завдань, наявність спікерів-учасників процесу, повнота розбору проблеми з орієнтацією на суб'єктів ІБ. Форум кібербезпеки 2021 саме такий.

Що це?

Форум — це майданчик для зустрічі і обміну думок фахівців, які перебувають по різні боки питання: представників бізнесу, постачальників рішень в

якості спікерів, а також ІБ-фахівців з держструктур і сфери енергетики як учасників.

Навіщо це?

Мета Форуму — дати сторонам розуміння проблем і завдань один одного, а також окреслити очікування і зміни, які чекають на них в майбутньому.

Як ми це зробимо?

За два дні:

Доповіді спікерів, на яких вони будуть розкривати свою сторону проблематики. Ви дізнаєтеся, як змінюються атаки, який вплив SOC на сферу ІБ, які активності і проекти вже реалізовані в цій темі, які є завдання на законодавчому рівні і чим небезпечна неповна і застаріла законодавча база. Також ви дізнаєтеся, як виглядають рішення, що відповідають викликам часу і здатні реагувати на існуючі та майбутні атаки. В рамках першого дня вас чекають дві панельні дискусії на глобальні теми Форуму: енергетика і державний сектор.

Кіберполігон — день для технічних фахівців галузі. Експерти в ІБ покажуть сценарії можливих кібератак, які зловмисники можуть здійснювати на рівні кінцевих точок, мережі, пошти та ін. Ми покажемо наживо, як можна швидко виявляти і реагувати на ці атаки. Йтиметься про технології, рішення, підходи та архітектуру ІБ. Цей досвід допоможе вам оцінити існуючі ризики безпеки для організації і зрозуміти, які підходи і технології потрібні для їх зниження до прийнятного рівня.

Хто там буде?

Євген Владіміров — заступник міністра з цифрового розвитку, цифрової трансформації та діджиталізації, Міненерго.

Олександр Галущенко — провідний інспектор, Апарат Ради національної безпеки і оборони України.

Андрій Кузьміч — начальник Державного центру кіберзахисту, Державна служба спеціального зв’язку та захисту інформації України.

Євген Єнтіс — заступник Голови з питань цифрового розвитку, цифрових трансформацій і цифровізації, Державна митна служба України.

Роман Боярчук — голова правління, Міжнародний університет кібербезпеки.

Василь Цвєтков — начальник центру кіберзахисту, Державне підприємство «Галузевий центр цифровізації і кібербезпеки».

Наталія Рєпіна — комерційний директор, Дата-центр «Парковий».

Коли, де, скільки кошутє?

Форум пройде в онлайн-форматі з 2 по 3 червня…». ***(Форум з кібербезпеки 2021. Держсектор і енергетика: як йдуть справи та що можна зробити вже зараз? // AIN.UA (https://ain.ua/2021/05/27/forum-z-kiberbezpeki-2021-derzhsektor-i-energetika-yak-jdut-spravi-ta-shho-mozhna-zrobiti-vzhe-zaraz/). 27.05.2021).***

***

«В Україні відкрили оновлений Кіберцентр UA30 – це перший крок до побудови системи кіберзахисту світового рівня.

Про це повідомили у пресслужбі Мінцифри.

Унікальність центру

Кіберцентр UA30 (вебсторінка нової платформи – ua30.gov.ua) входить до структури Державної служби спеціального зв'язку та захисту інформації України.

Це новітній державний центр реагування на кіберінциденти, здобуття навичок та знань у сфері кіберзахисту.

До його складу входить також оновлений тренінговий майданчик з унікальною технологією відпрацювання реальних сценаріїв кібератак у навчальному середовищі.

У світі налічується всього близько 20 таких платформ, шість з яких у США.

Завдання нової структури

Серед пріоритетів — захист критичної інформаційної інфраструктури. Це:

державні реєстри,

цифрові послуги,

державні інформаційні ресурси,

інформаційні системи критичних підприємств.

Питання кібербезпеки і зокрема захисту персональних даних громадян — один з головних пріоритетів Мінцифри.

Крім того, Кіберцентр стає адміністратором безпеки Національного центру резервування державних інформаційних ресурсів, куди до 2024 року мають бути перенесені 80% реєстрів.

Тут також працює урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA. Це єдина команда з України, що має акредитацію у FIRST та може оперативно взаємодіяти з командами реагування з 97 країн світу.

Кіберцентр надаватиме послуги кіберзахисту, виявлення та реагування на кіберзагрози як для державних організацій, так і для пересічних громадян. Це захист, який раніше був доступний лише державним структурам…» ***(Марина Конопльова. В Україні запрацював Кіберцентр UA30 для захисту держструктур і бізнесу від кібератак // #ШоТам (https://shotam.info/v-ukraini-zapratsiuvav-kibertsentr-ua30-dlia-zakhystu-derzhstruktur-i-biznesu-vid-kiberatak/). 13.05.2021).***

***

«В ходе третьего заседания Национального кластера по кибербезопасности, которое состоялось в конце апреля, участники обсудили будущую Стратегию кибербезопасности Украины и текущее состояние кибербезопасности в энергетическом секторе.

…об этом сообщает пресс-служба СНБО.

«Мощные кибератаки против энергетического сектора, которые произошли в 2015 и 2017 годах, ускорили разработки Аппаратом СНБО Украины новой Стратегии кибербезопасности Украины, которая, как ожидается, вскоре будет

утверждена на заседании СНБО Украины и введена в действие Указом Президента Украины. Важным элементом функционирования национальной системы кибербезопасности является обеспечение кибербезопасности объектов критической инфраструктуры (далее - ОКИ), в частности энергетического сектора», - заявил руководитель управления обеспечения деятельности Национальным координационным центром кибербезопасности при СНБО Украины (НКЦК) Сергей Прокопенко.

По его словам, развитие целостной системы обеспечения кибербезопасности ОКИ государства требует также четкого определения перечня их ИТС, создания и ведения общегосударственного реестра объектов критической инфраструктуры, проведения аудита информационной безопасности на объектах критической инфраструктуры, а также принятие соответствующего законодательства.

Заместитель министра энергетики Украины по вопросам цифрового развития, цифровых трансформаций и цифровизации Евгений Владимиров рассказал об основаниях и основных моментах формирования Концепции кибербезопасности в энергетической отрасли, которую разработало министерство. Как отмечается, документ сейчас находится в процессе согласования с заинтересованными государственными органами и вскоре будет представлен на утверждение в Кабинет Министров. Концепция, по его словам, коррелируется с национальной системой кибербезопасности, а также с общепринятыми международными стандартами NIST 800-SERIES, ISO 27000, NERC CIP, MITRE и др.

В свою очередь специалист по политическим вопросам Посольства США Натали Олдани отметила, что результаты заседаний Кластера высоко оцениваются американскими партнерами; благодаря этой платформе происходит эффективное сотрудничество ключевых партнеров и заинтересованных сторон, и Соединенные Штаты являются надежным партнером Украины в вопросах кибербезопасности.

Директор проекта деятельности USAID по кибербезопасности Тимоти Дюбель и Директор проекта энергетической безопасности Программы USAID в Украине Дин Уайт рассказали об основных направлениях и текущих проектах помощи USAID украинской энергетической экосистеме, улучшении ее кибербезопасности и устойчивости к разным угрозам.

Кроме того, по словам пресс-службы, старший менеджер проектов по кибербезопасности представительства CRDF Global Ольга Стрельцова представила первую в Украине программу профессиональной подготовки и реинтеграции в сфере кибербезопасности для ветеранов АТО/ООС с последующей поддержкой ветеранов в восстановлении и построении карьеры в сфере кибербезопасности.

Участники мероприятия обсудили нынешнее состояние кибербезопасности и проекты основных стейкхолдеров энергетического сектора Украины, в частности, ПАО Национальная энергетическая компания «Укрэнерго», НАК «Нафтогаз України», ООО «Оператор ГТС Украины», ГП «Национальная атомная энергогенерирующая компания «Энергоатом», ООО «ДТЭК», ЧАО «Укргидроэнерго».

Участие в мероприятии также приняли представители основных субъектов обеспечения кибербезопасности Украины, посольств иностранных государств,

представители частного сектора и общественных организаций, донорских и международных организаций, в частности USAID, DAI и т. п.

Организаторы Кластера призвали участников и основных докладчиков определить проблемные вопросы и проекты в энергетическом секторе, к решению которых целесообразно привлечь международную техническую либо консультационную помощь в целях эффективного воплощения приоритетных проектов по кибербезопасности на национальном уровне…» ***(В Украине обсудили Концепцию кибербезопасности в энергетической отрасли // Укринформ (https://www.ukrinform.ru/rubric-economy/3240384-v-ukraine-obsudili-koncepciu-kiberbezopasnosti-v-energeticeskoj-otrasli.html). 05.05.2021).***

***

Правове забезпечення кібербезпеки в Україні

«Новый проект Стратегии кибербезопасности Украины в ближайшее время будет вынесен на рассмотрение Совета национальной безопасности и обороны.

Об этом рассказала руководитель службы по вопросам информационной безопасности и кибербезопасности аппарата СНБО Наталья Ткачук во время Всеукраинского форума «Украина 30. Безопасность страны», сообщает корреспондент Укринформа.

«Национальный координационный центр кибербезопасности (НКЦК) по поручению Президента Украины уже завершил работу над проектом новой стратегии, и мы ожидаем, что он будет вынесен на рассмотрение СНБО», - сказала Ткачук.

По ее словам, к работе над проектом были привлечены СБУ, Госспецсвязи, Нацполиция, НБУ, Генштаб ВСУ, Минобороны, Министерство цифровой трансформации, комитеты ВР, представители частного сектора и международные партнеры.

Ткачук отметила, что новый проект стратегии является открытым документом, он обнародован в полном объеме на сайте СНБО. По ее словам, многие предложения, которые вносились во время работы над документом, были учтены.

Представительница аппарата СНБО также обратила внимание на то, что в Украине пока отсутствует перечень объектов критической инфраструктуры и соответствующий закон в этой сфере, что существенно усложняет работу по киберзащите, а также не в полной мере имплементирована Конвенция Совета Европы по киберпреступности.

По ее мнению, нуждается в улучшении и система подготовки кадров в сфере кибербезопасности.

Ткачук напомнила, что в 2014 году, с началом гибридной агрессии РФ, Украина превратилась в полигон, где испытывалось кибероружие РФ. Тогда впервые военные действия страны-агрессора сопровождались атаками на объекты критической инфраструктуры Украины. В 2016 году была принята Стратегия

кибербезопасности, которая стала основой развития национальной системы кибербезопасности.

Украина уже может делиться опытом локализации кибератак, и большая заслуга в этом киберволонтеров, которые поддерживали государственные органы в борьбе с агрессором, подчеркнула представительница аппарата СНБО.

При этом, по ее убеждению, в состав Национального координационного центра кибербезопасности необходимо ввести специалистов Министерства иностранных дел.

«Очень существенно возрастает роль международного сотрудничества. И мы видим, что следующим членом НКЦК должен стать МИД. Потому что без международного взаимодействия невозможно преодолеть актуальные киберугрозы», - отметила Ткачук…». ***(Обновленную Стратегию кибербезопасности вынесут на рассмотрение СНБО // Укринформ (https://www.ukrinform.ru/rubric-polytics/3244770-obnovlennuu-strategiu-kiberbezopasnosti-vynesut-na-rassmotrenie-snbo.html). 13.05.2021).***

***

«Рада нацбезпеки та оборони (РНБО) ухвалила стратегію кіберзахисту України до кінця 2025 року, яка дозволить зробити країну передовою державою в цій сфері. Про це заявив міністр цифрової політики Михайло Федоров після засідання РНБО…

«Перше питання стосувалося кібербезпеки нашої країни. Хочу зазначити, що була ухвалена стратегія розвитку кібербезпеки на наступні п'ять років. Мені здається, що і підхід до формування цієї стратегії, і якість формування документа, і актуальність – вони на найвищому рівні», – сказав він.

Міністр додав, що все – від аудиту сьогоднішньої ситуації, від розуміння того, що нам потрібно робити, щоб наша країна стала за кіберзахистом передовою країною світу – зазначено у стратегії…» ***(Влада ухвалила стратегію кіберзахисту України до 2025 року // 5 канал (https://www.5.ua/polityka/vlada-ukhvalyla-stratehiiu-kiberzakhystu-ukrainy-do-2025-roku-244438.html). 14.05.2021).***

***

«Президент Володимир Зеленський найближчим часом може підписати указ про створення кібервійськ. Це питання обговорювалося на засіданні Ради національної безпеки і оборони в п'ятницю, 14 травня, повідомив секретар РНБО Олексій Данілов.

«Сьогодні в таємному режимі ми розглядали питання створення кібервійськ у нашій країні. Можу сказати, що це рішення підтримане всіма 21 членами одноголосно, присутніми на засіданні. Я думаю, що найближчим часом буде указ президента про це. Ви дізнаєтеся від президента», - заявив Данілов в ефірі ток-шоу «Свобода слова Савіка Шустера».

Серед восьми питань, що розглядалися на засіданні РНБО, було затвердження стратегії кібербезпеки України. Також розглядалося питання біологічної безпеки.

Крім того, за словами Данилова, на засіданні РНБО було «ухвалено важливе і фундаментальне рішення щодо ліків і вакцин», зміст якого поки що не розголошується…». ***(Данілов розповів про плани створення українських кібервійськ // Дзеркало тижня. Україна (https://zn.ua/ukr/UKRAINE/danilov-rozpoviv-pro-plani-stvorennja-ukrajinskikh-kibervijsk.html). 15.05.2021).***

***

«Рада національної безпеки та оборони України на засіданні 14 травня затвердила Стратегію кібербезпеки України на 2021-2025 роки, а також ухвалила рішення про створення загальнонаціональної цифрової багатоканальної телемережі Мультиплекс МХ-7.

Як повідомляє кореспондент Укрінформу, про це заявив віцепрем'єр-міністр - міністр цифрової трансформації Михайло Федоров під час брифінгу за підсумками засідання РНБО під головуванням Президента Володимира Зеленського.

«Сьогодні два важливих рішення було прийнято, які стосуються нашої діяльності. Це - Стратегія кібербезпеки нашої країни, і тепер у нас є офіційний документ, який нам дозволяє і фінансувати, і здійснювати заходи в цьому напрямку, і покращувати ту ситуацію, в якій ми знаходимось. І другий важливий крок - це рішення про створення і виділення фінансування для побудови Мультиплексу МХ7, який дозволить нам більш якісніше комунікувати з українцями і покращить сигнал», - зазначив Федоров, додавши що Стратегія кібербезпеки є якісним та актуальним документом.

Крім того, Федоров нагадав, що нині в Україні склалася ситуація, коли мешканці прикордонних областей не мають змоги безкоштовно дивитись українські телеканали. Адже минулого року відбулося кодування супутникового телебачення, а єдиний оператор цифрового мовлення покриває не всю країну. Мешканці прикордонних областей наразі позбавлені цього сигналу, а для того, аби продовжити дивитись українські телеканали, їм необхідно купувати новий тюнер та оформлювати підписку з провайдером.

Тож рішення про створення загальнонаціональної цифрової багатоканальної телемережі Мультиплекс МХ-7 вирішить згадані проблеми, наголосив міністр.

Як повідомила Державна служба спеціального зв'язку та захисту інформації України за результатами засідання РНБО, завдяки Мультиплекс МХ-7 до кінця 2021 року доступ до якісного цифрового мовлення МХ-7 буде на 95% підконтрольної території України, навіть у прикордонних регіонах. Державна інфраструктура ефірного цифрового телебачення запрацює у 158 населених пунктах, у тому числі – на прикордонних територіях.

МХ-7 транслюватиме щонайменше 12 каналів. Перш за все державні телекомпанії та Суспільне мовлення. Наповнення мережі визначатиме Національна рада України з питань телебачення і радіомовлення. Канали будуть незакодовані.

«Мережа МХ-7 будується за технологією європейського стандарту ефірного цифрового телебачення другого покоління (DVB-T2). Мовлення здійснюватиметься в смузі частот метрового діапазону 174-230 МГц. Хвилі у цьому діапазоні добре проникають в будівлі і покривають великі території. Для отримання сигналу користувачі потребуватимуть антени, що залишились у багатьох після вимкнення

аналогового мовлення, та цифрового тюнера. Доступ до контенту – безкоштовний», - повідомляють у Держспецзв'язку.

Оператором мультиплексу визначений державний Концерн радіомовлення, радіозв'язку та телебачення, що входить до сфери управління Держспецзв'язку…». ***(Стратегія кібербезпеки і потужний телесигнал: РНБО ухвалила «цифрові» рішення // Укрінформ (https://www.ukrinform.ua/rubric-polytics/3245725-rnbo-zatverdila-strategiu-kiberbezpeki-ukraini-do-2025-roku.html). 14.05.2021).***

***

«Национальный банк повышает уровень информационной безопасности и киберзащиту в сфере перевода средств…

С целью усиления надежности и эффективности работы платежных систем регулятор устанавливает четкие требования к участникам платежного рынка относительно: построения системы защиты информации и обеспечения кибербезопасности, а также порядка действий во время обнаружения кибератак, которые снижают надежность функционирования платежных систем.

Соответствующие новации изложены в постановлении Правления Национального банка Украины от 19 мая 2021 года №43 «Об утверждении Положения о защите информации и киберзащите в платежных системах», требования которого распространяются на: платежные организации платежных систем, созданных резидентами Украины, операторов услуг платежной инфраструктуры, участников платежных систем.

Документ предусматривает: введение риск-ориентированного подхода к защите информации в зависимости от суммы возможных убытков (требования к ключевым участникам платежного рынка будут усиливаться), установление требований к использованию средств защиты информации, определение политики управления доступом и повышение уровня безопасности платежных услуг для пользователей.

Это даст возможность минимизировать количество инцидентов информационной безопасности и киберинцидентов в сфере перевода средств, урегулировать вопросы использования средств защиты информации, а также ускорить процесс модернизации платежных систем с учетом современных технологий защиты информации.

Постановление №43 вступает в силу с 29 мая 2021 года.

В то же время участники платежного рынка будут иметь комфортный переходный период (следующие 12 месяцев), чтобы доработать свои внутренние процедуры и документы относительно информационной безопасности и киберзащиты и привести свою деятельность в соответствие с требованиями этого постановления». ***(НБУ повышает киберзащиту в сфере перевода средств // Укринформ (https://www.ukrinform.ru/rubric-economy/3254712-nbu-povysaet-kiberzasitu-v-sfere-perevoda-sredstv.html). 28.05.2021).***

***

«Зростання кібератак під час посилення концентрації військ Росії на кордонах з Україною було зафіксовано співробітниками СБУ.

– Так, дійсно, ми фіксували таке зростання, – заявив начальник управління Департаменту кібербезпеки СБУ Ілля Вітюк під час форуму Україна 30. Безпека країни.

За словами Вітюка, за 2021 рік СБУ зафіксувала понад 600 кібератак і інцідентів. Зважаючи на це, ключовою вимогою служби є саме посилення системи протидії кіберзагрозам.

Наразі службовці "створюють чітку дорожню карту", зокрема персоніфікують відповідальність за такі злочини.

Вітюк відзначив високий рівень протидії кіберзагрозам всіх служб країни.

Він також підкреслив, що вдалося налагодити системну роботу з протидії кіберзагрозам як в частині фінансового та матеріального забезпечення, так і в належній підготовці кадрів…» ***(Абрамова Юлія. СБУ зафіксувала 600 кібератак під час військових дій РФ поблизу кордонів України // ФАКТИ. ICTV (https://fakty.com.ua/ua/ukraine/20210513-sbu-zafiksuvala-600-kiberatak-pid-chas-vijskovyh-dij-rf-poblyzu-kordoniv-ukrayiny/). 13.05.2021).***

***

«Во время наращивания военного присутствия у украинской границы Россия увеличила количество кибератак на Украину.

Об этом на Форуме «Украина 30» сказал начальник управления Департамента кибербезопасности Службы безопасности Илья Витюк, сообщается на сайте СБУ.

«СБУ зафиксировала существенный рост количества кибератак накануне и во время скопления военных РФ вблизи госграницы Украины», — заявил он.

Витюк отметил, что ситуация в киберсфере нуждается во всестороннем подходе к предупреждению хакерских атак и противодействию угрозам.

По его словам, благодаря уникальному опыту по блокированию сложных кибератак СБУ выстроила эффективные партнерские отношения с ведущими мировыми спецслужбами, выступает флагманом в противодействии угрозам кибербезопасности национального уровня, способствует консолидации усилий гражданского общества и госорганов.

Представитель СБУ заявил, что сейчас идет активная наработка правовой и законодательной базы для слаженной работы органов власти, частного сектора и объектов критической инфраструктуры. Он отметил, что уровень терроризма и шпионажа в киберсфере, которые выступают инструментами гибридной войны, давно стал критическим в мире и продолжает повышаться.

Витюк сообщил, что только за этот неполный год СБУ удалось нейтрализовать более 600 кибератак и инцидентов, разоблачить попытки кибершпионажа в отношении украинских органов исполнительной власти, а также субъектов в сфере безопасности и обороны. При этом он отметил, что даже одна хорошо организованная хакерская атака может закончиться непоправимым вредом

и привел в пример недавнюю атаку на компьютерные системы нефтепровода в США…» ***(В СБУ заявили о росте кибератак России на Украину // Хвиля (https://hvylya.net/news/230452-v-sbu-zayavili-o-roste-kiberatak-rossii-na-ukrainu). 13.05.2021).***

***

Боротьба з кіберзлочинністю в Україні

«Суд приговорил к штрафу жителя Винницы за создание вредоносного программного обеспечения…

В ходе досудебного расследования было установлено, что в июне 2017 года подсудимый приобрел у неустановленного следствием лица и загрузил на свой ноутбук программу «All-in-One-Checker».

В дальнейшем злоумышленник модифицировал вышеуказанную программу и использовал её для получения персональных данных пользователей, о чем, согласно заключению эксперта, свидетельствует содержание имеющегося на изъятых носителях каталога «Results», который содержится в папке с исполняемым файлом «AIOC.exe».

Указанные действия подсудимого органом досудебного расследования были квалифицированы по ч. 1 ст. 361-1 УК Украины (создание с целью использования вредоносных программных средств, предназначенных для несанкционированного вмешательства в работу компьютерных сетей).

В сентябре 2020 года между подозреваемым и прокурором было заключено соглашение о признании виновности, согласно которому стороны договорились о формулировке обвинения, всех существенных для данного уголовного производства обстоятельств, подозреваемый в полном объеме сформулированного обвинения безоговорочно признал свою виновность в совершении данного уголовного преступления. Также, сторонами сделки определено согласованное ими наказания в виде штрафа в размере 8500 гривен (500 необлагаемых минимумов доходов граждан).

Суд утвердил вышеуказанное соглашение. Кроме этого, подсудимый должен оплатить сумму в размере 16018 гривен за проведение судебных компьютерно-технических экспертиз». ***(Артем Сереженок. Суд приговорил украинца к штрафу за создание вредоносного ПО // Internetua (http://internetua.com/sud-prigovoril-ukrainca-k-shtrafu-za-sozdanie-vredonosnogo-po). 02.05.2021).***

***

«Руководитель небольшой львовской ИТ-компании, предлагающей услуги «неотложной компьютерной помощи», предлагал клиентам установку, настройку, обновление и конфигурацию программ «1С:Предприятие».

Клиенты могли самостоятельно выбрать: хотят ли они установить лицензионную или пиратскую версии ПО. Соответствующее объявление айтишник разместил в интернете.

Там оно попало в поле зрения сотрудников консалтинговой компании ТОВ «Международная правовая группа», представляющей в Украине интересы эстонского правообладателя программного продукта – «Molenari OU».

Чтобы наказать львовского айтишника за нарушение авторских прав, юристы связались с ним и заказали установку программы «1С: Предприятие 8.3», в «бюджетной» взломанной версии. Стоимость этой услуги составила всего лишь 500 гривен, в то время как лицензионная программа, на тот момент, стоила около 40 тысяч гривен.

Специалист произвел установку указанной программы «1С: Предприятие 8.3» в конфигурации «Управление торговым предприятием для Украины». Сделал он это при помощи программы TeamViewer, которая позволяет удаленно производить манипуляции на чужом компьютере Чтобы программа заработала в обход лицензионных ключей, ему пришлось применить патчи, которые активируют программу для пиратского использования.

После того, как юристы получили неоспоримое доказательство нарушения авторских прав, потребовался еще целый год, прежде чем они обратились в правоохранительные органы, которые санкционировали повторную контрольную закупку противозаконной услуги, которая могла бы быть приобщенной к уголовному делу.

На этот раз специалист прибыл в офис компании и собственноручно произвел установку и настройку ПО, получив за свои услуги 700 гривен, чем повторно нанес правообладателю ущерб в размере 45 тысяч гривен.

Его действия были квалифицированы сразу по двум статьям Уголовного Кодекса Украины – ст.176 «Нарушение авторского и других смежных прав», а также ст.361 «Несанкционированное вмешательство в работу компьютерных систем».

Собранных улик и показаний свидетелей хватило, чтобы доказать в суде вину, однако обвиняемый отказался признавать ее и не стал свидетельствовать против себя, сославшись на ст. 63 Конституции Украины. Кроме того, он поставил под сомнение правомерность некоторых следственных действий, включая обыск в офисе консалтинговой компании, поскольку он не был санкционирован судом, а проводился полицейскими с разрешения хозяев помещения. Это несколько усложнило и затянуло разбирательство.

Права на программное обеспечение «1С» ранее принадлежали российскому разработчику. Однако, с началом вооруженного конфликта между Россией и Украиной, данная компания, вместе с дочерними компаниями, попала в санкционный список и утратила право продавать свою продукцию на территории Украины и передавать кому-либо права на нее.

С этого момента, на сцену выходит некая эстонская компания, заявляющая, что является новым правообладателем программного обеспечения «1С». К примеру, Черкасский суд, который состоялся по аналогичному поводу в 2019 году, претензии представителей иностранного «правообладателя» опроверг:

«Утверждение компании «Molenari OU» о принадлежности ей прав на основании факта создания программы вызывают сомнения и опровергаются общеизвестными данными российских правообладателей на использование

программного обеспечения. Учитывая то, что компания «Molenari OU» не является надлежащим юридическим лицом, которому принадлежат исключительные права интеллектуальной собственности, соответственно она не вправе разрешать или запрещать продавать программный продукт, который является предметом договора, на территории Украины», - говорится в постановлении суда.

Тем не менее, Львовский суд рассудил иначе и обвиняемому присудили 2 года лишения свободы, которые заменили испытательным сроком в 1 год, с обязательным возмещением причиненного «правообладателю» ущерба в полном объеме – 83,086 гривен 00 копеек». ***(Андрей Майданик. Украинского айтишника осудили за нарушение авторских прав российской компании, находящейся под санкциями //Internetua (http://internetua.com/ukrainskogo-aitishnika-osudili-za-narushenie-avtorskih-prav-rossiiskoi-kompanii-nahodyasxeisya-pod-sankciyami). 05.05.2021).***

***

«Кіберфахівці Служби безпеки України у Чернігові припинили діяльність ботоферми, яку адміністрували з Росії.

…про це повідомляє Служба безпеки України.

Співробітники спецслужби встановили, що через ботоферму поширювалась фейкова інформація для створення панічних настроїв серед населення. Зокрема розміщувались повідомлення для дискредитації української влади і заклики до повалення конституційного ладу. Також боти публікували неправдиву інформацію про мінування об’єктів, у тому числі критичної інфраструктури.

Виконавці використовували спеціалізований апаратно-програмний комплекс, через який, зокрема здійснювали транзакції у санкційних електронних платіжних системах.

Під час обшуку за місцем проживання організатора, де знаходилась ботоферма, правоохоронці вилучили сім 16-канальних GSM-шлюзів; дві сім-банки на 128 карток кожен; 370 сім-карток російського мобільного оператора; три ноутбуки, через які здійснювалось керування телекомобладнанням ботоферми…». ***(СБУ заблокувала ботоферму, яку адміністрували з Росії // Укрінформ (https://www.ukrinform.ua/rubric-regions/3250303-sbu-zablokuvala-botofermu-aku-administruvali-z-rosii.html). 21.05.2021).***

***

«У Києві затримали двох братів, які торгували даними українців. Усього в їхній базі було 32 мільйони осіб. Дані отримували від працівників банків і державних органів. Інформацію ділки продавали на одному зі столичних ринків під виглядом комп'ютерних ігор.

Під час обшуків у зловмисників вилучили ноутбуки, жорсткі диски, телефони та накопичувачі інформації. Одному затриманому суд уже призначив домашній арешт. Щодо іншого - запобіжний захід ще обирають». ***(Просяник Олександр. Кияни торгували даними українців під виглядом комп'ютерних ігор // ООО "Национальные информационные системы" (https://podrobnosti.ua/2401004-kijani-torguvali-danimi-ukrantsv-pd-vigljadom-kompjuternih-gor.html). 06.05.2021).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Питання кібербезпеки – дуже важливе для України з огляду на російську агресію, тому вона веде дуже активний кібердіалог зі Сполученими Штатами, які мають великий досвід, заявила посол України у США Оксана Маркарова.

За її словами, з початку російської агресії у 2014 році Україна зазнає різноманітних кібератак як на критично важливу інфраструктуру, так і на банки, на фінансову систему.

Маркарова повідомила, що у взаємодії з американськими колегами зупинили понад 350 таких кібератак.

– Ми хочемо підняти це питання на наступний рівень. Тобто, крім активної двосторонньої співпраці зі США, ми також заявили про своє бажання приєднатися до навчань Cyber Flag, що дозволить нам розширити тренування та навчання фахівців, – розповіла посол…». ***(Валентина Летяк. Україна планує долучитися до американських навчань Cyber Flag з кібербезпеки // ФАКТИ. ICTV (https://fakty.com.ua/ua/ukraine/20210514-ukrayina-planuye-doluchytysya-do-amerykanskyh-navchan-cyber-flag-z-kiberbezpeky/). 14.05.2021).***

***

«Украина будет первой среди стран Восточного партнерства, с которой Европейский Союз планирует начать тесный диалог в сфере кибербезопасности в рамках программы EU4Digital.

Об этом заявил руководитель программ сотрудничества Представительства ЕС в Украине Фредерик Куне в видеообращении к участникам Всеукраинского форума «Украина 30. Безопасность страны», сообщает корреспондент Укринформа.

Куне отметил, что сотрудничество между Украиной, ЕС и США стало решающим фактором в создании безопасного киберпространства в Украине.

«В рамках Программы EU4Digital в Украине, которая, по сути, направлена на трансграничное цифровое развитие, мы предлагаем проводить технические учения и налаживать взаимодействие между ведомствами, которые занимаются цифровизацией, и "Киберцентром UA30 ". Перед следующим саммитом (Восточного партнерства - ред.) Мы будем запускать именно такой диалог в сфере кибербезопасности. Украина будет первой страной добрососедства, с которой будет установлен такой диалог», - сказал Кунео.

Он заверил, что Европейский Союз и в дальнейшем будет тесно сотрудничать с Украиной в сфере кибербезопасности. Это сотрудничество будет включать, в частности, повышение потенциала страны, а также совместные действия на международных площадках и обмен соответствующим опытом…

Программа EU4Digital дополняет двустороннюю поддержку ЕС для Украины в применении решений электронного управления для местных органов власти и в

повышении функциональной совместимости административных услуг, а также в повышении устойчивости киберпространства, особенно перед выборами». ***(Украина - первая среди стран Восточного партнерства, с которой ЕС планирует тесный кибердиалог // Укринформ (https://www.ukrinform.ru/rubric-technology/3244662-ukraina-pervaa-sredi-stran-vostocnogo-partnerstva-s-kotoroj-es-planiruet-tesnyj-kiberdialog.html). 13.05.2021).***

***

«Глава Служби безпеки України Іван Баканов заявив, що СБУ зацікавлена у співпраці з американськими спецслужбами з низки важливих питань, що стосуються нацбезпеки, зокрема, кібербезпеки, протидії гібридній війні, боротьби з тероризмом і професійної підготовки співробітників. Про це повідомив пресцентр спецслужби в понеділок, 17 травня.

«Партнерство зі США дозволяє більш ефективно захищати нашу державу. А це дуже важливо, коли Україна протистоїть такому потужному ворогу, як Росія. І присутність цієї загрози вимагає від нас діяти системно й ефективно», - сказав Баканов в ході зустрічі з представниками Американської ради зовнішньої політики (AFPC).

За словами глави української спецслужби, Стратегія нацбезпеки визначає для України євроатлантичної вектор.

«Україна прагне отримати статус основного союзника США поза НАТО, а в перспективі - членство в Альянсі. На переконання глави СБУ, це буде сприяти не тільки військовій співпраці, а й ефективному захисту України від російської агресії і деокупації Донбасу й Криму», - уточнив глава СБУ, акцентувавши на тому, що таке партнерство варто розширювати вже сьогодні.

Уточнюється, що українська спецслужба особливо зацікавлена, зокрема, в кібербезпеці, протидії гібридній війні, боротьбі з тероризмом і професійній підготовці співробітників.

Глава СБУ закликав AFPC сприяти приєднанню України до ініціативи президента США Cyber Flag для колективного захисту держав в кіберпросторі…» ***(СБУ зацікавлена у співпраці з американськими спецслужбами в питаннях кібербезпеки — Баканов // Дзеркало тижня. Україна (https://zn.ua/ukr/POLITICS/sbu-zatsikavlena-u-spivpratsi-z-amerikanskimi-spetssluzhbami-v-pitannjakh-kiberbezpeki-bakanov.html). 17.05.2021).***

***

«Министр иностранных дел Великобритании Доминик Рааб в среду призвал к глобальному сотрудничеству в борьбе с кибератаками со стороны «враждебных государственных субъектов» и преступных группировок.

Raab также пообещал выделить 22 миллиона фунтов (31 миллион долларов) в поддержку «уязвимых» стран Африки и Индо-Тихоокеанского региона для повышения их потенциала цифровой защиты.

Он сказал, что Великобритания и Запад должны усилить кибербезопасность или столкнуться с «многосторонним вакуумом», который заполняют Китай и Россия.

«Нам нужно сочетание устойчивой защиты, а также наступательных возможностей и глобального дипломатического влияния, которое дает современная киберсила», - сказал Рааб в речи на конференции Национального центра кибербезопасности в Лондоне.

Он сказал, что финансирование пойдет на национальные группы киберреагирования, информационные кампании и операционный центр Интерпола в Африке.

Министр иностранных дел обвинил Москву и Пекин в том, что они входят в число «авторитарных режимов», которые не принимают мер против кибератак, исходящих с их собственной территории.

Он сказал, что выборы стали «главной целью» вмешательства с целью дестабилизации демократических государств.

В прошлом месяце администрация Байдена объявила о санкциях против России и изгнала дипломатов из-за масштабной хакерской кампании, нацеленной на федеральные агентства, известной как нарушение SolarWinds, а также за вмешательство в голосование.

Россия, которая отрицала свою причастность к нарушению, ответила тем же на то, что она назвала неспровоцированными действиями.

В апреле Китай отрицал связь с работой хакеров, которые месяцами шпионили за десятками важных государственных, оборонных и финансовых объектов в США и Европе с помощью устройств Pulse Connect Secure.

Рааб также рассказал об атаках на программы исследования вакцины COVID-19 и цепочки поставок в Великобритании, а также на университеты, школы и больницы. «Кажется, что для киберпреступников нет почти ничего запретного», - сказал он.

Ранее в этом месяце Рааб встречался с министрами иностранных дел стран Большой семерки в Лондоне, и вопрос безопасности был на первом месте.

Были также приглашены высокопоставленные дипломаты из Австралии, Индии, Южной Африки и Южной Кореи, при этом Рааб сказал, что завоевание доверия «единомышленников» было «необходимо».» ***(UK Foreign Secretary Calls for Cooperation on Cybersecurity // Wired Business Media (https://www.securityweek.com/uk-foreign-secretary-calls-cooperation-cybersecurity). 13.05.2021).***

***

«Заступник голови Офісу президента України Ігор Жовква заявив, що низка положень Угоди про асоціацію між Україною та ЄС у частині цифровізації потребують оновлення, щоб зафіксувати досягнення України у цій сфері за останні роки.

Про це він сказав під час виступу на Всеукраїнському форумі "Україна 30. Цифровізація"…

«Відтоді (з моменту укладення Угоди у 2014 році - ред), особливо за два останні роки, Україна настільки стрибнула вперед у сфері цифрового ринку, нам треба цю Угоду переглядати в частині «цифри». Тому я звертаюся до наших

європейських колег - переглянути додаток XVII до цієї Угоди, зафіксувати його в актуальному контексті», - зазначив Жовква.

Він наголосив, що наразі Україна випереджає деякі країни Євросоюзу у сфері диджиталізації, тому Угода потребує оновлення в цій частині.

Жовква також зазначив, що Євросоюз позитивно оцінив рух України до Єдиного цифрового ринку згідно з планом, затвердженим на саміті Україна - ЄС у жовтні 2020 року.

"На саміті, який відбудеться цього року, я гадаю, ми фіксуватимемо на папері визначені досягнення та визначатимемо нові амбітні кроки", - упевнений він.

За його словами, план інтеграції в цифровий ринок ЄС, який реалізує Україна, передбачає, зокрема, запровадження Європейського кодексу електронних комунікацій і посилення кібербезпеки.

«Кібербезпека - це загальний виклик і для України, і для держав-членів ЄС, і для всього світу. І Україна має позитивний досвід співпраці з ЄС у питанні кіберзахисту, зокрема під час виборів у 2019 році, щоб уникнути втручання в критичну інфраструктуру», - зазначив Жовква.

Важливими аспектами інтеграції України у цифровий ринок Євросоюзу також є захист персональних даних, електронні довірчі послуги та скасування роумінгу з державами-членами ЄС. Крім того, Україна та Євросоюз працюють над взаємним визнанням «цифрових зелених сертифікатів».

Жовква наголосив, що Україна робить дуже багато на шляху до Єдиного цифрового ринку ЄС.

«Сподіваюся, що наприкінці цього року ми з ЄС підіб'ємо позитивні підсумки і намітимо нові цілі та завдання», - резюмував він». ***(В ОП хочуть оновлення положень Угоди про асоціацію з ЄС в частині цифровізації // Європейська правда (https://www.eurointegration.com.ua/news/2021/05/19/7123372/). 19.05.2021).***

***

«Співпраця з США надає Україні більше можливостей для побудови ефективної системи національної безпеки.

Про це голова СБУ Іван Баканов сказав під час зустрічі з представниками Американської ради зовнішньої політики (AFPC), повідомляє Укрінформ з посиланням на пресцентр СБУ.

«Партнерство з США дозволяє більш ефективно захищати нашу державу. А це дуже важливо, коли Україні протистоїть такий потужний ворог, як Росія. І присутність цієї загрози вимагає від нас діяти системно та ефективно», – наголосив Баканов.

Він зауважив, що Стратегія національної безпеки визначає для України лише євроантлантичний вектор. На його думку, таке партнерство варто розширювати.

За словами голови СБУ, Україна прагне набути статусу основного союзника США поза НАТО, а в перспективі – членства в Альянсі. На переконання Баканова, це сприятиме не лише військовому співробітництву, а й ефективному захисту України від російської агресії та деокупації сходу України і Криму.

Очільник відомства також окреслив напрями співпраці з США, в яких особливо зацікавлена українська спецслужба. Зокрема, це кібербезпека, протидія гібридній війні, боротьба з тероризмом, фахова підготовка співробітників.

Крім того, він закликав AFPC сприяти приєднанню України до ініціативи президента США «Cyber Flag» для колективного захисту держав у кіберпросторі.

Американську сторону на зустрічі представляли президент Американської Ради з питань зовнішньої політики Герман Пірчнер, посол США в ОБСЄ у 2019-2021 роках Джеймс Гілмор, колишній заступник постійного представника США в ООН Джон Лернер, директор Центру відносин США-Україна у м. Вашингтон Микола Грицковян, старший науковий співробітник AFPC та колишній заступник помічника президента та керівника апарату Ради національної безпеки США при Білому домі Александр Грей…». ***(Баканов назвав напрями співпраці Служби безпеки з США // Укрінформ (https://www.ukrinform.ua/rubric-polytics/3246640-bakanov-nazvav-naprami-spivpraci-sluzbi-bezpeki-z-ssa.html). 17.05.2021).***

***

«Європейський Союз вчиться в України не лише протистояти Росії у військовій сфері, а й протидіяти кампаніям дезінформації та кібератакам.

Про це заявив посол ЄС в Україні Матті Маасікас на форумі «Україна 30. Безпека країни», повідомляє кореспондент Укрінформу.

Голова Представництва ЄС відзначив, що міжнародна підтримка України, її суверенітету та територіальної цілісності в межах міжнародно визнаних кордонах є надзвичайно сильною і базується на спільних цінностях та міжнародному праві.

«Наша співпраця з Україною – це не дорога з одностороннім рухом. Це не те, що Євросоюз допомагає Україні, а Україна тільки отримує допомогу… ЄС вчиться в України не тільки досвіду війни проти РФ, а й тому, яким чином протистояти гібридній агресії, постійним кампаніям дезінформації, а також як протистояти кібератакам. І це не збіг, що Україна є однією з шести країн світу, з ким ЄС має дуже активний діалог з теми кібербезпеки», - сказав Маасікас.

Він додав, що ЄС робить усе можливе, щоб підтримати Україну на економічному та політичному рівні. У цьому контексті дипломат нагадав, що Євросоюз пов'язав свою політику щодо РФ з Мінськими домовленостями, і запевнив, що санкції діятимуть до повного їх виконання Росією…». ***(Посол Маасікас сказав, чому ЄС вчиться в України // Укрінформ (https://www.ukrinform.ua/rubric-polytics/3243362-posol-maasikas-skazav-comu-es-vcitsa-v-ukraini.html). 11.05.2021).***

***

«Україна буде першою з-поміж країн Східного партнерства, з якою Європейський Союз планує розпочати тісний діалог у сфері кібербезпеки в межах програми EU4Digital.

Про це заявив керівник програм співробітництва Представництва ЄС в Україні Фредерік Куне у відеозверненні до учасників Всеукраїнського форуму «Україна 30. Безпека країни», повідомляє кореспондент Укрінформу.

Куне зазначив, що співпраця між Україною, ЄС і США стала вирішальним чинником у створенні безпечного кіберпростору в Україні.

«В межах Програми EU4Digital в Україні, яка, по суті, спрямована на транскордонний цифровий розвиток, ми пропонуємо проводити технічні навчання і налагоджувати взаємодію між відомствами, які займаються цифровізацією, та «Кіберцентром UA30». Перед наступним самітом (Східного партнерства – ред.) ми будемо запускати саме такий діалог у сфері кібербезпеки. Україна буде першою країною добросусідства, з якою буде встановлено такий діалог», - сказав Куне.

Він запевнив, що Європейський Союз і надалі тісно співпрацюватиме з Україною у сфері кібербезпеки. Ця співпраця включатиме, зокрема, підвищення потенціалу країни, а також спільні дії на міжнародних майданчиках і обмін відповідним досвідом…

Програма EU4Digital доповнює двосторонню підтримку ЄС для України в застосуванні рішень електронного управління для місцевих органів влади і в підвищенні функціональної сумісності адміністративних послуг, а також у підвищенні стійкості кіберпростору, особливо перед виборами». ***(Україна – перша серед країн Східного партнерства, з якою ЄС планує тісний кібердіалог // Укрінформ (https://www.ukrinform.ua/rubric-technology/3244661-ukraina-persa-sered-krain-shidnogo-partnerstva-z-akou-es-planue-tisnij-kiberdialog.html). 13.05.2021).***

***

«Почти 200 украинских и американских специалистов по кибербезопасности отработали защиту объектов критической инфраструктуры и обсудили аспекты соответствующего законопроекта.

…об этом сообщает пресс-служба СНБО.

«27 мая в рамках сотрудничества между Национальным координационным центром кибербезопасности при Совете национальной безопасности и обороны Украины (НКЦК) и Фондом гражданских исследований и развития Соединенных Штатов Америки (CRDF Global) (при поддержке Государственного департамента США) состоялось четвертое заседание Национального кластера по кибербезопасности, посвященное вопросам защиты критической инфраструктуры, ее устойчивости, а также проблемам, которые существуют в этой сфере, и путям их решения», - говорится в сообщении.

Как отмечается, заместитель секретаря СНБО Украины Сергей Демедюк подчеркнул, что этот проект является платформой, на которой ведущие специалисты «могут непосредственно обменяться мнениями, предложениями, интересными идеями». В частности, защита объектов критической инфраструктуры является крайне важной для обеспечения жизнедеятельности государства и каждого гражданина, а во время заседания кластера можно наработать пути непрерывного обеспечения «безопасности этих объектов - начиная от атомной энергетики и заканчивая маленькими финансовыми компаниями, которые могут быть отнесены к объектам критической инфраструктуры», подчеркнул он.

Представитель Посольства США в Украине Адам Марлоу отметил, что «США является надежным партнером Украины в сфере кибербезопасности». По

его словам, в прошлом году США оказали помощь Украине почти на 700 млн долларов и готовы дальше продолжать диалог и сотрудничество с Украиной, в частности, в вопросах защиты критической инфраструктуры, «что стало ключевым в сфере кибербезопасности».

По информации заместителя менеджера по программам кибербезопасности CRDF Global в Украине Михаила Верича, участие в работе четвертого кластера по кибербезопасности принимают 33 специалиста в режиме реального времени и 163 - онлайн, и это мероприятие является одним из самых многочисленных в рамках сотрудничества между CRDF Global и НКЦК.

Как отмечается, заместитель руководителя службы информационной безопасности и кибербезопасности Аппарата СНБО Украины Владимир Зверев подчеркнул, что принятая на заседании СНБО Украины 14 мая 2021 года Стратегия кибербезопасности Украины на период 2021-2025 годов предусматривает существенное усиление взаимодействия с частным сектором и развитие государственно-частного партнерства, и ключевую роль в этом занимает НКЦК.

«Украина введет сервисную модель государственного участия в мероприятиях по защите от киберугроз, при которой государство будет восприниматься не как источник требований, а как партнер в развитии национальной системы кибербезопасности», - сказал он, добавив, что эффективной моделью взаимоотношений в сфере кибербезопасности является «модель, построенная на доверии».

В свою очередь, руководитель службы по вопросам безопасности критической инфраструктуры Аппарата СНБО Украины Ирина Тимошенко подчеркнула важность рассмотрения и принятия законопроекта о защите критической инфраструктуры, зарегистрированного в парламенте. По ее словам, этот документ является стратегически важным.

Кроме того, Тимошенко представила проект концепции развития системы подготовки специалистов для защиты критической инфраструктуры. Целью концепции является создание системы подготовки, переподготовки и повышения квалификации специалистов по защите критической инфраструктуры, включая просветительскую деятельность, и информирование населения для удовлетворения потребностей страны в специалистах, улучшение уровня осведомленности всех слоев населения и его готовности противостоять вызовам в сфере безопасности.

Участники заседания обсудили организационные и правовые основы обеспечения безопасности и устойчивости критической инфраструктуры, международную помощь в становлении отечественной системы защиты критической инфраструктуры, особенности их классификации. Также были проанализированы законопроекты по защите критической инфраструктуры.

По информации пресс-службы, иностранные специалисты представили лучшие мировые практики подготовки специалистов в сфере защиты критической инфраструктуры. Эксперты CRDF Global презентовали онлайн-курс «Основы кибербезопасности для представителей государственных органов».

В СНБО сообщили, что в мероприятии участвовали представители основных субъектов обеспечения кибербезопасности Украины, народные депутаты, представители Посольства США, Европейской комиссии, ОБСЕ, компаний Next

Peak, Sovereign Ventures, CyberNB, представители международного академического сообщества…». ***(Украинские и американские специалисты обсудили устойчивость инфраструктуры к кибератакам // Укринформ (https://www.ukrinform.ru/rubric-society/3254379-ukrainskie-i-amerikanskie-specialisty-obsudili-ustojcivost-infrastruktury-k-kiberatakam.html). 28.05.2021).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Сингапур поручил Facebook и Twitter размещать уведомления об исправлениях в сообщениях, в которых утверждается, что существует местный штамм вируса COVID-19. Однако порядок распространяется только на пользователей платформ в стране.

Министерство здравоохранения заявило в четверг, что директива была также передана журналам SPH, в частности, его пользовательскому форуму HardwareZone. Это потребует от онлайн-платформ уведомлений об исправлениях для «всех конечных пользователей в Сингапуре», которые имеют доступ к Facebook, Twitter и HardwareZone.com, заявило министерство.

Он ссылался на распространяющиеся в Интернете ложные заявления о том, что новый вариант COVID-19 возник в Сингапуре и находится под угрозой распространения в Индии.

«Не существует нового «сингапурского» варианта COVID-19. Нет и доказательств того, что какой-либо вариант COVID-19 «чрезвычайно опасен для детей», - заявили в министерстве здравоохранения. «Штамм, который преобладает во многих случаях COVID-19, выявленных в Сингапуре в последние недели, - это вариант B.1.617.2, который происходит из Индии. Существование и распространения варианта B.1.617.2 в Индии возникло еще до обнаружения варианта в Сингапуре, и об этом стало известно и о нем сообщили различные СМИ уже с 5 мая 2021 года».

Приказ об уведомлении об исправлении был издан Управлением Закона о защите от лжи и манипулирования в Интернете (POFMA), которому было поручено следить за соблюдением Закона.

Этот шаг был сделан через несколько дней после того, как главный министр Индии в Дели Арвинд Кеджривал заявил в Twitter, что сингапурский вариант вируса особенно вреден для детей и может вызвать третью волну инфекций в Индии. Он также призвал свое правительство отменить рейсы из Сингапура.

В ответ министерство иностранных дел Сингапура заявило в среду, что «сожалеет о необоснованных утверждениях» и «разочаровано» тем, что видный политический деятель не смог установить факты перед тем, как сделать такие заявления. Министерство добавило, что оно встретилось с Верховной комиссией Индии, чтобы выразить свою озабоченность.

Со своей стороны, министр иностранных дел Индии Субраманьям Джайшанкар упрекнул Кеджривала, который является представителем крупнейшей

оппозиционной партии страны «Ам Аадми». Джайшанкар сказал в Twitter: «Безответственные комментарии тех, кто должен знать лучше, могут повредить давним партнерским отношениям. Итак, позвольте мне уточнить - СМ Дели не говорит от имени Индии».

Он добавил, что обе страны были партнерами в борьбе с COVID-19, и Индия «благодарна» за роль Сингапура в качестве логистического центра и поставщика медицинского кислорода, в котором Индия нуждалась во время второй волны.

В среду Индия сообщила о ежедневном рекордном количестве смертей от COVID-19 в 4529 человек, что превышает предыдущий мировой рекорд в США, где 12 января было зарегистрировано 4475 смертей.

В настоящее время в Сингапуре наблюдается вторая волна инфекций: в среду было зарегистрировано 34 случая в сообществе, а такие инфекции были обнаружены 24-й день подряд. Всего в городе-государстве от вируса умер 31 человек.

POFMA был принят в мае 2019 года после коротких публичных дебатов, а в октябре 2019 года был отклонен с подробностями о том, как можно подавать апелляции на директивы. Законопроект был принят на фоне резкой критики за то, что он дает правительству широкие полномочия в отношении онлайн-общения и будет использоваться для подавления свободы слова, а также для подавления политических оппонентов.

Несоблюдение директивы POFMA является нарушением закона. Правонарушителям грозит лишение свободы на срок до трех или пяти лет, штраф в размере 30 000 сингапурских долларов или 50 000 сингапурских долларов либо и то, и другое. Если боты или неаутентичные учетные записи используются для распространения лжи, потенциальные штрафы, которые могут быть применены, будут удвоены. Между тем, интернет-посредники-нарушители могут столкнуться с штрафом до 1 миллиона сингапурских долларов, а также могут получить ежедневный штраф в размере 100 000 сингапурских долларов за каждый день, когда они продолжают нарушать Закон после осуждения». ***(Eileen Yu. Singapore orders Facebook, Twitter to post correction notice on COVID variant falsehoods // ZDNet (https://www.zdnet.com/article/singapore-orders-facebook-twitter-to-post-correction-notice-on-covid-variant-falsehoods/). 20.05.2021).***

***

«Хотя часто бывает трудно достичь группового консенсуса, все могут согласиться с чувством облегчения от того, что мы, возможно, преодолеваем худшее из пандемии. Хотя немногие хотят оглянуться на самые мрачные времена, в эти месяцы есть непрерывные уроки, которые можно преподать по кибербезопасности. Нравится вам это или нет, но отголоски 2020 года по-прежнему будут отражаться в 2021 году как в физическом, так и в цифровом мире, и мы игнорируем этот факт к своей опасности.

Да, первый год пандемии прошел, но она любезно оставила позади многие из своих проблем кибермошенничества, которые, как показывают исследования угроз, сохранятся в обозримом будущем. Злоумышленники продолжат фокусироваться на максимизации своей прибыли, используя традиционный анализ затрат и выгод для

определения наилучшего вектора атаки. Удаленная работа будет продолжаться, поскольку компании будут принимать изменения на рабочем месте, вызванные COVID-19. С точки зрения киберпреступников эти тенденции только увеличивают рентабельность инвестиций в мошенничество и мошенничество. Помня об этом, организации должны сохранять бдительность, чтобы защитить себя и свои конфиденциальные данные от этих методов атак.

Пост-вакцинные атаки социальной инженерии не утихнут

Киберпреступники видят в атаках социальной инженерии эффективную, действенную и недорогую методологию. Как и в случае с законным бизнесом, киберпреступники хотят максимизировать прибыль при одновременном сокращении операционных расходов. А благодаря обилию криминального программного обеспечения «как услуга», доступного через Dark Web, атаки с использованием социальной инженерии идеально подходят для достижения этих целей.

Что делает атаки социальной инженерии настолько успешными, так это то, что они нацелены на эмоции людей, манипулируя реакцией «бей или беги». Когда людей охватывают такие чувства, как страх или сочувствие, они часто принимают необдуманные решения. Когда началась пандемия, киберпреступники использовали эти эмоции для успешных фишинговых атак. Типичными темами были увольнения и выдача себя за органы здравоохранения. Позже мы увидели больше попыток, направленных на вакцину.

Изначально люди отчаянно нуждались в информации, поэтому они отказались от своей цифровой защиты, что привело к увеличению прибыльности. По мере того, как страны начинают предлагать больше возможностей для вакцинации, те же эмоции будут продолжать делать мошенничество с помощью социальной инженерии прибыльным. С таким желанием вернуться к «нормальной» жизни люди хотят верить, что положительная информация, связанная с пандемией, реальна. Это желание делает атаки социальной инженерии на вакцины более прибыльными. Только когда эта информация станет более конкретной и общедоступной, злоумышленники увидят, что жизнеспособность этих мошенников снижается с точки зрения затрат и выгод.

По мере того, как мир начинает открываться, и мы ползем к более светлому будущему, люди будут искать, чем заняться и куда пойти, поэтому мы также ожидаем, что атаки социальной инженерии начнут использовать такие вещи, как путешествия и отпуск, чтобы зацепить люди.

Домашний офис продолжает оставаться главной целью

В прошлом году различие между домом и офисом значительно стерлось, а это означает, что нацеливание на дом приближает злоумышленников к корпоративной сети. Во второй половине 2020 года список возглавили эксплойты, нацеленные на устройства Интернета вещей (IoT). Каждое устройство IoT представляет собой новую «границу» сети, которую необходимо защищать и требовать мониторинга и обеспечения безопасности. Поскольку многие компании продолжают разрешать хотя бы некоторым из своих сотрудников работать удаленно без оговоренной даты окончания, лидеры безопасности должны быть в курсе последних угроз, касающихся пограничного доступа и браузеров.

Хорошая новость для киберпреступников и плохая новость для всех остальных заключается в том, что вредоносный код более гибкий и способен проникать дальше в поверхность атаки. Одна вредоносная кампания может иметь широкий охват на разных устройствах и платформах. Например, Adrozek - это семейство вредоносных программ, успешно использовавшееся во многих браузерах и приложениях, и обладающее большой инфраструктурой. Это семейство контролирует сотни тысяч доменов. Само вредоносное ПО выполняет инъекцию в браузер для получения вредоносных результатов поиска после заражения этого браузера. Как только вы загрузите вредоносное расширение DLL, игра, по сути, окончена. Люди не понимают, что на многих периферийных устройствах также есть браузеры.

Браузеры необходимы устройству для получения сообщений и обновлений, даже если вы не открываете приложение и не вводите адрес веб-сайта. Плохие участники используют встроенный код браузера устройства. Люди привыкли считать, что браузеры безопасны; в большинстве случаев они обновляются автоматически. Но во многих случаях браузеры - это, по сути, новое преимущество.

Атаки не обязательно должны искать уязвимости в браузере, а только в серверной части - как браузер доставляет рекламу, как он обрабатывает такие вещи, как поиск или любой другой процесс, который дает злоумышленникам возможность. Ботнеты позволяют злоумышленникам создавать сотни тысяч дронов, которые могут атаковать самые разные машины, включая системы Windows, Mac, Linux, периферийные устройства, устройства IoT и другие.

Как победить подрывные атаки

Атаки социальной инженерии и угрозы, связанные с пограничным доступом / браузерами / Интернетом вещей, вместе представляют собой основные способы, которыми кибератаки нацеливаются на отдельных лиц, как способ проникновения в более крупные организации.

Борьба с киберпреступностью требует комплексной стратегии и широкой осведомленности.

Аналитика угроз останется центральным элементом для понимания этих угроз и способов защиты от них. Видимость также имеет решающее значение, особенно когда большой процент пользователей находится за пределами стандартного периметра сети. Каждое устройство создает новую границу сети, которую группа безопасности должна защищать и контролировать. Использование искусственного интеллекта и автоматического обнаружения угроз может помочь организациям отреагировать на атаки немедленно, а не в какой-то более поздний момент, и они необходимы для смягчения атак на высокой скорости и масштабируемости на всех уровнях. Организации также должны уделять первоочередное внимание обучению осведомленности о кибербезопасности, потому что кибергигиена - это не только сфера деятельности ИТ-специалистов и групп безопасности. Эти передовые практики помогут вам извлечь уроки из кибер-уроков 2020 года и защитить отдельных сотрудников и организацию в целом». ***(Aamir Lakhani. Shifting Threats in a Changed World: Edge, IoT and Vaccine Fraud // Threatpost (https://threatpost.com/threats-edge-iot-vaccine-fraud/166029/). 11.05.2021).***

***

Світові тенденції в галузі кібербезпеки

«В 2013 году Google был успешно взломан. Не через свои онлайн-платформы, а через систему управления зданием (BMS). Хакеры, два исследователя ИТ-безопасности, доказали свою правоту. BMS, установленная в офисе Google Wharf 7 в Сиднее, Австралия, использовала более старое программное обеспечение, которое было уязвимо для кибератак. После входа в систему хакеры могут получить доступ к различным функциям управления, включая сигналы тревоги и переопределения. Если бы у них был злой умысел, результат мог бы оказаться разрушительным и дорогостоящим.

Когда мы говорим о киберугрозах, мы склонны думать о хакерах, крадущих данные или устанавливающих вредоносное ПО, которое отключает ИТ-системы. Дело в том, что физические здания, которые мы занимаем, сами по себе уязвимы для кибератак, потому что современная искусственная среда встроена в технологию, которая требует доступа к онлайн-платформам. Если эти платформы будут скомпрометированы, существует реальная вероятность серьезных сбоев.

Более того, физический ущерб зданиям не исключен. Системы отопления, охлаждения и управления питанием являются примерами функций, которые в случае атаки могут привести к физическому ущербу. Также нет ничего необычного в том, что ИТ-инфраструктура (оборудование) подвергается атаке и становится бесполезной («замораживание»). С конца 2000-х годов риск физического повреждения стал реальностью, и мы стали свидетелями серии громких хакерских инцидентов, попавших в заголовки международных газет.

Киберугрозы в заголовках

В 2010 году было обнаружено, что вредоносная программа под названием Stuxnet (которая, как многие полагают, была разработана правительствами США и Израиля) нацелена на иранский завод по обогащению урана и манипулирует компьютерными системами, вызывая систематические сбои на самом заводе - первая подтвержденная кибератака, которая вызвали физическое разрушение.

В 2014 году хакеры атаковали сталелитейный завод в Германии, используя целевую фишинговую атаку (целевые электронные письма, содержащие вредоносное ПО, которое, по всей видимости, пришло из надежного источника), чтобы проникнуть в корпоративную сеть. Системы мельницы были повреждены до такой степени, что доменная печь не могла быть остановлена должным образом, что привело к серьезным физическим повреждениям мельницы.

В 2017 году нефтеперерабатывающие заводы Саудовской Аравии подверглись атаке Triton, еще одной вредоносной программы, предназначенной для атаки на системы безопасности, что привело к остановке процессов нефтепереработки. Позже выяснилось, что плохо настроенный брандмауэр позволял хакерам получить доступ к компьютерам внутри организации, а оттуда и к оперативным технологиям.

Выявление уязвимостей

Промышленные здания особенно подвержены физическим нарушениям и ущербу в результате кибератак из-за их зависимости от промышленных систем управления, которые никогда не были предназначены для подключения к Интернету.

Компьютеризированные промышленные средства управления используются в течение некоторого времени, но устаревшие системы были разработаны для работы изолированно и часто используют устаревшее программное обеспечение. Подключение их к Интернету может повысить эффективность, но также подвергнет старые системы современным атакам. Серьезные кибератаки на промышленную и критическую инфраструктуру вызывают тревогу, но уязвимы и более повседневные цели, включая торговые центры, склады, офисы и отели.

Как и в офисе Google Wharf 7, в большинстве современных коммерческих зданий используется BMS для мониторинга и управления механическим и электрическим оборудованием и другими системами. Благодаря более доступным и широко распространенным беспроводным технологиям эти BMS становятся все более изощренными, но при недостаточной защите сопряжены с повышенным риском. Если хакерам удастся получить доступ к сети, они могут нанести физический ущерб и сбой, манипулируя механическим и электрическим оборудованием.

Например:

Манипулирование системами отопления, вентиляции и кондиционирования воздуха может сделать работу в здании в лучшем случае неудобной, а в худшем - опасной.

Энергопотребление здания может быть нарушено несанкционированным включением или выключением света.

Камеры видеонаблюдения или детекторы движения могут быть включены или выключены, а отснятый материал можно удалить, чтобы замаскировать преступную деятельность.

Системами контроля доступа можно манипулировать так, чтобы привилегии можно было отозвать или предоставить всему зданию (через считыватели карт или иным способом) или открыть двери в закрытые зоны.

Могут срабатывать системы контроля и пожаротушения, включая сигнализацию и спринклеры.

Управление доступом к лифту может быть подавлено или отменено.

Помимо физического повреждения и сбоев, личные данные и конфиденциальная информация также могут быть скомпрометированы из-за недостаточно защищенных устройств BMS, о чем мы подробнее поговорим в нашей следующей статье.

Ответственность за эти уязвимости может лежать на любом количестве заинтересованных сторон.

Поставщик BMS мог не создать безопасный продукт; возможно, застройщик не установил или не интегрировал BMS должным образом; конечный пользователь может иметь слабые методы безопасности (технические или физические). Общая идея заключается в том, что с большей интеграцией технологий в структуру наших

зданий возникает соответствующая потребность в обеспечении надлежащего обслуживания и замены технологий, которые стоят за ними.

Бум киберугроз привел к соответствующему буму услуг кибербезопасности. Большинство хорошо подготовленных корпораций инвестируют в них, и руководители зданий должны следить за тем, чтобы их системы и средства управления были в актуальном состоянии.

Страхование от кибератак

Хотя нет замены надежному профилю кибербезопасности (профилактика лучше лечения), страхование станет частью стратегии снижения рисков многих организаций. Рынок киберстрахования является относительно зрелым, поскольку уже более десяти лет он находится на переднем крае оценки подверженности киберрискам. Однако проблемы остаются, и физический ущерб, причиненный кибератаками, ни в коем случае не является стандартным риском.

Способность киберрисков попадать в промежутки между традиционными линиями страхового покрытия хорошо известна: убытки могут иметь элементы, которые могут вызывать претензии по нескольким различным типам полисов - например, повреждение материального имущества (ноутбуки с кирпичом), традиционные страхование зданий, прерывание хозяйственной деятельности, преступления (кража в результате мошенничества с перенаправлением платежей) и профессиональная халатность (претензии в связи с потерей данных).

Когда речь идет о физическом повреждении зданий, на которые распространяются традиционные полисы страхования зданий, существует вероятность того, что кибер-убытки могут составить «злонамеренный ущерб», который обычно включается в страховой риск. Это связано с тем, что по большей части сравнительно легко оценить злонамеренный мотив в киберсобытии - большинство нарушений, которые мы видим, являются злонамеренными, за исключением странных случаев халатности или ошибки. Чего нельзя сказать о «террористических угрозах», которые требуют политического, религиозного или идеологического мотива.

Ключевым полем битвы, учитывая возможные потери, является прерывание бизнеса. Физический ущерб зданию может быть незначительным, но все же может вызвать проблемы, которые нанесут вред бизнесу. Например, атака, которая приводит к сбоям в системах отопления, вентиляции и кондиционирования воздуха или в мониторе качества воздуха, может легко сделать здание временно непригодным для проживания. В зависимости от функции здания, это может вызвать немедленные и дорогостоящие проблемы - например, на заводе или на складе распределения.

Претензия в соответствии с политикой прерывания бизнеса может проследить основную причину проблемы до кибер-события и привести к связанным с этим проблемам с покрытием. Для страховщиков это проблема «молчаливой кибернетической защиты» - то есть степень, в которой киберсобытие может вызвать страхование неожиданным образом просто потому, что оно в целом попадает в пределы определенного триггера или определенного убытка и не было специально исключено. Это привело к громким спорам.

Страховой рынок начинает приспосабливаться к этим новым вызовам. С 1 января 2020 года андеррайтеры Ллойда, составляющие полисы страхования от повреждений имущества первой стороны, должны были прямо подтвердить или исключить страхование кибер-событий. Однако возмещение физического ущерба вряд ли является нормой в таких полисах (и это распространяется на любые последующие убытки от прерывания бизнеса).

В зависимости от характера ущерба и условий различных действующих страховых полисов, потенциальный пробел в покрытии, таким образом, сохраняется, и владельцы и арендаторы не должны предполагать, что физический ущерб или разрушение будут покрываться страховкой.

Кто платит?

В зависимости от того, передали ли они на аутсорсинг свои функции ИТ-безопасности, владельцы и арендаторы могут предъявить иск своему поставщику технологий в связи с кибератакой, если они смогут доказать, что халатность или нарушение контракта при предоставлении соответствующих услуг привело к убыткам.

Если здание подлежит профессиональной аренде, в договоре аренды будет указано, кто будет платить за страховую защиту и что произойдет, если здание будет повреждено в результате страхового риска. Было бы необычно, если бы в договоре аренды кибератака указывалась в качестве застрахованного риска, но (как объяснялось выше) ссылки на злонамеренный ущерб или терроризм вполне может быть достаточным для включения кибератаки в условия страхования в договоре аренды.

Эти положения будут определять, есть ли у арендодателя обязательство обеспечить покрытие и несет ли арендодатель или арендатор риск любого причиненного физического ущерба, но арендодатели и арендаторы, которые особенно обеспокоены киберрисками (возможно, потому, что природа здания делает это особенно уязвим для кибератак или арендатор сам является объектом повышенного риска) следует рассмотреть возможность включения в договор аренды конкретных положений. Индивидуальное страхование может быть решением, но страхование физического ущерба может быть платным.

Развивающийся риск

Недвижимость стала воплощением технологических достижений, а здания стали более отзывчивыми, экологичными и удобными для пользователей, чем когда-либо. Нельзя позволять киберугрозам сорвать эту эволюцию, но застройщики, владельцы и арендаторы должны осознавать физические риски, присущие технологии, и обеспечивать средства для предотвращения, борьбы и снижения рисков кибератак». ***(Seaton Gordon, Laura Oliver. When cyber threats get physical // Clyde & Co LLP (https://www.clydeco.com/en/insights/2021/05/when-cyber-threats-get-physical). 17.05.2021).***

***

«Для защиты от кибератак важно «демистифицировать» кибербезопасность и разбить ее на риски, которыми может управлять любая

организация, - говорит Кьяран Мартин, бывший директор Национального центра кибербезопасности Великобритании.

Выступая в четверг на конференции по компьютерной безопасности AusCERT в Австралии, Мартин, ныне профессор Оксфордского университета, сказал, что представление о том, что киберинциденты невозможно остановить, является ложным.

По его словам, в случае атаки вымогателя Colonial Pipeline в США возникает картина, в которой преступники находятся над их головами, добавив, что группа DarkSide и ее дочерние компании постоянно используют основные слабые места в корпоративной безопасности.

«Они зашли слишком далеко, потому что не осознавали, что взлом ИТ-системы трубопроводной компании может привести к тому, что компания - по какой-либо причине - остановит трубопровод», - сказал Мартин.

«Это история, которая повторяется снова и снова, что приводит к ряду событий, которые могут привести к большим проблемам», - сказал Мартин. Но к кибербезопасности следует подходить таким образом, чтобы не внушать страха ни в общественных, ни в корпоративных залах заседаний.

«Очень легко бояться кибербезопасности», - сказал Мартин. «Очень легко быть инфантилизированным киберрисками и шумихой вокруг кибербезопасности».

Риск-ориентированный подход

Colonial Pipeline прекратил свою деятельность в качестве меры предосторожности после того, как ее корпоративные системы, в том числе важнейшие биллинговые системы, были поражены программой-вымогателем. По трубопроводу поступает около 45% печного топлива, бензина и авиакеросина, используемых на Восточном побережье США. Пока трубопровод был закрыт, на бензоколонках в регионе закончилось топливо.

Мартин сказал, что инцидент демонстрирует, как структурные недостатки в способах реализации кибербезопасности могут привести к серьезным последствиям для общественности. Но этот инцидент также указывает на то, как кибербезопасность должна быть разбита на управляемые риски, добавил он.

В своем программном выступлении Мартин показал слайд, в котором перечислены ключевые шаги кибербезопасности, включая обеспечение актуальности программного обеспечения, обеспечение защиты данных партнерами и поставщиками и анализ методов аутентификации, используемых для доступа к системам.

По его словам, важным шагом является обеспечение того, чтобы организация знала, какие данные она хранит и кто, скорее всего, может попытаться нацелить их, чтобы можно было развернуть правильные меры безопасности. По его словам, например, большинство организаций не будут подвергаться нападениям со стороны национальных государств.

«Просто достаточно хорошо управляйте рисками», - сказал Мартин. «Вам не нужна защита национального государства».

Мартин сказал, что даже с программами-вымогателями это не так уж и плохо. Некоторые организации продемонстрировали замечательную устойчивость.

Возьмем, к примеру, польского разработчика видеоигр CD Projekt, который в феврале был атакован группой вымогателей.

Мартин говорит, что компания практиковала хорошее реагирование на инциденты после заражения и у нее были хорошие резервные копии. CD Projekt отказалась платить выкуп, а также опубликовала технические подробности атаки, которая помогла сообществу специалистов по безопасности, сказал Мартин аудитории.

По словам Мартина, никто не просит небольшие организации или университеты, например, противостоять самой опытной государственной хакерской группе в Китае. Он сказал, что гораздо важнее, чтобы они систематически повышали устойчивость. По словам Мартина, хорошим примером этого является работа, проделанная в США перед выборами 2020 года по снижению киберрисков.

«Так что понимайте вред, используйте подход, основанный на оценке рисков - реалистичный подход, и работайте с партнерами», - сказал Мартин. «Мы можем решить эту проблему». ***(Jeremy Kirk. How to 'Demystify' Cybersecurity // Information Security Media Group (https://www.inforisktoday.com/how-to-demystify-cybersecurity-a-16593). 14.05.2021).***

***

«Как показывает недавняя атака программ-вымогателей на Colonial Pipeline, хакеры заняты как никогда раньше - и все больше проникают в критически важные компоненты повседневной жизни.

В то время как нарушение работы крупнейшего в стране трубопровода для нефтепродуктов (и вызванные этой атакой волновые эффекты) застало многих врасплох, сотрудники правоохранительных органов, вероятно, были немного менее шокированы. По данным Федерального бюро расследований США, во втором квартале средний размер выплат жертвами программ-вымогателей подскочил на 31% по сравнению с тем же периодом 2020 года. Жалобы на кибербезопасность в ФБР во время пандемии в прошлом году увеличились более чем в три раза.

Правительственные чиновники годами изо всех сил старались не отставать - и они обращаются за помощью к корпорациям. Еще в 2019 году директор ФБР Кристофер Рэй заявил Совету по международным отношениям, что лучший способ борьбы со все более агрессивными хакерами - это партнерство с экспертами по компьютерной безопасности из частного сектора…

Ранее в этом году Рэй продолжал настаивать на сотрудничестве, заявив на Международной конференции по кибербезопасности Университета Фордхэма, что «есть поговорка, что лучше всего ремонтировать крышу, когда светит солнце. Здесь та же концепция. Мы хотим, чтобы люди начали налаживать эти отношения со своим местным полевым отделением ФБР до того, как они совершат серьезное вторжение».

Однако отчасти проблема заключается в нехватке профессионалов в области кибербезопасности из частного сектора. Исследование Cybersecurity Workforce Study 2020 (ISC) ² изучило глобальную нехватку талантов в этой области и показало, что компании могут использовать 3,1 миллиона дополнительных

сотрудников, что почти вдвое больше, чем существует сегодня. (Только в США необходимо еще 879 000 человек.) Более половины респондентов исследования - около 56% - заявили, что нехватка специалистов по кибербезопасности подвергает риску их организации.

«Проще говоря, нехватка кадров в области кибербезопасности - это разница между количеством квалифицированных специалистов, необходимых организациям для защиты своих критически важных активов, и фактическими возможностями, доступными для выполнения этой работы», - говорится в исследовании. «Это не оценка открытых вакансий, доступных для соискателей».

Хорошей новостью является то, что разрыв сократился с 4 миллионов до 3,1 миллиона в прошлом году. Плохая новость в том, что некоторые из этих пробелов играют важную роль. Например, в Colonial Pipeline, как сообщается, были вакантны две ключевые руководящие должности в сфере безопасности, когда она подверглась атаке с использованием программ-вымогателей.

Удивительно, но, несмотря на риски и недавние вторжения, такие как взлом SolarWinds, который скомпрометировал ряд правительственных агентств США и крупных корпораций, нет большого толчка для увеличения найма в сфере кибербезопасности. Около 48% респондентов исследования (ISC) ² заявили, что планируют увеличить штат сотрудников в этой области в течение следующих 12 месяцев, примерно столько же, сколько в предыдущие два года. (Любопытно, что 15% заявили, что планируют сократить штат сотрудников по кибербезопасности, что на 5% больше, чем два года назад.)

Однако, несмотря на эту нехватку, государственно-частное партнерство все еще имеет место. Программа обмена кибер-информацией и сотрудничества (CISCP) Министерства внутренней безопасности США (DHS) поощряет сотрудничество в области корпоративной безопасности посредством несекретного обмена информацией об угрозах и уязвимостях. Европол идет еще дальше, создав веб-сайт, который позволяет государственным чиновникам и частным компаниям обмениваться инструментами дешифрования программ-вымогателей, чтобы не платить хакерам…». ***(Chris Morris. Cybersecurity Has a Workforce Gap // Nasdaq, Inc (https://www.nasdaq.com/articles/cybersecurity-has-a-workforce-gap-2021-05-14). 14.05.2021).***

***

«Согласно ежегодному исследованию, опубликованному в среду компанией, занимающейся кибербезопасностью и соблюдением требований, двое из трех глобальных руководителей по информационной безопасности чувствуют себя не готовыми к кибератаке.

Отчет Proofpoint's Voice of the CISO от 2021 года, основанный на опросе более 1400 директоров по информационной безопасности в 14 странах, показал, что 66 процентов руководителей признали, что их организации не были готовы противостоять целевым кибератакам в этом году.

Кроме того, более половины руководителей информационной безопасности (53 процента) признали, что их больше беспокоят последствия кибератаки в этом году, чем в 2020 году.

«Кибератаки становятся все более яростными и становятся все более частыми с каждой минутой», - заявил Сарью Найяр, генеральный директор Gurucul, компании по разведке угроз в Эль-Сегундо, Калифорния.

«Такое ощущение, что мы движемся к точке, где ни одна компания не будет по-настоящему безопасной, и ничто не сможет остановить киберпреступников», - сказала она TechNewsWorld. «Так что нет, никто не подготовлен должным образом к будущим кибератакам - даже директора по информационной безопасности».

Опрос также показал, что почти три из пяти руководителей по информационной безопасности (58 процентов) считают человеческий фактор своей самой большой кибер-уязвимостью.

Несогласованное смягчение последствий

«Дело не в том, что директора по информационной безопасности не стараются изо всех сил подготовиться. Дело в том, что кибератаки очень сложно предотвратить в первую очередь; и большинство руководителей по информационной безопасности не направляют свои ресурсы против правильных угроз», - утверждает Роджер Граймс. - управляемый защитным евангелистом KnowBe4, провайдера тренингов по вопросам безопасности в Клируотере, штат Флорида.

В качестве примера Граймс объяснил, что подавляющее большинство успешных злонамеренных атак происходит от социальной инженерии и фишинга. Многие опросы считают фишинг ответственным за от 70 до 90 процентов всех успешных кибератак.

«Тем не менее, - сказал он TechNewsWorld, - большинство организаций выделяют на это менее пяти процентов своего бюджета на ИТ-безопасность».

«Это фундаментальное несовпадение мер по снижению рисков с основной причиной эксплойтов, из-за чего кибербезопасность становится такой неэффективной», - сказал он.

«Большинство руководителей по информационной безопасности рассматривают угрозы как пузыри в бокале шампанского и им не говорят, что один или два из этих пузырей намного больше, чем все остальные пузыри вместе взятые», - заметил он.

«Это приводит к тому, что к ряду угроз относятся более одинаково, чем следовало бы, и, к сожалению, самые большие угрозы остаются слабо устраненными», - добавил он.

Главные угрозы

Опрос также показал, что 64% руководителей по информационной безопасности рискуют подвергнуться существенной кибератаке в ближайшие 12 месяцев.

Атаки, с которыми, по словам руководителей информационной безопасности, ожидают в ближайшие месяцы, включают:

Компрометация деловой электронной почты (34 процента)

Взлом аккаунтов (33 процента)

Инсайдерские угрозы (31 процент)

Компромисс цепочки поставок (29 процентов)

Программы-вымогатели (27 процентов)

«Инсайдерские угрозы часто игнорируются в пользу инструментов для защиты от внешних угроз», - отмечает Мори Хабер, технический директор и директор по информационной безопасности в BeyondTrust, разработчике решений для управления привилегированными учетными записями и уязвимостей в Карлсбаде, Калифорния.

«Однако мы не можем недооценивать риск инсайдерской угрозы», - сказал он TechNewsWorld.

«Когда мы думаем об инсайдерских угрозах, мы часто представляем себе недовольных сотрудников, стремящихся отомстить своим бывшим работодателям», - пояснил он. «В действительности подавляющее большинство этих угроз чаще всего вызвано честными ошибками, такими как переход по вредоносным ссылкам или открытие фишинговых писем».

«В любом случае инсайдерские угрозы очень сложно обнаружить, и они представляют собой угрозу, с которой предприятиям сложно бороться», - добавил он.

Компромисс с учетными данными

Пиюш Пандей, генеральный директор Appsian Security, компании по обеспечению безопасности и соответствия ERP-данных из Далласа, согласился с тем, что угрозы, нацеленные на пользователей, должны быть главной проблемой для руководителей по информационной безопасности, особенно угрозы, направленные на компрометацию учетных данных.

«Прямо сейчас личность пользователя обычно идентифицируется по учетным данным, с которыми он входит в систему», - сказал он TechNewsWorld. «Учитывая, что фишинг и атаки методом грубой силы настолько распространены, организации должны обеспечить динамический и контекстно-зависимый доступ к конфиденциальным бизнес-данным, чтобы обеспечить эффективное соответствие привилегий уровню риска при доступе».

Инсайдерские угрозы также не ограничиваются людьми.

«Объем угроз, исходящих от облачной инфраструктуры, такой как Microsoft 365 и Google Workspace, означает, что злоумышленники используют доверенные системы - и, возможно, даже системы, которые организация использует сами, - чтобы атаковать их», - заметил Джек. Миллер, бывший директор по информационной безопасности и нынешний руководитель глобальных профессиональных услуг в Menlo Security, провайдере облачной безопасности в Маунтин-Вью, Калифорния.

«Мы не можем считать, что «моя»установка OneDrive безопасна, - сказал он TechNewsWorld. «Мы должны предполагать, что все является вредоносным, в том числе и наши собственные системы. Фишинг и кража учетных данных могут облегчить злоумышленникам внедрение своих угроз внутри организации».

Проблемы удаленной работы

Хотя в ходе опроса директора по информационным технологиям, похоже, преуменьшили значение программ-вымогателей как угрозы, они остаются опасными, особенно в мире с большим количеством удаленных сотрудников, чем когда-либо.

«Злоумышленники были заняты тем, что использовали более широкую поверхность атаки, потому что персонал теперь удален, - пояснил Брайан Эмбри, директор по маркетингу продуктов в Zentry Security, компании удаленного доступа с нулевым доверием в Милипитасе, Калифорния.

«Сотрудники используют незащищенный Wi-Fi, личные устройства и получают доступ к приложениям и ресурсам в гибридной ИТ-среде», - сказал он TechNewsWorld. «Все это открывает возможности для эксплуатации вредоносных программ».

«И 2020 год не помог директорам по информационным технологиям», - сказал он. «Учитывая быстрый переход персонала к удаленной работе, руководители по информационной безопасности добавляли лицензии к своим существующим сетям VPN как можно быстрее, чтобы поддерживать работу и продуктивность своих организаций. Однако виртуальные частные сети часто бывают громоздкими и сложными и обеспечивают более широкий доступ, чем необходимо».

Действительно, более половины опрошенных руководителей по информационной безопасности согласились с тем, что удаленная работа сделала их организации более уязвимыми для целевых кибератак, причем три из пяти сообщили, что за последние 12 месяцев они наблюдали рост числа целевых атак.

«В прошлом году командам по кибербезопасности по всему миру была поставлена задача буквально в мгновение ока усилить свою позицию по обеспечению безопасности в этом новом и меняющемся ландшафте», - говорится в заявлении Лючии Милики, глобального директора по информационной безопасности компании Proofpoint.

«Для этого потребовалось найти баланс между поддержкой удаленной работы и предотвращением прерывания бизнеса при одновременном обеспечении безопасности этих сред. Поскольку будущее работы становится все более гибким, эта проблема теперь распространяется на следующий год и далее», - пояснила она.

«Помимо защиты множества точек атаки и обучения пользователей долгосрочной удаленной и гибридной работе, директора по информационным технологиям должны внушать уверенность клиентам, внутренним заинтересованным сторонам и рынку в том, что такие настройки могут работать бесконечно», - добавила Милица». ***(John P. Mello Jr. Two-Thirds of CISOs Admit They're Not Ready to Face a Cyberattack // ECT News Network, Inc. (https://www.technewsworld.com/story/87127.html). 12.05.2021).***

***

«За последние несколько лет потребители и предприятия стали лучше осознавать важность надлежащей гигиены кибербезопасности и необходимость распознавать общие угрозы в Интернете.

Кибератаки, мошенники и разработчики вредоносного ПО ушли с тех времен, когда компьютерное заражение означало просто неотзывчивый компьютер, всплывающие рекламные окна и, в худшем случае, синий экран смерти.

Вместо этого потребители сталкиваются со сложным мошенничеством и убедительными попытками фишинга, предназначенными для загрузки скрытых

троянов на устройство жертвы с целью кражи данных, поддельных мобильных приложений, которые маскируются под приложения для торговли криптовалютой, но вместо этого позволяют операторам забирать ваши деньги и запускать, и шпионское ПО, которое будет отслеживать каждое ваше движение и действие без вашего ведома.

Кибератаки - это не просто потенциальный ущерб для машины; Вместо этого они могут быть сосредоточены на краже данных, слежке и саботаже.

По мере развития угроз защиты, необходимые для снижения риска успешной атаки, также должны были улучшаться.

Поставщики технологий постоянно работают над обновлением своего программного обеспечения и устранением уязвимостей, прежде чем они будут использованы в дикой природе, правительства и некоммерческие организации снимают телевизионную рекламу, чтобы предупредить нас о том, что искать в онлайн-мошенничестве, а теперь компании предлагают передовые решения для защиты всего. от потребительских устройств до корпоративных сетей.

Однако базовым уровнем защиты домашних систем является антивирусное программное обеспечение, и рекомендуется, чтобы оно было установлено не только на домашнем ПК, но теперь и на мобильном устройстве.

Антивирусное (AV) программное обеспечение - это программный пакет, предназначенный для обнаружения, изоляции и удаления вредоносного кода (также известного как вредоносное ПО) из компьютерной системы.

В активном состоянии антивирусное программное обеспечение будет отслеживать входящий и исходящий трафик устройства, а также сканировать файлы, приложения и другой контент.

Многие формы антивирусного программного обеспечения будут использовать базы данных вредоносных сигнатур, создаваемые поставщиками кибербезопасности с течением времени, для обнаружения подозрительного кода.

Сигнатуры вредоносных программ, связанные с современными угрозами, добавляются в базу данных и предоставляют антивирусные программы для проверки цифровых отпечатков пальцев. Однако базы данных на основе сигнатур необходимо постоянно обновлять, поскольку обнаруживаются новые штаммы вредоносных программ и разработчики вмешиваются в свои творения, чтобы избежать обнаружения (или по мере выпуска полиморфных штаммов вредоносных программ, которые со временем изменяют собственные сигнатуры кода).

Современное антивирусное программное обеспечение также часто использует методы эвристического анализа для выявления пока неизвестных, новых и измененных штаммов вредоносных программ в дикой природе.

Если файл сопоставлен или обнаружен как похожий на запись в базе данных, файл будет считаться вредоносным, и пользователи будут предупреждены о потенциальном заражении. Затем файлы могут быть помещены в карантин для дальнейшего изучения или полностью удалены.

Приложения, созданные с учетом определенного поведения, такие как незаконный взлом программного обеспечения, созданного с целью избежать требований лицензирования, также обычно помечаются таким же образом. Однако следует отметить, что AV-продукты иногда могут давать ложные срабатывания.

Термины «антивирус» и «защита от вредоносных программ» часто являются взаимозаменяемыми, хотя антивирусное программное обеспечение обычно в первую очередь направлено на предотвращение заражения вашего ПК или мобильного устройства, тогда как решения для защиты от вредоносных программ могут быть больше ориентированы на глубокое сканирование и удаление вредоносных программ. Обе категории, однако, предназначены для защиты компьютерных систем.

Программное обеспечение AV также может помешать вам открывать и запускать подозрительные файлы и может предупреждать вас, когда вы посещаете взломанные веб-сайты.

В целом, вы должны рассматривать антивирусное программное обеспечение как активный уровень защиты от вредоносных программ и других угроз, но антивирусное решение не должно быть единственным препятствием, которое у вас есть.

Популярное антивирусное программное обеспечение включает продукты, предлагаемые Kaspersky, ESET, Norton, McAfee, Malwarebytes, Bitdefender и Avast.

Потребители могут выбрать бесплатную или платную версию - последняя обычно включает дополнительные, премиальные функции - тогда как предприятиям обычно необходимо платить за подписку, покрывающую количество устройств, которые им необходимо защитить.

Бесплатные варианты могут быть только пробными или предлагать базовую антивирусную защиту без дополнительных функций или поддержки.

Нужна ли мне антивирусная программа?

Microsoft Defender - это антивирусный компонент современных операционных систем Windows, а macOS от Apple также включает встроенную антивирусную защиту.

Однако одних этих решений недостаточно для защиты от современных угроз. Кроме того, наши мобильные устройства теперь также подвергаются риску взлома операторами вредоносных программ, и большинство поставщиков AV-продуктов предлагают программное обеспечение для защиты не только вашего ПК, но и вашего телефона.

Что умеет антивирусное ПО?

Функциональность варьируется в зависимости от того, какое программное обеспечение вы решите использовать. Однако функции часто включают в себя:

Сканирование: пользователи могут выполнять сканирование своих устройств вручную или настроить расписание для автоматического запуска проверок системы. В качестве альтернативы, антивирусные продукты часто предлагают возможности фонового сканирования в реальном времени, которое проверяет новые файлы, архивы и действия браузера на наличие потенциальных угроз. Пользователи могут выбирать отдельные файлы, диски или целые системы, которые необходимо сканировать, а также выполнять быстрое сканирование, которое обычно занимает не более нескольких минут, для общих проверок «работоспособности».

Просмотр веб-страниц: можно включить мониторинг интернет-угроз в режиме реального времени для защиты пользователей от попыток фишинга,

вредоносных веб-сайтов, загрузки или выполнения подозрительных исполняемых файлов, непреднамеренных загрузок и т. Д.

Брандмауэры: современные операционные системы будут включать брандмауэр, который представляет собой систему мониторинга сети, которая блокирует входящий и исходящий трафик в соответствии с установленными правилами. Неавторизованные или подозрительные подключения могут быть остановлены, чтобы предотвратить вторжение.

Подключения к виртуальной частной сети (VPN): некоторые продукты AV теперь предлагают дополнительное встроенное подключение VPN. VPN не заменяет AV-продукт, а скорее следует рассматривать как полезное дополнение для сокрытия вашего IP-адреса, шифрования связи между вами и онлайн-сервисами и предотвращения как мониторинга, так и отслеживания третьими сторонами.

Менеджеры паролей: менеджеры паролей блокируют, управляют и генерируют пароли, используемые для доступа к онлайн-сервисам, а также могут автоматически заполнять формы от имени пользователя. Некоторые AV-продукты теперь даже включают диспетчер паролей.

Родительский контроль: они могут включать блокировку веб-сайтов для контента для взрослых и мониторинг ключевых слов.

Очистка от нежелательной почты, оптимизация системы: функции программного обеспечения Bolt-on AV могут включать очистку от мусора и ненужных файлов, тем самым освобождая место на вашем ПК или мобильном устройстве.

Защита платежей: продукты AV могут включать функцию отслеживания посещений подозреваемых поддельных веб-сайтов банковских или платежных систем и предупреждать вас, если вы собираетесь ввести свои данные на вредоносный веб-сайт. Кроме того, продукты AV могут предоставлять настраиваемое окно браузера, которое является изолированным и защищенным, обеспечивая более безопасную среду для совершения покупок в Интернете.

Автоматические обновления: программное обеспечение AV будет автоматически обновляться до новых версий, и эти обновления будут включать изменения в базы данных сигнатур.

Защита нескольких устройств: в зависимости от условий лицензии на программное обеспечение AV вы можете использовать одну и ту же подписку для защиты нескольких ПК или мобильных устройств. Обычно это платный вариант для пользователей.

Мониторинг Wi-Fi: AV-продукт также может отслеживать, к какой точке доступа Wi-Fi подключается ваше устройство, чтобы предупредить вас, если это небезопасно, например, открытая точка доступа в общественных местах или в отелях.

Как машины заражаются вредоносным ПО?

Мошеннические электронные письма, SMS-сообщения, поддельные веб-сайты и общие ресурсы, такие как накопители или файлы, могут использоваться как средства для развертывания вредоносного ПО.

Один из наиболее распространенных способов атаки - это фишинговые или спам-электронные письма, которые могут быть отправлены вашим банком,

налоговой инспекцией или известными брендами, такими как Amazon, PayPal или Facebook.

Мошенники часто используют тактику социальной инженерии, чтобы заманить жертв, чтобы они переходили по подозрительным ссылкам или попадались на эти поддельные электронные письма, пытаясь вызвать страх, панику или жадность. Например, они могут содержать:

Угрозы со стороны налоговой службы с требованием уплаты под угрозой уголовного преследования

Уведомления о доставке, отправленные из Amazon или PayPal, предупреждают о транзакции

Обещает, что вы выиграли приз, деньги в лотерее или бесплатную криптовалюту.

Угрозы, чтобы все ваши контакты знали, какие сайты для взрослых вы посещали

Схемы быстрого обогащения

В деловом мире атаки компрометации деловой электронной почты (BEC) часто адаптируются к отделам кадров, счетам-фактурам и запросам расценок.

Если цель попадает на фишинговое письмо, которое может быть отправлено во время кампании массового спама «спрей и молись» или с помощью специального целевого фишинга, его могут попросить щелкнуть ссылку на взломанный или вредоносный веб-сайт, содержащий полезная нагрузка или, альтернативно, электронное письмо может содержать вредоносное вложение, такое как документ Microsoft Word, в котором макросы извлекают вредоносное ПО.

К другим распространенным переносчикам инфекции относятся:

Вредоносная реклама через всплывающие окна в Интернете: в то время как поставщики технологий ограничивают старые методы развертывания вредоносного ПО - например, всплывающие окна, в которых утверждается, что ваш компьютер заражен вредоносным ПО, - вредоносная реклама, использование поддельной и вредоносной рекламы для распространения вредоносных программ по-прежнему распространено. Жертв могут попросить посетить веб-сайт и загрузить файл, например поддельный плагин для браузера или антивирусное решение, которое вместо этого запускает вредоносное ПО.

Вредоносные, взломанные веб-сайты. Вредоносная реклама, когда она обслуживается сторонними рекламными сетями, может превратить законный домен в плацдарм для распространения вредоносного ПО. Точно так же веб-сайты, которые были скомпрометированы - например, из-за внутренней уязвимости в системе управления контентом (CMS) - могут обслуживать посетителей вредоносных пакетов или могут перенаправлять их на другие домены, принадлежащие злоумышленникам.

Обновления вредоносного программного обеспечения: кибератаки постоянно совершенствуют свою тактику и методы заражения систем, и один относительно новый способ сделать это - выполнить атаку на цепочку поставок. Злоумышленники скомпрометируют центральный объект, например компанию, разрабатывающую популярное программное обеспечение, и вмешиваются в обновления программного обеспечения, которые автоматически отправляются

пользователям. SolarWinds инцидент является недавним примером того, насколько опустошения этого вида кибератаки может вызвать. Этот вектор атаки чаще используется для взлома корпоративных сетей.

Пакеты программного обеспечения. Некоторое программное обеспечение может поставляться в комплекте с вредоносным или нежелательным программным обеспечением, таким как рекламное или шпионское ПО.

Общие ресурсы: в дикой природе существуют варианты вредоносных программ, которые содержат червячные функции, позволяющие программам распространяться через общие ресурсы, включая отдельные файлы, внешнее хранилище и USB-накопители.

Распространенные онлайн-угрозы и вредоносные программы, на которые следует обращать внимание

Угрозы, которые могут попасть на ваш компьютер, обширны: от разрушительного вредоносного ПО до шпионского ПО, которое скрытно отслеживает ваши действия, рекламного ПО, которое постоянно обслуживает вас рекламой во время сеансов браузера, и потенциально нежелательных программ (ПНП), также известных как нежелательные или неприятные программы. ЩЕНКИ могут показывать рекламу, замедлять работу вашего компьютера или загружать дополнительное программное обеспечение без вашего явного согласия.

Вредоносное ПО - это общий термин для обозначения различных видов вредоносного ПО, как описано ниже:

Вирус: компьютерный вирус предназначен для захвата законного файла, его повреждения и самораспространения через устройства и электронную почту. Они могут украсть данные, повредить системы и поддерживать постоянство на зараженной машине, выполняясь каждый раз при запуске легитимного скомпрометированного приложения. Вирусы могут быть полиморфными и изменять свой код, чтобы избежать антивирусных программ.

Червь: многие варианты вредоносного ПО теперь содержат возможности «червя» как часть более широкого набора инструментов. Однако черви также могут быть автономными программами, которые распространяются через системные сети или по электронной почте в виде вредоносных вложений. Червь может распространяться после попадания в уязвимую систему, а также может быть разработан для кражи данных, повреждения файлов или снижения производительности ПК.

Троян: троян или троянский конь - это вариант вредоносного ПО, который часто маскируется под легитимную программу. После установки в системе жертвы трояны могут создавать бэкдор для постоянного доступа, осуществлять наблюдение, загружать и запускать дополнительные вредоносные программы и красть информацию. Многие трояны сегодня ориентированы на кражу финансовых данных.

Программы-вымогатели: программы- вымогатели стали одним из наиболее потенциально вредоносных типов вредоносных программ, которые попадают как в потребительские, так и в корпоративные системы. Этот вариант вредоносного ПО будет шифровать зараженную систему, предотвращать доступ пользователей к их файлам и службам, а также будет выдавать записку о выкупе, требуя оплаты в

криптовалюте в обмен на ключ дешифрования. Некоторые из худших вымогателей инцидентов, влияющих на бизнес на сегодняшний день являются глобальная WannaCry атака, вспышка в Ирландии службы здравоохранения, а также закрытие Colonial трубопровод операций на всей территории Соединенных Штатов.

Шпионское ПО: шпионское ПО, также известное в худших формах как сталкерское ПО, является неэтичным, нарушающим конфиденциальность программным обеспечением, которое шпионит за пользователями устройств, собирая данные, включая, помимо прочего, действия и журналы браузера, записи электронной почты, списки контактов, социальные сети. активность, изображения, видео и журналы VoIP. При установке на мобильное устройство также можно отслеживать данные GPS, местоположение и сообщения SMS / MMS.

Рекламное ПО. Допустимое рекламное ПО может быть установлено с согласия - например, в обмен на копию оплаченного иным образом программного обеспечения. Однако оскорбительные варианты рекламного ПО недобросовестно продвигают рекламу в систему пользователя, чтобы ее операторы получали деньги.

Руткиты: Руткиты могут быть внедрены в приложения, гипервизоры, прошивки или уровень ядра операционной системы. Эти наборы инструментов могут использоваться для сокрытия активности других вредоносных программ, работать с высокими привилегиями, и их часто бывает очень сложно обнаружить. Недавний пример использования руткита был описан Kaspersky в разделе Operation Tunnelsnake.

Ботнеты: вредоносное ПО на основе ботнетов предназначено для порабощения ПК, мобильных устройств и устройств Интернета вещей (IoT) в более широкой сети, которая может иметь дополнительную полезную нагрузку, развернутую в «подчиненных» системах, заставляя их становиться плательщиками в распределенном отказе сервисные (DDoS) атаки, рассылка спама и многое другое.

Гибрид: современные штаммы вредоносных программ не всегда можно четко классифицировать, и они могут включать в себя модули для различных целей, таких как функции программ-вымогателей, бэкдоры, функции шпионского ПО или возможность выполнять бесфайловые атаки.

Майнеры криптовалюты: хотя киберпреступники не являются вредоносными по своей сути, они могут развертывать программное обеспечение для майнинга криптовалюты, такое как XMRig, на уязвимых серверах и ПК, чтобы использовать украденные компьютерные ресурсы для тайного майнинга монет. Затем эти монеты отправляются в кошелек, контролируемый злоумышленником.

Каковы симптомы заражения вредоносным ПО?

Существует ряд изменений в типичном поведении вашего устройства, которые могут указывать на наличие вредоносного ПО. Это включает:

Низкая производительность: одним из первых индикаторов того, что на вашем компьютере что-то не так, являются изменения типичных уровней производительности, такие как высокая загрузка процессора, зависания, сбои и задержки во время сеансов браузера. Если скорость обработки или производительность внезапно меняются, это может быть признаком заражения вредоносным ПО. Когда дело доходит до вашего телефона, могут возникнуть аналогичные симптомы, такие как резкое сокращение срока службы батареи,

дополнительное тепловыделение, лаги и сбои. Однако нельзя полагаться только на использование ЦП или ресурсов как на признак того, что вы заражены. Некоторые вредоносные программы, в том числе штаммы майнеров криптовалюты, будут загружать конкурирующие вредоносные программы и управлять их использованием ресурсов, чтобы предотвратить проблемы с производительностью и, следовательно, потенциальное обнаружение.

Всплывающие окна и перенаправление браузера: если вы столкнулись с неожиданной рекламной бомбардировкой или перенаправлением браузера, это может быть признаком того, что вашими сеансами манипулируют.

Изменения ПК и устройства: если вы обнаружите, что внезапно появляются и запускаются программы, с которыми вы не знакомы, изменения на домашней странице браузера или поисковой системы, или изменения настроек, которые вы не делали, это также может быть индикатором заражения.

Потеря места для хранения: если ваши жесткие диски заполняются без какой-либо известной причины, это может означать, что вы были скомпрометированы. Этот симптом чаще встречается у рекламного и вредоносного ПО.

Сообщения о необычном общении: если друзья, коллеги или партнеры спрашивают вас об электронных письмах или сообщениях, которые вы якобы отправили, которые кажутся подозрительными, это может указывать на то, что-либо ваше устройство взломано, либо принадлежащая вам учетная запись была взломана.

Заблокированные экраны: типичным признаком программ-вымогателей, в частности, является невозможность доступа к вашей системе за пределами главного экрана, на котором будет загружена записка с требованием выкупа. В этих случаях вполне вероятно, что ваши файлы были зашифрованы и не могут быть восстановлены без дешифратора программы-вымогателя.

Существующие антивирусные решения: если существующее антивирусное программное обеспечение или брандмауэры были отключены без предупреждения, это распространенный индикатор заражения вредоносным ПО.

Нужна ли антивирусная защита мобильным устройствам?

Мобильные вредоносные программы далеко не так распространены, как штаммы для ПК, но к мобильным угрозам следует относиться не менее серьезно. Если доступ к вашему мобильному телефону разрешен, варианты мобильного вредоносного ПО могут вести наблюдение (например, в случае приложений-преследователей), загружать вредоносное и рекламное ПО, красть ваши личные данные, собирать учетные данные, используемые для доступа к услугам мобильного банкинга, или украсть ваш банк. учетной записи, автоматически звоня или отправляя сообщения на премиум-номера.

В репозиториях мобильных приложений, включая Apple App Store и Google Play, есть средства защиты, которые не позволяют разработчикам использовать их в качестве хостов для вредоносных приложений, но бывают случаи, когда-либо вредоносное ПО проскальзывает через сеть, либо безобидные приложения внезапно обновляются для распространения вредоносного ПО. Таким образом, мобильный антивирусный продукт может оказаться неоценимым средством предотвращения распространения инфекций.

Я должен платить?

Большинство антивирусных продуктов либо бесплатны, либо основаны на шестимесячной / годовой подписке после пробного периода, со скидками при условии предоплаты за полный срок.

Бесплатное антивирусное программное обеспечение, предлагаемое уважаемыми поставщиками, имеет все или большую часть основных основных функций, необходимых для адекватной защиты домашнего ПК или мобильного устройства. Однако, как и в случае с большинством видов бесплатного программного обеспечения, вам придется время от времени сталкиваться с всплывающими окнами с просьбой обновиться и заплатить.

Самые впечатляющие функции современных антивирусных продуктов хранятся за платным доступом, но бесплатные решения, предоставляемые поставщиками кибербезопасности, не предназначены для нанесения ущерба безопасности пользователей - в конце концов, какая-то форма антивируса лучше, чем ничего. Если есть некоторые функции, которые вам абсолютно необходимы (например, VPN, родительский контроль, покрытие нескольких устройств или защита платежей), тогда большинство решений AV доступны по цене, и вам следует подумать о регистрации.

Компаниям, независимо от того, насколько они малы, следует серьезно рассматривать дополнительные функции, обычно предоставляемые платным программным обеспечением AV премиум-класса, как вложение, а не роскошь.

Что мне следует искать в антивирусном продукте?

Сначала вы должны подумать, какой тип антивирусного продукта подходит вам. Сканеры в реальном времени - одна из самых полезных функций AV-продукта, и вам, безусловно, следует выбрать тот, который предлагает эту форму защиты. Однако адекватная безопасность не может быть основана только на сканировании и базах данных сигнатур вредоносных программ - они должны постоянно обновляться, чтобы оставаться эффективными и актуальными, учитывая, что новые штаммы вредоносных программ обнаруживаются ежедневно.

Также следует учитывать удобство использования и возможное влияние на производительность ПК или мобильных устройств. Например, если вы используете более старую машину, легкий AV-продукт может быть более подходящим, чем надежное программное обеспечение бизнес-уровня.

Если вы хотите подписаться на премиум-вариант, также важно решить, для скольких устройств вам нужна защита, будь то только один компьютер или мобильное устройство, или нужен ли вам семейный тарифный план. Вы также можете рассмотреть отзывы поставщиков, когда речь идет не только о защите, но и о поддержке клиентов.

Антивирусные продукты, предлагающие родительский контроль, должны быть одними из лучших вариантов для родителей, которые хотят управлять контентом, который их детям разрешено просматривать в Интернете.

Что еще я могу сделать, чтобы защитить свой компьютер и мобильное устройство?

Ни один антивирусный продукт не является универсальным решением для обеспечения безопасности, поэтому их следует рассматривать как важный аспект

защиты ваших устройств наряду с общей осведомленностью, осторожностью и в сочетании с другими решениями безопасности.

Будьте осторожны: если электронное письмо выглядит подозрительно, доверяйте своей интуиции. Если вы получили сообщение от надежного источника, содержащего ссылку, например, посетите домен организации напрямую, а не переходите по нему.

Загрузки веб-сайтов: загрузка файлов с сомнительных веб-сайтов, таких как крэк, варез или пиратские домены, обычно вызывает проблемы.

Сторонние приложения: обычно рекомендуется загружать приложения только из источников, в которых есть собственные механизмы безопасности, таких как Google Play или Apple App Store.

Брандмауэры: вы должны постоянно держать программное обеспечение брандмауэра вашей операционной системы включенным.

Wi-Fi: следует избегать общедоступных незащищенных точек доступа Wi-Fi, поскольку они могут быть приманками или позволять злоумышленникам отслеживать вашу активность и потенциально перенаправлять вас на вредоносные веб-сайты. Вместо этого придерживайтесь безопасных мест или мобильной связи.

Резервное копирование: вы должны регулярно делать резервные копии ценного контента на своих устройствах. Хотя это не защитит вашу систему, эта практика может помочь вам восстановиться в худшем случае». ***(Charlie Osborne. Antivirus software, explained // ZDNet (https://www.zdnet.com/article/antivirus-software-explained/). 18.05.2021).***

***

«Исследование показало, что пандемия и растущие потребности в ИТ оказывают серьезное негативное влияние на психическое здоровье руководителей информационной безопасности.

Директора по информационной безопасности не в порядке.

Новое исследование показало, что пандемия усилила давление со стороны сотрудников на должности до уровня «экстремального стресса» среди руководителей информационной безопасности (CISO) и заставила их бороться за механизмы преодоления, начиная от тренировок и заканчивая наркотиками.

OneLogin опубликовал результаты своего опроса 250 технологических лидеров по всему миру, который показал, что 77 процентов респондентов считают, что пандемия усилила их рабочий стресс, а 67 процентов заявили, что они работали больше часов.

Поскольку пандемический приказ о том, чтобы оставаться дома, вступил в силу весной 2020 года, ИТ-отделам было оставлено решать, как команды могут работать удаленно и обеспечивать безопасность. В то же время резко возросло количество атак - программы- вымогатели, изощренный целевой фишинг, грубая сила и распределенный отказ в обслуживании (DDoS) - вот лишь некоторые из тактик, которые широко применялись киберпреступниками для извлечения выгоды из COVID-19 и его последствий.

Опрос не лишен дополнительных доказательств. Verizon только что опубликовал свой отчет об утечке данных за 2021 год, в котором оператор признал

подорванный моральный дух, пронизывающий круги ИТ-безопасности, и описал прошедший год как «непредсказуемую антиутопическую пустошь». Он также похвалил сообщество кибербезопасности за то, что оно «по-прежнему имеет достаточно интереса и энергии, чтобы заботиться о том, чтобы сделать мир более безопасным».

Но все это сказывается на психическом здоровье руководителей по информационной безопасности на передовой.

Как директора по информационной безопасности справляются со стрессом

Подавляющее большинство респондентов по информационной безопасности (80 процентов) сказали OneLogin, что они используют упражнения, чтобы справиться с давлением, 40 процентов сказали, что медитация была большим подспорьем, а 24 процента сказали, что занимаются самолечением с помощью наркотиков, алкоголя, наркотиков или рецептурных лекарств.

Директора по информационной безопасности в большинстве своем считают, что работодатели заботятся об их благополучии. Фактически, 75% заявили, что чувствуют, что их организации ценят их. Но задача, стоящая перед ИТ-командами, становится все более сложной.

В то время как CISO сталкиваются с определенным набором проблем, связанных с COVID-19, доктор Робин Мэсси, цитируемый в отчете, предупредил, что существует сложный набор факторов, которые влияют на уровень стресса человека.

«Хотя результаты опроса дают представление о некоторых видах поведения для снижения стресса с высоты 30 000 футов, важно отметить, что биология и окружающая среда также играют значительную роль в поведении», - сказал Мэсси. «Исторически сложилось так, что бизнес был озабочен эффективностью, жертвуя человеческими отношениями. На каком-то уровне эта точка зрения могла работать в прошлом, но времена изменились. Мы знаем, что текущее состояние тела влияет на поведение, чувства и мышление. Поэтому важно понимать, как физиологические факторы взаимосвязаны с реляционными и психологическими».

Мэсси предложила несколько советов по управлению стрессом, в том числе научиться распознавать физические признаки стресса, делать перерывы и получать качественный сон, которые, по ее словам, имеют решающее значение для психического здоровья, а также для здоровья организации.

«Лидеры не могут дать то, чего у них нет», - добавил Мэсси. «Чтобы заботиться о своих командах, они сами должны соблюдать принципы». ***(Becky Bracken. CISOs Struggle to Cope with Mounting Job Stress // Threatpost (https://threatpost.com/cisos-struggle-job-stress/166221/). 17.05.2021).***

***

«Если вы искали работу в сфере ИТ в 2020 или 2021 году, вы, вероятно, не могли бы выбрать более востребованную ИТ-специальность, чем кибербезопасность. Между защитой устройств множества новых сотрудников, работающих на дому, и реагированием на новые угрозы на горизонте, такие как взлом SolarWinds, организации вкладывали средства в найм большего количества специалистов по безопасности в то время, когда многие другие работники на рынке

труда боялись быть уволен. В течение нескольких недель после атаки программы-вымогателя Colonial Pipeline нет никаких признаков того, что это изменится.

Это один из результатов нового опроса 300 руководителей служб безопасности США. В ходе опроса также рассматривались инвестиционные приоритеты руководителей в области безопасности, насколько тесно эти руководители работали со своими руководителями, их планы в отношении технологий автоматизации безопасности и другие тенденции. Это пятый ежегодный опрос, проведенный по заказу Scale Venture Partners и проводимый Market Cube.

Полные 40% респондентов в опросе этого года заявили, что они увеличили численность сотрудников службы безопасности в 2020 году. Из тех, кто увеличил численность персонала, 32% заявили, что она увеличилась на 50% и более. Более того, 63% заявили, что их бюджет безопасности увеличился за последние 12 месяцев. Из тех, кто увеличил свой бюджет, 45% заявили, что он увеличился вдвое. (Для сравнения, 31% респондентов работали в компаниях с численностью персонала от 500 до 999 человек; 28% - в компаниях с численностью персонала от 1000 до 2499 человек и 18% - в компаниях с численностью персонала от 2500 до 5999 человек).

По словам Ариэля Цейтлина, партнера Scale Venture Partners, специализирующегося на облачных технологиях и безопасности, подбор персонала по-прежнему является проблемой в сфере кибербезопасности. Спрос на специалистов по безопасности увеличился за последний год во время пандемии на фоне новых и серьезных инцидентов в сфере безопасности.

«Я не уверен, что мы можем многое сделать для увеличения количества специалистов по безопасности», - сказал он. Вместо этого он считает, что рынок обратится к двум другим возможным решениям для устранения дисбаланса между спросом и предложением на таланты - средства автоматизации безопасности или продукты безопасности, объединенные с услугами.

Этот более высокий спрос был вызван новыми угрозами и изменившейся средой, в которой произошел огромный поворот в перемещении рабочей силы на работу из дома. 36% опрошенных руководителей службы безопасности связали рост числа инцидентов с переездом на работу из дома. Полные 52% руководителей службы безопасности заявили, что количество инцидентов безопасности, связанных с атаками на скомпрометированные данные, устройства, системы или сети, увеличилось.

Но одним из самых больших инцидентов, о которых думал каждый руководитель службы безопасности, был взлом SolarWinds.

«SolarWinds выдвинула на первый план внимание к рискам третьих сторон и рискам поставщиков», - сказал Цейтлин. «Все понимали, что у них не очень хорошая видимость».

Исследование Scale показало, что руководители служб безопасности переоснащают свои операции по обеспечению безопасности в ответ на меняющуюся среду угроз. Например, 57% заявили, что они усилили интеграцию с другими командами, такими как ИТ и разработка программного обеспечения. Кроме того, 36% заявили, что ожидают роста рисков третьих лиц в течение

следующих 12 месяцев. Более того, 47% заявили, что риски третьих лиц являются главным фактором, влияющим на понимание высшего руководства о влиянии безопасности на бизнес, за утечками данных (57%) и удаленной работой (54%).

Что делают эти организации для снижения рисков третьих лиц? Проведение аудита процедур сторонних поставщиков возглавило список с 51%. Другие меры включали использование сторонних услуг по оценке рисков (48%) и просьбу к поставщикам заполнять анкеты для самооценки (47%).

Цейтлин сказал, что опрос показал, что организации создают технологии автоматизации безопасности, чтобы помочь справиться с растущим разрастанием инструментов. Например, 51% респондентов заявили, что они создали собственное решение для кибербезопасности за последние 12 месяцев, а 23% заявили, что они создали технологию автоматизации безопасности.

«Существует так много разных инструментов, - сказал Цейтлин. «Организации стремятся инвестировать в программное обеспечение, которое объединяет и объединяет все различные сигналы от инструментов безопасности». ***(Jessica Davis. How SolarWinds Changed Cybersecurity Leadership's Priorities // Informa PLC (https://www.informationweek.com/strategic-cio/security-and-risk-strategy/how-solarwinds-changed-cybersecurity-leaderships-priorities/d/d-id/1341120). 26.05.2021).***

***

«Принимая во внимание недавние объявления о крупных атаках, вызванных внешними злоумышленниками, включая атаку программ-вымогателей на бензиновый трубопровод в США, необходимость повышения уровня безопасности как никогда важна, а многоуровневая безопасность остается ключевым фактором.

В заголовках газет доминируют безудержные атаки программ-вымогателей и другие инциденты, связанные с кибербезопасностью, организации и правительства уделяют больше внимания, и многие готовы тратить деньги, необходимые для решения некоторых проблем, которые позволяют этим злоумышленникам успешно проникнуть в компьютерную систему и взломать или сеть. На этой неделе президент Джо Байден подписал указ, который включает инициативы, направленные на повышение кибербезопасности страны; По другую сторону Атлантики недавний отчет Национального центра кибербезопасности Великобритании показывает, как Великобритания наращивает меры по защите кибербезопасности.

Между тем, согласно недавно опубликованным отчету Cisco «Будущее безопасной удаленной работы», в котором приняли участие более 3000 руководителей ИТ-служб по всему миру в 30 отраслях, 85% респондентов заявили, что кибербезопасность стала чрезвычайно важной с начала пандемии. Это в значительной степени связано с тем, что организациям пришлось быстро перейти к модели работы большинства из дома, что означало изменение политик и подходов к безопасности в соответствии с новой нормой.

Многоуровневая безопасность не устарела

Об этом говорили снова и снова, но это стоит повторить. Многоуровневый подход к безопасности - лучший способ снизить вероятность успешного взлома или нарушения безопасности. И хотя некоторые уровни безопасности могут показаться тривиальными или очевидными, все они одинаково важны.

Это похоже на систему очистки воды. Подобно тому, как первый уровень очистки воды включает удаление крупных и очевидных частиц, первым уровнем кибербезопасности может быть просто сетевой брандмауэр, блокирующий явно вредоносный трафик. Было бы нелепо пробовать обратный осмос в неочищенных сточных водах без предварительной очистки явно токсичных материалов.

С каждым уровнем, который вы добавляете в свою сеть, вы, вероятно, устраняете все больше и больше загрязняющих веществ, т. Е. Злонамеренных действий. Таким образом, добавление брандмауэров, систем предотвращения и обнаружения вторжений и антивируса для борьбы с вредоносными программами - всегда хороший способ снизить вероятность проникновения.

Но иногда вам нужен дополнительный анализ этих данных. Как и в случае с водой, без надлежащего анализа невозможно узнать, плохо ли она.

Как правильно анализировать сетевой трафик

Попытка проанализировать сетевой трафик в реальном времени может быть столь же сложной, как попытка проверить всю текущую воду, выходящую из пожарного шланга. Вы можете сделать это с непомерно большими деньгами, но это не масштабируемо. Что еще более усложняет ситуацию, так это то, что злоумышленники почти всегда применяют методы, чтобы оставаться незамеченными, в том числе используют методы низкой и медленной передачи данных, чтобы ускользнуть из поля зрения.

Для борьбы с этими методами необходимо собирать и анализировать сетевые данные в течение длительного периода времени, чтобы определить, откуда исходит вредоносный трафик. В частности, машинное обучение с помощью систем обнаружения и реагирования на сеть (NDR) почти всегда следует развертывать, чтобы помочь сетям и группам безопасности выявлять вредоносный трафик.

Безопасность для гибридных рабочих моделей

Многие организации разрешают вакцинированным работникам вернуться в офис и позволяют сотрудникам решать, когда или возвращаться, переход к гибридной модели безопасности почти наверняка станет постоянным. Это увеличивает потребность в отчете о недоставке, поскольку потребности организации в безопасности меняются по мере того, как сотрудники меняют место работы. Организациям будет сложнее создавать общие правила для сетевых подключений, когда сотрудники постоянно меняют IP-адреса или местоположение.

Хотя некоторые организации заставляют сотрудников подключаться к корпоративной VPN, это не всегда практично, особенно когда пропускная способность домашней сети ограничена. Вместо этого изучение того, как трафик течет по сети с течением времени, позволяет службам безопасности правильно обнаруживать аномалии.

В то время как сотрудники могут перемещаться, типы подключений и данных, которые они потребляют, вероятно, будут меняться так же часто. Использование систем с поддержкой NDR дает организациям понимание,

необходимое для определения того, когда члены их отдела продаж начинают загружать контент через SSH-соединение или когда HR начинает устанавливать исходящие соединения через FTP. Это особенно верно, когда не все пользователи постоянно подключены к сети. Как только это соединение возобновится, наличие исторических данных имеет решающее значение для выявления потенциально зараженных устройств.

Люди: самое слабое звено безопасности

К сожалению, самым слабым звеном являются люди, поэтому способность определять базовые параметры поведения и определять отклонения в схемах трафика - лучший способ обнаружения вредоносных действий. Но, задействуя многоуровневый подход с долгосрочным базовым анализом сетевого трафика, организации могут гарантировать высочайший уровень безопасности, даже когда сотрудники постоянно меняются местами работы.

Использование такого многоуровневого подхода - действительно единственный способ защититься от атак. Хотя не все атаки можно остановить, наносимый ими урон можно значительно уменьшить». ***(Justin Jett. Building Multilayered Security for Modern Threats // Threatpost (https://threatpost.com/multilayered-security-modern-threats/166457/). 28.05.2021).***

***

Сполучені Штати Америки

«Нещодавно наглядова рада Facebook постановила, що компанія виправдано заблокувала акаунт екс-президента США Дональда Трампа. Але дискусія про те, чи було це правильним рішенням, затьмарила іншу, більш актуальну проблему: чи повинна приватна компанія вирішувати, коли відкрите висловлення думок у соцмережах загрожує громадському порядку, пише Financial Times.

Технологічна революція вже почалася, але влада досі не вирішила питання про те, хто повинен керувати використанням цифрових технологій. Законодавці демократичних країн, зокрема США, наразі фактично дозволяють компаніям занадто легко встановлювати власні правила.

Зокрема, Facebook самостійно встановив багато норм збору та обробки даних.

І майже всі комерційні сайти використовують файли cookie - невеликі шматочки даних, для ідентифікації користувачів. Вони «рухаються разом із людьми» в Інтернеті, коли ті переглядають продовольчі товари, шукають одяг або ліки, що дозволяє компаніям точніше «націлювати» рекламу на людей.

Компанія Apple вирішила дозволити користувачам відмовитися від такого «широкого стеження». Це важливий крок до обмеження обміну даними. Але водночас, це показує, що приватні технологічні компанії мають вплив там, де регуляторні органи не змогли прийняти та застосувати власні правила.

Для прикладу, можна поглянути на «ринок шпигунських програм». Використання шпигунського програмного забезпечення для слідкування за користувачами, які навіть про це не підозрюють, зовсім не відповідає

демократичним стандартам, таким як захист свободи слова та прав людини, але саме ця сфера залишається фактично нерегульованою у багатьох країнах. Подібні технології часто сприймаються як засоби боротьби з тероризмом та іншими загрозами, але дуже часто вони використовуються у протилежних цілях.

Яскравим прикладом є історія з WhatsApp. WhatsApp та її материнська компанія Facebook подали скаргу до федерального суду США, стверджуючи, що ізраїльська компанія мобільного спостереження NSO Group використала «лазівку» у програмі обміну повідомленнями для надсилання шкідливого програмного забезпечення, спрямованого на вилучення даних близько 1400 мобільних пристроїв. Частина цих мобільних телефонів належала правозахисникам, дисидентам, дипломатам та чиновникам.

Результат, ймовірно, створить прецедент щодо того, які обмеження повинні застосовуватись до використання таких технологій та засобів спостереження. Але водночас конституційні права на приватність та безпеку руйнуються, коли технологічні компанії, зокрема і через силу закону, встановлюють власні стандарти. У сфері інноваційних технологій уряди часто відстають у питанні регулювання.

Системи розпізнавання обличчя - ще одна технологія, яка може створювати багато проблем. Для прикладу, такі системи заборонені для використання у декількох штатах США, але продовжують розповсюджуватися.

Компанія Clearview AI, що базується в Нью-Йорку, зберігає зображення «мільярдів облич», «вилучених» у Facebook, YouTube та інших веб-сайтів, у великій базі даних. Як повідомляється, компанія продає послуги миттєвої ідентифікації тренажерним залам, казино та правоохоронним органам.

Саме тому з’явилася загроза «функціональності влади» у питанні цифрового регулювання. Демократичні уряди, часто використовують свої засоби захисту кібербезпеки через такі компанії програмного забезпечення, як SolarWinds та Microsoft.

Але навіть потужне програмне забезпечення не гарантує повного захисту, як вже показала минулого року масштабна хакерська атака на SolarWinds. А нещодавня кібератака на Colonial Pipeline ще раз підкреслила відсутність стійкості в американській інфраструктурі.

Регулятивні органи можуть отримати перевагу в цій сфері. Загальний регламент ЄС про захист даних, який обмежує можливості технологічних компаній збирати та зберігати дані, надає більше прав користувачам. Microsoft прийняла Загальний регламент ЄС про захист даних як глобальний стандарт, а багато інших країн продовжили розробляти подібні закони.

Світ може вчитися на цьому успіху. Технологічні компанії не повинні мати повноважень визначати параметри доступу до інформації, безпеку чи ступінь захисту конфіденційності для сотень мільйонів людей. Уряди повинні не просто реагувати на інциденти, а розробляти правила, які ставлять права користувачів та безпеку даних на перше місце, резюмує видання.

Додатки для обміну повідомленнями можуть збирати інформацію про місцезнаходження і фінансові операції користувачів.

Портал Phonearena склав рейтинг месенджерів, грунтуючись на тому, які дані користувача ті збирають». ***(Правам людей потрібен сильніший захист у цифровому світі — FT // Дзеркало тижня. Україна (https://zn.ua/ukr/WORLD/pravam-ljudej-potriben-silnishij-zakhist-u-tsifrovomu-sviti-ft.html). 18.05.2021).***

***

«…администрация Байдена подробно рассказала, как она хочет профинансировать усилия по противодействию волне массовых взломов после атаки вымогателей Colonial Pipeline в этом месяце.

В заявлении, сделанном во вторник, Белый дом подробно описал кибер-элемент уже предложенного президентом Джо Байдена американского плана занятости, в том числе 20 миллиардов долларов для населенных пунктов для укрепления энергетических систем и 2 миллиарда долларов в виде грантов для энергосетей в зонах повышенного риска.

Запланированный Байденом план инвестиций в широкополосную связь в размере 100 миллиардов долларов также представлен как расходы на кибербезопасность на том основании, что получателям грантов будет предложено использовать их у «надежных поставщиков».

Безопасность энергосистемы США уже давно вызывает беспокойство экспертов по кибербезопасности. Отключение электроэнергии в регионах в 2003 и 2011 годах привлекло внимание к уязвимости энергосистемы, а примеры из-за рубежа также вызвали озабоченность.

В прошлом году Министерство юстиции США обвинило сотрудников российской разведки в наглых атаках на украинскую энергосистему, в результате которых миллионы людей на короткое время остались без электричества.

Объем финансирования, вероятно, станет ключевым вопросом, поскольку Байден стремится заручиться поддержкой обеих партий для своего плана инфраструктуры стоимостью 2,3 триллиона долларов, а республиканцы Сената, как ожидается, представят свое последнее контрпредложение позже во вторник.

Их первоначальная контрмера в целом требовала доли предлагаемых Байденом расходов, добиваясь в общей сложности 568 миллиардов долларов, сосредоточенных исключительно на традиционной инфраструктуре и доступе в Интернет.

Представление плана Байдена как минимум частично направленного на повышение кибербезопасности - редкая область двустороннего сотрудничества - может быть направлено на то, чтобы помочь преодолеть разрыв между предложениями, особенно после атаки на Colonial Pipeline Co, которая перекрыла критически важный топливопровод. и спровоцировали панические покупки в некоторых частях Восточного побережья…» ***(Biden administration eyes cybersecurity funding after hacks // Surperformance (https://www.marketscreener.com/news/latest/Biden-administration-eyes-cybersecurity-funding-after-hacks--33290221/). 18.05.2021).***

***

«12 мая администрация Байдена издала «Указ о повышении кибербезопасности страны». Документ направлен на усиление способности федерального правительства реагировать на угрозы кибербезопасности и предотвращать их, в том числе путем модернизации федеральных сетей, повышения безопасности цепочки поставок программного обеспечения федерального правительства, внедрения улучшенных практик и процедур кибербезопасности в федеральном правительстве и создания общегосударственных планов для реагирование на инциденты. Указ охватывает широкий круг вопросов и процессов, устанавливая многочисленные крайние сроки для рекомендаций и действий со стороны федеральных агентств и уделяя особое внимание усилению защиты федеральных сетей в партнерстве с поставщиками услуг, на которых полагаются федеральные агентства. Субъекты частного сектора, включая федеральных подрядчиков и поставщиков услуг, будут иметь возможность внести свой вклад в некоторые из этих действий.

В частности, среди прочего, Указ:

стремится устранить препятствия для обмена информацией об угрозах между частным сектором и федеральными агентствами;

требует, чтобы программное обеспечение, приобретаемое федеральным правительством, соответствовало новым стандартам кибербезопасности;

обсуждает безопасность облачных систем, включая системы информационных технологий (ИТ), которые обрабатывают данные, и системы операционных технологий (ОТ), которые управляют жизненно важным оборудованием и инфраструктурой;

стремится навязать новые требования к отчетности о киберинцидентах определенным поставщикам ИТ и ОТ, а также поставщикам программных продуктов и услуг и создает Совет по анализу кибербезопасности для рассмотрения и оценки таких киберинцидентов и других киберинцидентов, а также;

рассматривает создание пилотных программ, связанных с маркировкой потребителей, в связи с возможностями кибербезопасности устройств Интернета вещей (IoT).

Приказ содержит восемь основных разделов, которые перечислены здесь и более подробно обсуждаются ниже:

Раздел 2 - Устранение препятствий для обмена информацией об угрозах

Раздел 3 - Модернизация кибербезопасности федерального правительства

Раздел 4 - Повышение безопасности цепочки поставок программного обеспечения

Раздел 5 - Создание Совета по обзору кибербезопасности

Раздел 6 - Стандартизация политики федерального правительства по реагированию на уязвимости и инциденты в области кибербезопасности

Раздел 7 - Улучшение обнаружения уязвимостей и инцидентов кибербезопасности в сетях федерального правительства

Раздел 8 - Расширение возможностей федерального правительства в области расследования и исправления положения

Раздел 9 - Системы национальной безопасности

В приведенных ниже резюме обсуждаются основные моменты из этих разделов…

Раздел 2 - Устранение препятствий для обмена информацией об угрозах

Указ признает, что федеральное правительство регулярно заключает контракты с поставщиками ИТ- и ОТ-услуг, которые имеют «уникальный доступ к информации о киберугрозах и инцидентах и информацию о них» в «Федеральных информационных системах». Несмотря на эти специальные знания, в Указе отмечается, что «условия контракта» могут ограничивать способность этих компаний делиться информацией об угрозах или инцидентах с федеральными агентствами. (Из Указа неясно, ограничиваются ли такие «условия контрактов» положениями основных и субподрядных договоров федерального правительства, или же правительство также уделяет внимание коммерческим условиям, которые подрядчики используют в своих негосударственных контрактах.) Указ требует от директора Управления управления и бюджета (OMB) пересмотреть действующие правила заключения договоров с поставщиками ИТ- и ОТ-услуг и рекомендовать обновления для улучшения способности этих поставщиков сохранять и сообщать данные, относящиеся к предотвращению и устранению киберинцидентов.

Кроме того, приказ требует, чтобы министр внутренней безопасности рекомендовал формулировку контракта, требующую отчетности об инцидентах, включая виды инцидентов, о которых необходимо сообщать, типы информации, о которой необходимо сообщать, период времени для отчетности и другие вопросы.

Раздел 3 - Модернизация кибербезопасности федерального правительства

В этом разделе обсуждается модернизация федеральных систем, включая инвестиции в технологии и персонал, повышение уровня внедрения и безопасности использования облачных сервисов, предоставляемых государственным системам, оценка типов и уязвимости несекретной информации в федеральных сетях, использование мульти- факторная аутентификация (MFA) и шифрование, а также другие вопросы. Среди прочего, этот раздел поручает директору OMB разработать федеральную стратегию безопасности облачных вычислений, усилить требования к авторизации и соответствию программам FedRAMP, а также разработать план реализации архитектуры Zero Trust (подход к сетевой безопасности, который фокусируется на аутентификации пользователей и ограничении доступ по служебной необходимости).

Раздел 4 - Повышение безопасности цепочки поставок программного обеспечения

В этом разделе делается попытка «реализовать более строгие и предсказуемые механизмы» для оценки безопасности коммерческого программного обеспечения, используемого федеральным правительством. После получения информации от частного сектора, ученых и других, Орден поручает Министру торговли (через Национальный институт стандартов и технологий, «NIST») разработать руководящие принципы для оценки безопасности коммерческого программного обеспечения. Эти руководящие принципы будут включать, среди прочего, стандарты для безопасных сред разработки программного обеспечения, аутентификации и аудита доступа пользователей, шифрования данных, мониторинга и оповещения о киберинцидентах, устранения уязвимостей,

аутентификации источника программного кода и раскрытия уязвимостей и соответствия требованиям безопасные методы разработки. Важно отметить, что для каждого продукта в соответствии с минимальными элементами, опубликованными NIST.

После публикации этих руководящих принципов приказ требует от агентств убедиться, что закупленное программное обеспечение соответствует этим руководящим принципам. Приказ также потребует от поставщиков программного обеспечения самосертификации в своих договорных соглашениях с федеральными гражданскими агентствами о том, что они выполнили правила, будет налагать требования к поставщикам представлять документацию о соответствии по запросу и приказывает агентствам удалять программные продукты, которые не предоставляют данное свидетельство из списков федеральных закупок.

В этом разделе также содержится указание министру торговли через NIST создать пилотные программы для ознакомления общественности с возможностями безопасности устройств и программного обеспечения IoT с помощью программ маркировки потребителей, а также создать стимулы для поощрения производителей и разработчиков к участию в этих пилотных программах.

Раздел 5 - Создание комиссии по обзору кибербезопасности

Этот раздел требует, чтобы министр внутренней безопасности учредил Наблюдательный совет по кибербезопасности для оценки серьезных киберинцидентов, затрагивающих системы федеральных гражданских агентств или нефедеральные системы. В состав Совета войдут представители Министерства обороны, Министерства юстиции, Агентства по кибербезопасности и безопасности инфраструктуры (CISA), АНБ и ФБР, а также представители частного сектора кибербезопасности или поставщиков программного обеспечения.

Совет директоров начнет с проведения первоначальной проверки, связанной со взломом SolarWinds, в результате которого в декабре 2020 года была создана Cyber Unified Coordination Group. Эта первоначальная проверка также рассмотрит миссию, объем и обязанности Правления, создаст структуру управления Правлением и установит пороговые значения и критерии для типов киберинцидентов, которые оно будет оценивать. После этого Совет будет созван в ответ на серьезные киберинциденты или по указанию президента.

Раздел 6 - Стандартизация политики федерального правительства по реагированию на уязвимости и инциденты в области кибербезопасности

Этот раздел направлен на стандартизацию реакции федерального правительства на киберинциденты, требуя от министра внутренней безопасности разработать стандартный набор процедур («учебник»), который будет использоваться для планирования и проведения реагирования на киберинциденты. Пособие будет включать все соответствующие стандарты NIST и должно использоваться всеми федеральными гражданскими агентствами. В учебном пособии будут определены ключевые термины и они будут использоваться последовательно, чтобы предоставить федеральным гражданским агентствам общий словарь для реагирования на инциденты. В этом разделе также требуется, чтобы CISA ежегодно пересматривала и обновляла руководство.

Пособие должно включать в себя процесс, позволяющий CISA проверять и проверять результаты реагирования на инциденты и результатов устранения инцидентов федеральными гражданскими агентствами после завершения реагирования на инциденты либо напрямую, либо с помощью другого агентства или сторонней группы реагирования на инциденты.

Раздел 7 - Улучшение обнаружения уязвимостей и инцидентов кибербезопасности в сетях федерального правительства

Чтобы улучшить раннее обнаружение кибер-уязвимостей и инцидентов, Приказ предписывает всем федеральным гражданским агентствам развернуть инициативу по обнаружению и реагированию на конечные точки (EDR). Агентства должны координировать свои инициативы EDR с CISA. Этот раздел предписывает OMB установить общегосударственные требования к инициативам EDR и обеспечить наличие у агентств адекватных ресурсов для выполнения этих требований.

Этот раздел также предписывает CISA оценивать действия по поиску угроз в сетях федеральных гражданских агентств, чтобы убедиться, что эти действия не нарушают работу критически важных систем, а владельцы систем уведомляются об уязвимостях.

Раздел 8 - Расширение возможностей федерального правительства в области расследования и исправления положения

Чтобы улучшить способность федерального правительства расследовать и устранять киберинциденты, этот раздел требует, чтобы министр внутренней безопасности предоставил директору OMB рекомендации по регистрации событий и сохранению данных в системах агентства, включая период времени для регистрации, и рекомендуемые требования к ведению журнала и безопасности. Он предписывает агентствам защищать журналы с помощью шифрования для обеспечения судебной целостности.

Этот раздел также предписывает OMB предоставить агентствам соответствующие ресурсы для выполнения этих требований, а также предписывает федеральным гражданским агентствам передавать эти журналы в CISA и ФБР по запросу в соответствии с действующим законодательством.

Раздел 9 - Системы национальной безопасности

В этом разделе указывается, что в течение 60 дней с момента приказа министр обороны должен принять требования к «Системам национальной безопасности», «которые эквивалентны или превышают требования кибербезопасности, изложенные в этом приказе», которые в противном случае уже не применимы к таким системам. системы. Приказ допускает исключения из таких требований «в обстоятельствах, обусловленных особыми потребностями миссии» и требует, чтобы требования были кодифицированы в «Меморандуме о национальной безопасности»…» ***(Susan B. Cassidy, Trisha Anderson, Micaela McMurrough, Robert Huffman. President Biden Signs Executive Order Aimed at Improving Government Cybersecurity // COVINGTON & BURLING LLP (https://www.insideprivacy.com/cybersecurity-2/president-biden-signs-executive-order-aimed-at-improving-government-cybersecurity/#page=1). 18.05.2021).***

***

«13 мая NYDFS объявила о мировом соглашении со страховой компанией, чтобы разрешить обвинения в том, что брокер нарушил правила кибербезопасности штата (23 NYCRR Part 500), не реализовав многофакторную аутентификацию или разумно эквивалентные или более безопасные средства контроля доступа. В соответствии с Частью 500.12 (b), для реализации таких протоколов требуются охваченные организации. Расследование NYDFS также показало, что страховая компания ложно подтвердила свое соблюдение правил кибербезопасности на 2018 год. Согласно условиям приказа о согласии, компания выплатит гражданский денежный штраф в размере 1,8 миллиона долларов и предпримет улучшения для усиления своей существующей программы кибербезопасности для обеспечения соблюдения с 23 NYCRR Part 500. NYDFS признала «похвальное» сотрудничество брокера в ходе проверки и расследования и заявила, что брокер продемонстрировал свою приверженность к исправлению ситуации». ***(NYDFS, insurance company reach $1.8 million cyber breach settlement // Buckley LLP (https://buckleyfirm.com/blog/2021-05-14/nydfs-insurance-company-reach-18-million-cyber-breach-settlement#page=1). 14.05.2021).***

***

«Новая публикация под названием «Защита от атак на цепочку поставок программного обеспечения» была выпущена CISA и Национальным институтом стандартов и технологий (NIST). В нем представлен обзор проблем цепочки поставок программного обеспечения и дает рекомендации о том, как заказчики и поставщики программного обеспечения могут выявлять, оценивать и снижать риски цепочки поставок программного обеспечения. Публикация также предоставляет практическое руководство, связанное с использованием структуры управления рисками цепочки поставок (C-SCRM) NIST и структуры безопасной разработки программного обеспечения (SSDF)». ***(Liza Craig. The Cybersecurity and Infrastructure Security Agency (CISA) releases new cybersecurity resource // Reed Smith LLP (https://viewpoints.reedsmith.com/post/102gwo4/the-cybersecurity-and-infrastructure-security-agency-cisa-releases-new-cybersec). 14.05.2021).***

***

«14 апреля 2021 года Министерство труда США выпустило руководство по кибербезопасности для планов вознаграждения сотрудников. Руководство, состоящее из трех частей, предназначено для спонсоров и доверенных лиц плана, поставщиков услуг планирования и самих участников плана.

Руководство по кибербезопасности от DOL появилось давно. Существенные изменения в технологии и ее использовании в управлении пенсионными планами произошли после принятия Закона о пенсионном обеспечении сотрудников 1974 года (ERISA), который устанавливает минимальные стандарты для большинства частных пенсионных планов и планов медицинского обслуживания, предназначенных для защиты участников плана. Управление текущим планом льгот включает в себя значительный объем информации об участниках плана льгот, включая личную информацию, позволяющую установить личность (PII), и

защищенную медицинскую информацию. Увеличение передачи на аутсорсинг администрирования плана льгот регистраторам и / или другим сторонним администраторам означает, что существует множество ИТ-систем, взаимодействующих друг с другом. Переход в ландшафте пенсионных планов от планов с установленными выплатами к планам с установленными взносами для индивидуальных клиентов усугубил эти тенденции. Тот факт, что участники обычно могут получить доступ к своей учетной записи пенсионного плана или плана медицинского страхования, означает, что домашние компьютеры часто взаимодействуют со сторонним поставщиком услуг или системами работодателя. Суть в том, что современное администрирование плана льгот требует регулярного перемещения информации и активов между несколькими сторонами, что увеличивает количество точек доступа для утечек данных и злоумышленников.

Поскольку интеграция технологий в управление планами вознаграждений сотрудников стала практически повсеместной, риски раскрытия или потерь из-за кибератак или утечки данных экспоненциально увеличились. PII очень ценна для киберпреступников, поскольку обычно постоянно связана с отдельным лицом и поэтому имеет очень длительный срок хранения. Сумма денег, хранящаяся в пенсионных планах США, также делает их богатой мишенью для хакеров и других злоумышленников. Имея мало законодательных указаний, кроме как в области медицинского страхования, спонсоры плана и фидуциары пытаются решить, какие обязанности по плану льгот связаны с кибербезопасностью. А поскольку риски кибербезопасности возросли, недавние судебные разбирательства были направлены против фидуциаров за нарушение своих фидуциарных обязанностей в отношении кибербезопасности.

Как в 2011 году [1], так и в 2016 году [2] Консультативные советы ERISA выпустили отчеты, в которых рекомендуется, чтобы DOL выпустил какую-либо форму руководства по кибербезопасности. В феврале 2021 года Счетная палата правительства (GAO) выпустила отчет «Планы с установленными взносами: федеральное руководство может помочь снизить риски кибербезопасности в 401 (k) и других пенсионных планах » (курсив добавлен). В отчете GAO отмечалось, что руководства DOL по кибербезопасности не существует, и рекомендовалось, чтобы DOL официально указывал, является ли снижение рисков кибербезопасности фидуциарной ответственностью плана, и предоставлял рекомендации, которые определяют минимальные ожидания для устранения рисков кибербезопасности.

Текущее руководство

Три части руководства DOL лишь поверхностно представляют полезные рекомендации для спонсоров плана, доверенных лиц и поставщиков услуг, но, тем не менее, их следует учитывать при реализации стратегий кибербезопасности при администрировании пенсионных планов.

Советы по найму поставщика услуг с надежной практикой кибербезопасности

В этом руководстве изложены шаги и действия, которые спонсоры и доверенные лица должны предпринять для осмотрительной оценки программы и практики кибербезопасности стороннего поставщика услуг в соответствии с ERISA. Хотя эти принципы направлены на выход на пенсию и к поставщикам

услуг 401 (k), они в целом применимы к любому поставщику услуг. Хотя руководство направлено на осмотрительность, необходимую для осмотрительного решения о приеме на работу, оно также представляет собой дорожную карту для осмотрительного мониторинга. Требуемое усердие включает рекомендуемые вопросы и действия:

Каковы стандарты, практики и политики информационной безопасности поставщика услуг, а также результаты аудита?

Сравните эти ответы с отраслевыми стандартами, принятыми другими финансовыми учреждениями. Ищите поставщиков, которые следуют признанным стандартам информационной безопасности, и получайте ежегодные аудиты сторонними аудиторами для проверки и подтверждения кибербезопасности.

Как поставщик услуг проверяет свою практику? Какие уровни стандартов безопасности внедряет поставщик услуг?

Договоритесь о праве проверять результаты аудита программы кибербезопасности поставщика услуг. Даже с существующим поставщиком услуг, учитывая направленность DOL, подумайте о том, чтобы запросить этот аудит и задокументировать его.

Испытывал ли поставщик услуг в прошлом нарушения безопасности? Если да, то что произошло и как была решена проблема?

Осуществляйте тщательную проверку репутации поставщика услуг в отрасли, включая поиск в Интернете и судебных разбирательств в отношении инцидентов безопасности, судебных разбирательств или других судебных разбирательств (например, расследования и рассмотрение того, как прошлые инциденты безопасности были разрешены, например, посредством сотрудничества со спонсором плана или через судебный процесс).

Есть ли у поставщика услуг какие-либо страховые полисы, покрывающие убытки, вызванные кибербезопасностью и кражей личных данных, и если да, то каков объем этой страховки?

Если после рассмотрения вышеперечисленных вопросов в связи с решением о найме спонсор плана или доверенное лицо решает использовать поставщика услуг в качестве администратора плана льгот, DOL предлагает несколько договорных положений, которые спонсор плана или доверенное лицо должны гарантировать, что контракт содержит. Вот некоторые из этих положений:

Постоянное соблюдение отраслевых стандартов кибербезопасности и информационной безопасности, включая передовые методы программы кибербезопасности DOL (обсуждаемые ниже), а также всех применимых федеральных, государственных и местных законов о хранении и уничтожении записей, конфиденциальности и информационной безопасности;

Положения, ограничивающие использование и обмен информацией об участниках плана, которую поставщик услуг получает при администрировании плана;

Политики, которым необходимо следовать в случае нарушения кибербезопасности (например, требования к уведомлению, требования сотрудничества и распределение ответственности за внедрение решений); а также

Требование ежегодного независимого независимого аудита для определения адекватности практики поставщика услуг.

Спонсоры плана и фидуциары должны рассмотреть, должно ли контракт требовать страхового покрытия, специфичного для угроз кибербезопасности (например, страхование профессиональной ответственности и страхование ответственности за ошибки и упущения, страхование кибер-ответственности и страхование нарушения конфиденциальности, а также страхование от преступлений, связанных с залогом верности / бланка).

Учитывая, что у большинства спонсоров планов и доверенных лиц, вероятно, уже есть существующие поставщики услуг, которые помогают в администрировании их пенсионных планов, спонсоры плана и фидуциары могут рассмотреть возможность внесения поправок в применимое соглашение о предоставлении услуг, включив в него некоторые или все положения, рекомендованные выше, в той степени, в которой оно существует. не является достаточной договорной защитой по существующему соглашению.

Рекомендации по программе кибербезопасности для поставщиков услуг

В этом руководстве содержатся советы регистраторам и поставщикам услуг, отвечающим за ИТ-системы и данные, связанные с планом. Для выполнения своих обязательств по кибербезопасности в соответствии с ERISA регистраторы и поставщики услуг должны:

Иметь документированную программу кибербезопасности, которая защищает информацию участников плана от несанкционированного доступа и предоставляет политики для быстрого выявления, оценки и устранения внутренних и внешних рисков кибербезопасности;

Проводить осмотрительную ежегодную оценку рисков, чтобы идти в ногу с меняющимися ИТ-угрозами;

Проводить ежегодный независимый сторонний аудит средств безопасности;

Поручить высшему руководству контролировать программу кибербезопасности, а квалифицированный персонал ее реализовать;

Иметь строгие процедуры контроля доступа для обеспечения идентичности пользователей (например, права доступа, многофакторная аутентификация);

Гарантировать, что любые активы или данные, хранящиеся в облаке или управляемые сторонним поставщиком услуг, подлежат соответствующему анализу безопасности и независимой оценке безопасности;

Проводить периодические тренинги по повышению осведомленности о кибербезопасности, чтобы помочь сотрудникам распознавать векторы атак, предотвращать инциденты, связанные с кибербезопасностью, и реагировать на потенциальные угрозы;

Внедрить программу жизненного цикла разработки безопасной системы и управлять ею, чтобы гарантировать безопасную разработку приложений, используемых для администрирования плана;

Подготовить программу обеспечения устойчивости бизнеса, которая включает планы обеспечения непрерывности бизнеса, аварийного восстановления и реагирования на инциденты;

Шифровать конфиденциальные данные в соответствии с отраслевыми стандартами;

Внедрить строгий технический контроль с лучшими практиками безопасности (например, аппаратное, программное и микропрограммное обеспечение, используемое при администрировании плана, обновлено и обновлено); а также

Надлежащим образом реагируйте на любые инциденты кибербезопасности, расследуя инцидент и информируя соответствующие органы, страховщика и планируя контакты.

Более подробная информация об этих передовых методах программы кибербезопасности изложена в этом руководстве.

Советы по онлайн-безопасности

Это руководство предназначено для участников плана. Тот факт, что DOL выпустил это руководство, подтверждает, что участники плана также должны играть определенную роль в обеспечении безопасности своих данных и активов. Чтобы снизить риск мошенничества и потерь на счете участника, DOL рекомендует участникам плана:

Регулярно следите за своей учетной записью в Интернете;

Используйте надежные и уникальные пароли;

Используйте многофакторную аутентификацию;

Поддерживайте актуальность личной контактной информации;

Закройте или удалите неиспользуемые учетные записи;

Опасайтесь бесплатного Wi-Fi;

Остерегайтесь фишинговых атак;

Использовать антивирусное программное обеспечение и поддерживать приложения и программное обеспечение в актуальном состоянии; а также

Знайте, как сообщать о случаях кражи личных данных и кибербезопасности.

Большинство участников прочитают эти правила и подумают, что они очевидны. Тем не менее, спонсоры плана и доверенные лица должны поощрять участников плана помнить об этих рекомендациях.

Руководство - это руководство… а не закон

Три руководства DOL являются шагом в правильном направлении и могут дать спонсорам плана, фидуциарам и регистраторам некоторые указания относительно того, как выполнять свои обязанности в этой области. Однако реальность остается в том, что руководство DOL - это всего лишь руководство. Руководство не имеет полной силы закона или постановления. Тем не менее, неспособность адекватно отреагировать на это руководство может увеличить потенциальную ответственность спонсоров плана или доверенных лиц в связи с данными плана или другими нарушениями кибербезопасности…» ***(Sarah N. Lowe, Edward I. Rivin. A Long Time Comin': The DOL issues Cybersecurity Guidance // Frost Brown Todd LLC (https://frostbrowntodd.com/a-long-time-comin-the-dol-issues-cybersecurity-guidance/#page=1). 12.05.2021).***

***

«Губернатор Джорджии подписал законопроект 156, устанавливающий особые требования к уведомлению для государственных агентств и коммунальных служб, которые подвергаются атакам кибербезопасности, утечки данных или вредоносное ПО, и требующий уведомления директора штата по чрезвычайным ситуациям в Джорджии в течение двух часов после уведомления федеральных агентств по чрезвычайным ситуациям.

Кроме того, закон требует от директора штата Джорджия по управлению чрезвычайными ситуациями и внутренней безопасности разработать дополнительные правила и положения, касающиеся требований об уведомлении.

HB 156 был подписан 25 марта 2021 года и уже вступил в силу.

Сфера действия закона

Закон распространяется на коммунальные предприятия и агентства в штате Джорджия. Оба термина имеют широкое определение:

«Коммунальное предприятие» включает «любую линию, объект или систему, находящуюся в государственной, частной или совместной собственности, для производства, передачи или распределения электроэнергии, электричества, света, тепла или газа».

«Агентство» означает «исполнительную, судебную или законодательную ветви власти Грузии, а также любой департамент, агентство, правление, бюро, офис, комиссию, государственную корпорацию и орган власти; каждый округ, муниципальная корпорация, школьный округ или другое политическое подразделение; и каждый их отдел, агентство, правление, бюро, офис, комиссии или органы; и каждый город, округ, регион или другой орган власти, учрежденный в соответствии с законодательством Джорджии. Определение агентства специально исключает «любой округ, муниципальную корпорацию, государственную корпорацию или любой орган [то же самое, когда]… действующий в качестве поставщика оптовая или розничная торговля электроэнергией или газом или в качестве трубопровода, через который муниципальная корпорация предоставляет электрические или газовые услуги».

Ключевые положения: когда требуются отчеты

Закон требует, чтобы коммунальные предприятия и агентства отчитывались перед директором по чрезвычайным ситуациям и национальной безопасности Джорджии в двух случаях:

Любое агентство должно сообщать о любом инциденте кибератаки, утечке данных или идентифицированном использовании вредоносного ПО в агентстве, компьютере или сети, если характер атаки определяется как «создание события, связанного с безопасностью жизни, существенное влияние на безопасность. данные и информационные системы или влияют на критически важные системы, оборудование или предоставление услуг». Директор должен разработать дополнительные требования, определяющие механизм отчетности, необходимую информацию и сроки для составления отчета.

Когда от агентства или коммунального предприятия требуется сообщить об инциденте кибератаки, утечке данных или выявленном использовании вредоносного ПО на компьютере или сети коммунального предприятия или агентства правительству США или федеральному агентству, агентство или

коммунальное предприятие должно предоставить практически ту же информацию Директор Управления по чрезвычайным ситуациям и национальной безопасности Джорджии в течение двух часов после представления отчета правительству Соединенных Штатов.

Если федеральные законы, правила или постановления запрещают раскрытие информации, которая в противном случае подлежала бы передаче в соответствии с законом, закон разрешает коммунальному предприятию предоставлять информацию только после того, как запрет будет снят или истечет.

Отчеты и записи, сделанные в соответствии с законом, освобождены от государственных публичных записей и законов FOIA, которые сторонники закона и предложили законопроект 134 Палаты представителей, который разрешает закрытые правительственные заседания при обсуждении планов и процедур кибербезопасности, поддерживают по мере необходимости для защиты безопасности и интересов грузин.

Критики обеспокоены тем, что закон и предложенный закон могут подорвать принципы открытого правительства. Стоит отметить, что принятый закон не предусматривает конкретного механизма обеспечения соблюдения заявленных требований к отчетности.

Тренд

Хотя законодательный орган Джорджии не дал особых комментариев по этому конкретному закону, вполне вероятно, что он был частично вызван недавними громкими кибератаками и атаками программ-вымогателей, нацеленных на коммунальные предприятия и правительственные учреждения, включая местные органы власти города и страны. операции.

Закон во многом соответствует федеральному распоряжению исполнительной власти, разрабатываемому администрацией Байдена, который требует от федеральных агентств и частных лиц, работающих с правительством США, соблюдения определенных стандартов кибербезопасности, а также обязывает частные организации сообщать о любых кибератаках и нарушениях, или взломать своих клиентов из федерального правительства…» ***(Lael Bellamy, Emily Maus. Georgia's HB 156, requiring state notice for utility cybersecurity incidents, is now in effect // DLA Piper (https://blogs.dlapiper.com/privacymatters/georgias-hb-156-requiring-state-notice-for-utility-cybersecurity-incidents-is-now-in-effect/#page=1). 12.05.2021).***

***

«Если прошедший год и научил нас чему-то, так это тому, что нам еще предстоит проделать большую работу по укреплению кибербезопасности нашего правительства. Мы узнали, что противники знают, как приспосабливаться и развиваться, пересматривая свои методы, чтобы сделать их более изощренными, чем когда-либо. Согласно недавнему исследованию Okta, проведенному правительством 2020 года, количество целевых фишинговых атак, связанных с COVID, выросло более чем на 677%, что доказывает, что злоумышленники меняют свой менталитет на охоту на страхи перед пандемией и удаленную работу.

Взлом SolarWinds, один из крупнейших в 21 веке, является лишь последним из, казалось бы, бесконечной серии кибератак. Пришло время государственным органам пересмотреть свой подход к безопасности. Им необходимо удвоить основные принципы и решить не только технические проблемы, но и культурные барьеры, которые мешают более безопасной и надежной удаленной рабочей силе.

По данным Управления США по управлению персоналом это nnual отчет Конгресса о состоянии телеработы в федеральном правительстве, только 42% федеральных служащих имели право на телеработы до пандемии. Быстрый переход к удаленной работе требует изменения менталитета - более глубокого понимания безопасности и серьезных последствий плохой стратегии безопасности. В удаленной рабочей среде о безопасности нельзя забывать.

По мере того, как все больше правительственных организаций переводят услуги для граждан на мобильные и облачные платформы, многие осознают ценность реализации таких концепций безопасности, как нулевое доверие, управление доступом к идентификационной информации (IAM) и многофакторная аутентификация (MFA) для защиты устройств, подключающихся к правительственным сетям. тем не менее, идея поставить под сомнение и подтвердить подлинность тех, кто имеет доступ к различным частям сети, должна выходить за рамки технологии.

Команда сильна настолько, насколько силен ее самый слабый игрок

Глобальная пандемия потребовала серьезных социальных изменений, которые имеют решающее значение для остановки распространения вируса COVID-19. Социальное дистанцирование, мытье рук и ношение масок - рекомендуемые действия, которые при коллективном осуществлении в обществе могут замедлить распространение вируса с конечной целью создания коллективного иммунитета - когда большая часть сообщества становится невосприимчивой к болезни..

Та же концепция применяется в кибербезопасности. Чего сегодня не хватает правительству, так это более сильной культурной ориентации на минимизацию рисков в организациях. Все руководители служб безопасности несут общую ответственность за адаптацию и сохранение бдительности перед лицом постоянно растущей сложности, в том числе формирование культуры общих интересов безопасности для повышения устойчивости к угрозам. Агентства должны встроить безопасность в ДНК своей цифровой архитектуры. Успешная цифровая трансформация невозможна, если кибербезопасность не построена внутри.

Те, кто уже восприняли безопасность как культуру, в начале пандемии были в выгодном положении, чтобы адаптироваться к массовому телеработе, которая продолжалась. Забегая вперед, самое важное, что должны сделать отстающие, - это держать кибер-стратегии в центре внимания и относиться к ним как к первоклассному гражданину.

От специалистов по коммуникациям и контрактам до сотрудников отдела кадров и не только - всем в организации необходимо соблюдать правила кибергигиены, а не только ИТ-персоналу. Для руководителей службы безопасности мы должны максимально упростить этот процесс, чтобы побудить людей принять передовые методы обеспечения безопасности во всей организации.

Создание культурного фундамента

Чтобы заставить людей принять безопасность, нужно облегчить им задачу. Обеспечение положительного опыта конечных пользователей в каждом приложении и портале упрощает безопасность. Это также мощный шаг к достижению цели киберпространственного иммунитета. Например, ни одному сотруднику не понравится 10-минутное требование для входа в видеовызов из-за сверхчувствительного протокола, необходимого для присоединения к утренним собраниям.

Стеки ИТ и, соответственно, стеки безопасности стали слишком сложными, слишком громоздкими и готовы к раскрытию. Безопасность - это ответственность каждого, поэтому меньшее количество трений и бесполезных шагов, которые мы создаем, помогут сделать безопасные привычки легкими и привычными для команд.

Как мы видели в этом году, кампании по повышению осведомленности о здоровье являются ключевой тактикой профилактики для агентств общественного здравоохранения. Точно так же повышение осведомленности и информирование сотрудников о рисках безопасности, уязвимостях и мошенничестве - простой первый шаг к формированию нового кибер-мышления для всех частей организации. Обладая прочной культурой безопасности, организации могут наиболее эффективно выполнять общие стратегии безопасности, такие как нулевое доверие и MFA.

Достижение фундаментальных технологических целей

Концепция нулевого доверия - это концепция, которая существует уже много лет, начиная с работ Иерихонского форума в 2005 году. Такой подход гарантирует, что нужные люди имеют нужный уровень доступа, к нужным ресурсам, в нужном контексте, и что доступ оценивается непрерывно - и все это без дополнительных затруднений для пользователя. В связи с тем, что массовым телеработам не предвидится конца, агентствам не следует больше ждать, чтобы претворить эту модель в жизнь.

Сосредоточившись на управлении доступом и учетными данными, руководители службы безопасности могут снизить риск для слабых и уязвимых областей, которые злоумышленники стремятся использовать. Обязательно следуйте передовым методам защиты учетных данных, включая рекомендации и предупреждения от NSA, CISA, NIST и других агентств. Например, недавно АНБ выпустило руководство, в котором подробно описаны шаги по блокировке использования субъектов-служб, такие как аудит создания и использования учетных данных субъекта-службы.

Кроме того, включение MFA является важным шагом для поддержания работоспособности системы безопасности. Адаптивный MFA, который реагирует на риски и контекст, следует развертывать везде, где это возможно, а не только для привилегированных пользователей. Это ступенька к более надежной и безопасной аутентификации без пароля в агентствах. При средней стоимости утечки данных до 3,86 миллиона долларов внедрение адаптивной многофакторной аутентификации снижает риски для организации на 75%.

В 2021 году «новая нормальность» теперь просто нормальна, и руководителям служб безопасности необходимо продолжать адаптироваться к меняющимся условиям труда. Используйте этот новый год как возможность укрепить систему безопасности, которая защищает агентства, сотрудников и клиентов. Но также помните, что успешная стратегия кибербезопасности выходит за рамки технической основы. Когда мы, как лидеры, внедряем культуру, в которой мы сосредотачиваемся на образовании и осведомленности и упрощаем соблюдение всеми сотрудниками базового протокола безопасности, мы можем добиться иммунитета киберпространства и снизить влияние будущих инцидентов». ***(Sean Frazier. Building herd immunity into government cybersecurity // Hubbard Radio Washington DC, LLC (https://federalnewsnetwork.com/commentary/2021/05/building-herd-immunity-into-government-cybersecurity/). 12.05.2021).***

***

«Учитывая свою высокопрофессиональную миссию и широкую связь с общественностью, образовательными учреждениями и внешними исследовательскими центрами, НАСА представляет киберпреступникам более крупную потенциальную цель, чем большинство правительственных агентств. Обширное присутствие Агентства в Интернете, насчитывающее около 3000 веб-сайтов и более 42000 общедоступных наборов данных, также делает его очень уязвимым для вторжений. В последние годы НАСА работало над повышением готовности к кибербезопасности благодаря усилиям, возглавляемым Офисом главного информационного директора (OCIO). Тем не менее, только за последние 4 года НАСА пережило более 6000 кибератак, включая фишинговые атаки и внедрение вредоносных программ в системы Агентства. Следовательно, очень важно, чтобы Агентство разработало надежные методы кибербезопасности для защиты от текущих и будущих угроз.

Активы НАСА в области информационных технологий (ИТ) обычно делятся на две широкие категории: институциональные и командные системы. Эти активы контролируются тремя основными уровнями управления, которые отвечают за управление кибербезопасностью. Персонал OCIO наблюдает за институциональными возможностями и возможностями безопасности, которые поддерживают весь персонал НАСА. Миссии обычно финансируют свои собственные сети, а их ИТ-персонал имеет представление об эксплуатационных аспектах и аспектах безопасности этих сетей. Наконец, ИТ-персонал в центрах НАСА управляет и контролирует операции для программ и проектов, расположенных там, которые включают как институциональные сети, так и сети миссий.

Чтобы оценить готовность НАСА к кибербезопасности, мы исследовали, спроектирована ли: (1) архитектура предприятия OCIO для надлежащей оценки рисков и угроз кибербезопасности; (2) Стратегия защиты кибербезопасности НАСА основана на оценке рисков; (3) распределение ресурсов кибербезопасности является адекватным и соответствующим образом расставлено по приоритетам; и (4) риски кибербезопасности агентства эффективно оцениваются с использованием надежных практик ИТ-безопасности.

Чтобы завершить эту работу, мы изучили применимые законы и постановления, опросили персонал OCIO, изучили документацию Агентства, проанализировали бюджетные и кадровые данные, а также проанализировали прошлые кибер-нарушения. Мы опирались на рекомендации по структуре кибербезопасности Национального института стандартов и технологий (NIST) и специальным публикациям серии 800, Центру 20 основных средств контроля безопасности в Интернете и архитектуре федерального предприятия.

ЧТО МЫ НАХОДИЛИ

Атаки на сети НАСА - явление не новое, хотя попытки украсть важную информацию становятся все более сложными и серьезными. По мере того как злоумышленники становятся все более агрессивными, организованными и изощренными, управление и снижение рисков кибербезопасности становится критически важным для защиты обширной сети ИТ-систем НАСА от злонамеренных атак или взломов, которые могут серьезно помешать способности Агентства выполнять свою миссию. Хотя НАСА предприняло позитивные шаги для решения проблемы кибербезопасности в областях мониторинга сети, управления идентификацией и обновления своего стратегического плана ИТ, оно по-прежнему сталкивается с проблемами в укреплении основополагающих усилий по кибербезопасности.

Мы обнаружили, что способность НАСА предотвращать, обнаруживать и смягчать кибератаки ограничена неорганизованным подходом к архитектуре предприятия. Архитектура предприятия (EA) и Архитектура безопасности предприятия (ESA) - схемы того, как организация анализирует и управляет своими ИТ и кибербезопасностью, - являются ключевыми компонентами для эффективного управления ИТ. Архитектура предприятия разрабатывалась в НАСА более десяти лет, но все еще остается незавершенной, в то время как способ, которым Агентство управляет инвестициями и операциями в ИТ, остается разнообразным и разовым. К сожалению, фрагментированный подход к ИТ с многочисленными отдельными линиями полномочий долгое время был определяющей чертой среды, в которой решения по кибербезопасности принимаются в Агентстве.

Мы также отметили, что НАСА проводит свою оценку и авторизацию (A&A) ИТ-систем непоследовательно и неэффективно, при этом качество и стоимость оценок сильно различаются по Агентству. Эти несоответствия могут быть напрямую связаны с децентрализованным подходом НАСА к кибербезопасности. НАСА планирует заключить новый контракт с корпоративными решениями и услугами в области кибербезопасности и конфиденциальности (CyPrESS), направленный на устранение дублирующих киберсервисов, что могло бы предоставить Агентству средство для сброса процесса A&A для более эффективной защиты своих ИТ-систем.

ЧТО МЫ РЕКОМЕНДУЕМ

Чтобы повысить готовность НАСА к кибербезопасности и обеспечить непрерывность процессов и улучшить состояние безопасности систем НАСА, мы рекомендовали заместителю администратора и главному информационному директору:

1. Интегрируйте EA и ESA и разработайте показатели для отслеживания общего прогресса и эффективности EA.

2. Сотрудничать с главным инженером в разработке стратегий по выявлению и устранению пробелов в ЭА в рамках миссии и институциональных ИТ-границ.

3. Оцените оптимальное организационное размещение Enterprise Architect и Enterprise Security Architect во время и после внедрения MAP для повышения готовности к кибербезопасности.

4 Определите годовые затраты каждого центра на выполнение независимых оценок, включая укомплектование персоналом, в процессе A&A для 526 систем НАСА.

5. Разработайте базовые требования в запланированном контракте CyPrESS для специальной группы предприятия для управления и выполнения процесса оценки для всех систем NASA, подпадающих под действие A&A.

Мы предоставили проект этого отчета руководству НАСА, которое согласилось с нашими рекомендациями. Мы считаем комментарии руководства отзывчивыми; Таким образом, рекомендации считаются решенными и будут закрыты после завершения и проверки предлагаемых корректирующих действий». ***(NASA OIG: NASA's Cybersecurity Readiness // SpaceRef Interactive Inc (http://www.spaceref.com/news/viewsr.html?pid=54812). 18.05.2021).***

***

«…Согласно опросу 2020 года, проведенному (ISC) 2, международной некоммерческой организацией, которая предлагает программы обучения и сертификации в области кибербезопасности, в Соединенных Штатах насчитывается около 879000 специалистов по кибербезопасности, и существует потребность в еще 359000 сотрудников.

Группа заявляет, что в глобальном масштабе этот разрыв еще больше - почти 3,12 миллиона незаполненных вакансий. Ее генеральный директор Клар Россо сказала, что, по ее мнению, потребность может быть выше, поскольку некоторые компании откладывают прием на работу во время пандемии.

Потребности варьируются от аналитиков по безопасности начального уровня, которые отслеживают сетевой трафик для выявления потенциальных злоумышленников в системе, до руководителей высшего звена, которые могут сформулировать перед генеральными директорами и членами совета директоров потенциальные финансовые и репутационные риски, связанные с кибератаками.

Бюро статистики труда США проектов «аналитик по информационной безопасности» будет десятым самым быстрорастущим оккупации в течение следующего десятилетия, с темпом роста занятости на 31% по сравнению со средним темпом роста 4% для всех профессий.

Если спрос на профессионалов в области кибербезопасности в частном секторе резко возрастет, некоторые эксперты говорят, что талантливые работники могут уйти из правительства для получения более прибыльной корпоративной работы - риск, который особенно остро стоит для небольших местных правительственных агентств, которые управляют критически важной инфраструктурой в своих сообществах, но имеют ограниченные бюджеты..

«Подумайте о важности того, что делает ваше местное правительство: очистка воды, обработка отходов, управление дорожным движением, связь для правоохранительных органов, общественная безопасность, управление чрезвычайными ситуациями», - сказал Майк Гамильтон, главный специалист по информационной безопасности Critical Insight. «Но Amazon там размахивает сумками с наличными, чтобы защитить свои розничные операции».

Гамильтон, бывший главный специалист по информационной безопасности Сиэтла, штат Вашингтон, с 2006 по 2013 год, добавил, что местные органы власти «не могут привлекать и удерживать этих людей, когда конкуренция за них настолько высока, поэтому мы должны делать много их."

«Не краткосрочное решение»

Для решения этой проблемы уже работают различные программы образования, обучения и повышения квалификации.

GuidePoint помогает обучать ветеранов, покидающих армию, для работы в сфере кибербезопасности. А Гамильтон из Critical Insight управляет некоммерческой организацией под названием Системы кибероборазования в области безопасности общественной инфраструктуры, с помощью которой студенты пяти университетов получают практический опыт, выполняя мониторинг безопасности данных в реальном времени в сетях местных органов власти, предоставляя важные услуги для небольших городов и округов, которые иначе не смог бы себе это позволить.

Эксперты говорят, что есть возможность привлечь в отрасль новые таланты, сосредоточив внимание на разнообразии. По словам Россо, всего 25% профессионалов в области кибербезопасности составляют женщины, поэтому (ISC) 2 в этом году запустила программу разнообразия, равенства и интеграции, направленную на привлечение и удержание большего числа женщин в этой профессии.

«Мы должны признать, что существует огромное разнообразие людей, которые действительно могут выполнять... эту работу очень хорошо», - сказал Гамильтон, имея в виду аналитиков по безопасности, которые отслеживают трафик в сети, чтобы найти поведение, которое может указывать на то, что злоумышленник получил доступ к системе. «Как страна, мы не очень хорошо пользуемся теми ресурсами, которые у нас есть».

Между тем, по мере того, как отрасль работает над увеличением своей рабочей силы, это может стать огромной возможностью для компаний-поставщиков услуг и программного обеспечения, которые могут помочь фирмам усилить свои протоколы кибербезопасности без найма собственных команд.

Потому что даже при существующих программах обучения ожидается, что глобальный разрыв в рабочей силе в области кибербезопасности будет расти на 20–30% ежегодно в течение следующих нескольких лет, - сказал Россо из (ISC) 2. Эксперты говорят, что и государственный, и частный секторы должны больше инвестировать в рост рабочей силы в отрасли.

Части плана президента Джо Байдена по созданию рабочих мест в США на сумму 2 триллиона долларов могут помочь. Предложение по инфраструктуре включает 20 миллиардов долларов для государственных, местных и племенных

органов власти для обновления и улучшения мер кибербезопасности для своих энергетических систем.

Тем не менее, эксперты говорят, что необходимо сделать больше, предлагая широкое переосмысление систем образования от начальной школы до высшего образования, чтобы включить больше обучения кибербезопасности.

«К сожалению, краткосрочного решения нет», - сказал Орм из GuidePoint. «Я думаю, что нам нужно взглянуть на это в долгосрочной перспективе - как это делают многие наши противники - чтобы сказать, как мы можем систематически создавать следующее поколение и поколение после него и создавать маховик квалифицированных специалистов по безопасности, которые будут выход на рынок труда в ближайшие 50–100 лет?» ***(Clare Duffy. Wanted: Millions of cybersecurity pros. Salary: Whatever you want // Cable News Network (https://edition.cnn.com/2021/05/28/tech/cybersecurity-labor-shortage/index.html). 28.05.2021).***

***

«Сегодня Управление транспортной безопасности (TSA) Министерства внутренней безопасности объявило о Директиве по безопасности, которая позволит Департаменту лучше выявлять, защищать и реагировать на угрозы для критически важных компаний в секторе трубопроводов.

«Сфера кибербезопасности постоянно развивается, и мы должны адаптироваться к новым и возникающим угрозам», - сказал министр внутренней безопасности Алехандро Н. Майоркас. «Недавняя атака программ-вымогателей на крупный нефтепровод демонстрирует, что кибербезопасность трубопроводных систем имеет решающее значение для безопасности нашей страны. DHS продолжит тесное сотрудничество с нашими партнерами из частного сектора для поддержки их операций и повышения устойчивости критически важной инфраструктуры нашей страны».

Директива о безопасности потребует от владельцев и операторов критически важных трубопроводов сообщать о подтвержденных и потенциальных инцидентах кибербезопасности в Агентство по кибербезопасности и безопасности инфраструктуры (CISA) DHS и назначать координатора по кибербезопасности, который будет доступен 24 часа в сутки, семь дней в неделю. Это также потребует от владельцев и операторов критически важных трубопроводов пересмотреть свою текущую практику, а также выявить любые пробелы и соответствующие меры по устранению кибер-рисков и сообщить о результатах в TSA и CISA в течение 30 дней.

TSA также рассматривает последующие обязательные меры, которые еще больше поддержат трубопроводную отрасль в повышении ее кибербезопасности и укрепят государственно-частное партнерство, столь важное для кибербезопасности нашей страны.

С 2001 года TSA тесно сотрудничает с владельцами и операторами трубопроводов, а также со своими партнерами в федеральном правительстве, чтобы повысить готовность к физической безопасности систем трубопроводов для опасных жидкостей и природного газа в США. Как ведущее национальное

агентство по защите критически важной инфраструктуры от угроз кибербезопасности, CISA предоставляет ресурсы по кибербезопасности для снижения потенциальных рисков, в том числе через специальный центр, который распространяет информацию среди организаций, сообществ и отдельных лиц о том, как лучше защитить себя от атак программ- вымогателей.

Эта новая Директива TSA по безопасности также подчеркивает важную роль, которую CISA играет как национальный центр киберзащиты страны. В декабре прошлого года Конгресс посредством Закона о разрешении на национальную оборону уполномочил CISA выполнять свою миссию по защите федеральных сетей гражданского правительства и критически важной инфраструктуры нашей страны от физических и киберугроз». ***(DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators // Department of Homeland Security (https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators). 27.05.2021).***

***

«Двухпартийное руководство Научного комитета палаты представителей обратилось в Счетную палату правительства с просьбой расследовать деятельность НАСА в области кибербезопасности на фоне растущей обеспокоенности по поводу взлома правительственных компьютерных систем.

В письме от 27 мая высшие демократы и республиканцы комитета попросили GAO расследовать «риски кибербезопасности для конфиденциальных данных», связанные с крупными программами НАСА. Это включает в себя сравнение деятельности НАСА с ведущими практиками кибербезопасности и определение дополнительных методов, которые агентство должно принять.

В письме не указаны какие-либо конкретные нарушения кибербезопасности НАСА или другие события, которые побудили запрос на пересмотр, а скорее давние опасения по поводу уязвимостей агентства. «Степень, в которой эти постоянные недостатки повлияли на способность агентства защищать свои наиболее конфиденциальные данные, особенно данные, связанные с его крупными проектами освоения космоса, космическими кораблями и полетами человека в космос, не совсем понятна», - написали участники в письме.

Управление генерального инспектора НАСА (OIG) регулярно рассматривает и критикует подход НАСА к управлению информационными технологиями в целом и кибербезопасности в частности. В своем последнем отчете о кибербезопасности, опубликованном 18 мая, он предупредил о растущих угрозах кибербезопасности для агентства.

«Атаки на сети НАСА - явление не новое, хотя попытки украсть важную информацию становятся все более сложными и серьезными», - говорится в заключении OIG. В нем говорится, что количество попыток фишинга увеличилось более чем вдвое, а количество атак вредоносных программ увеличилось «экспоненциально» во время перехода к удаленной работе, вызванного пандемией.

«Киберугроза компьютерным сетям НАСА, исходящая от вторжений через Интернет, расширяется по размаху и частоте, и успех этих вторжений

демонстрирует все более сложный характер проблем кибербезопасности, с которыми сталкивается Агентство», - говорится в отчете. Эти угрозы, как описано в отчете, варьируются от скоординированных атак китайских хакерских групп до контрактного сотрудника НАСА, который установил программное обеспечение на компьютеры агентства для добычи криптовалюты.

В отчете OIG агентство подверглось критике за «неорганизованный» подход к управлению информационными технологиями, например за финансирование избыточных услуг. НАСА также уделяет приоритетное внимание кибербезопасности для некоторых ключевых программ, таких как Международная космическая станция, «оставляя кибербезопасность для других систем миссий как второстепенную задачу».

Руководство комитета по науке в своем письме в GAO предположило, что их запрос на исследование был также вызван проблемами кибербезопасности в других частях федерального правительства. «Недавние изощренные атаки кибербезопасности на несколько систем федерального правительства, которые оставались незамеченными в течение нескольких месяцев, подчеркивают важность наличия надежных процессов управления рисками кибербезопасности, связанными с конфиденциальными данными НАСА», - пишут они.

Это включает в себя так называемый «SolarWinds» взлом компьютерных систем государственного и частного секторов, совершенный, по мнению аналитиков кибербезопасности, хакерской группой, связанной с российской разведкой. Эти хакеры в прошлом году взломали программное обеспечение, разработанное компанией SolarWinds для управления сетью. Это дало хакерам доступ к компьютерным сетям клиентов SolarWinds, включая несколько крупных компаний и федеральных агентств.

«SolarWinds был большим тревожным сигналом», - сказала Кэти Людерс, помощник администратора НАСА по исследованиям и операциям человека, отвечая на вопрос о кибербезопасности в НАСА во время заседания Совета по аэронавтике и космической инженерии и Совета по космическим исследованиям 25 мая.

Она не вдавалась в подробности о конкретных шагах, которые НАСА предприняло после взлома SolarWinds, но подчеркнула важность, которую агентство придает кибербезопасности. «Это, безусловно, было нашей основной областью внимания на протяжении последних четырех-пяти лет».

Одна из проблем связана с компаниями и использованием коммерческих активов, уязвимости кибербезопасности которых могут стать способом обойти защиту кибербезопасности НАСА. «Это большое беспокойство для нас», - сказала она. «Мы должны выяснить, как сделать это и защитить себя, оставаясь при этом на передовой».

Письмо в GAO подписали представители Эдди Бернис Джонсон (штат Техас) и Фрэнк Лукас (штат Оклахома), председатель и высокопоставленный член, соответственно, полного научного комитета палаты представителей, и представитель Дона Бейера (демократия). Вирджиния) и Брайан Бабин» ***(R-Техас), председатель и высокопоставленный член космического подкомитета соответственно. (Jeff Foust. Congress asks GAO to investigate NASA cybersecurity***

// SpaceNews (https://spacenews.com/congress-asks-gao-to-investigate-nasa-cybersecurity/). 28.05.2021).

***

Країни ЄС та Великобританія

«В связи с ростом числа атак на цепочки поставок программного обеспечения правительство Великобритании предлагает новые правила для снижения угрозы взлома через надежное программное обеспечение, которое было взломано кибератаками.

Департамент цифровых технологий, культуры, СМИ и спорта (DCMS) призвал к ознакомлению с новыми правилами, которые могут потребовать, чтобы поставщики ИТ-услуг и поставщики управляемых услуг (MSP) прошли те же оценки кибербезопасности, что и поставщики важнейших национальных инфраструктур.

«По мере того как цепочки поставок становятся взаимосвязанными, уязвимости в продуктах и услугах поставщиков, соответственно, становятся более привлекательными целями для злоумышленников, которые хотят получить доступ к организациям», - заявили в правительстве. «Недавние громкие киберинциденты, когда злоумышленники использовали поставщиков управляемых услуг в качестве средства атаки на компании, являются суровым напоминанием о том, что субъекты киберугроз более чем способны использовать уязвимости в системе безопасности цепочки поставок, и, казалось бы, небольшие игроки в цепочке поставок организации могут ввести непропорционально высокий уровень киберриска».

Исследование DCMS показало, что только 12% организаций проверяют поставщиков на предмет рисков кибербезопасности и только около 5% устраняют уязвимости в своей более широкой цепочке поставок.

Правительство Великобритании особенно обеспокоено рисками, которые представляет для национальных предприятий и агентств ИТ-аутсорсинг, указывая на такие атаки, как «CloudHopper», при которых организации были скомпрометированы через своего поставщика управляемых услуг.

Новые правила могут означать, что MSP должны будут соответствовать британской системе оценки кибербезопасности (CAF), ставя этот сектор наряду с кибер-требованиями, предъявляемыми к поставщикам критически важной инфраструктуры Великобритании.

CAF направлен на обеспечение наличия политик в соответствующих секторах для защиты устройств и предотвращения несанкционированного доступа, обеспечение защиты данных в состоянии покоя и при передаче, обеспечение безопасности резервных копий и обучение персонала кибербезопасности.

Национальный центр кибербезопасности Великобритании (NCSC) в феврале предупредил, что количество атак на цепочки поставок растет, особенно это касается атак на конвейеры сборки программного обеспечения…». ***(Liam Tung. Supply chain hacking attacks: Government eyes new rules to tighten security // ZDNet***

(https://www.zdnet.com/article/supply-chain-hacking-attacks-government-eyes-new-rules-to-tighten-security/). 18.05.2021).

***

«Совет ЕС в понедельник расширил инструмент, позволяющий блоку замораживать активы и запрещать поездки для иностранных хакеров, в том числе введенные в прошлом году в отношении групп, поддерживаемых государством из России, Китая и Северной Кореи.

Национальные столицы «решили продлить рамки ограничительных мер против кибератак, угрожающих ЕС или его государствам-членам, еще на год, до 18 мая 2022 года», - говорится в заявлении Совета.

Эти так называемые «киберсанкции» - это мера, которую страны имеют в своем распоряжении с мая 2019 года, чтобы попытаться сдержать хакеров и отреагировать на атаки на европейские цели.

ЕС ввел первые в истории санкции в ответ на кибератаки в июле 2020 года, нацеленные на российских, китайских и северокорейских хакеров, причастных к серьезным инцидентам в предыдущие годы, а именно к вспышке вымогателя NotPetya, взлому цепочки поставок Cloud Hopper и атаке программы- вымогателя WannaCry.

В октябре 2020 года блок ввел санкции в отношении двух российских разведчиков и подразделения военной разведки ГРУ за их причастность к взлому парламента Германии в 2015 году». ***(LAURENS CERULUS. EU countries extend sanctions against Russian, Chinese hackers // POLITICO (https://www.politico.eu/article/eu-council-cyber-sanctions-russia-china-hackers/). 17.05.2021).***

***

«Прити Патель пообещал провести правительственный обзор Закона Великобритании о неправомерном использовании компьютеров, действующий 30 лет назад, «в этом году», а также осудить компании, которые подкупают преступников-вымогателей.

Министр внутренних дел пообещал провести юридический анализ в своем выступлении на конференции CyberUK сегодня днем, организованной Национальным центром кибербезопасности (NCSC).

«В рамках обеспечения того, чтобы у нас были правильные инструменты и механизмы для обнаружения, пресечения и сдерживания наших противников, я считаю, что сейчас подходящее время для проведения официального пересмотра Закона о неправомерном использовании компьютеров», - сказал Патель.

Принятый в 1990 году Закон о неправомерном использовании компьютеров (CMA) в последний раз подвергался значительным поправкам в 2008 году, продлевая срок тюремного заключения и явно криминализируя DDoS-атаки, что в то время правительство считало неясным.

«Сегодня я объявляю, что в этом году мы объявляем запрос на получение информации о Законе», - продолжил Патель. «Я призываю всех вас высказать свои открытые и честные взгляды на обеспечение того, чтобы наше законодательство и

полномочия продолжали отвечать вызовам, создаваемым угрозами киберпространству».

Обещание Пателя представляет собой победу кампании CyberUp, которая в течение последних двух лет опиралась на правительство, чтобы внести поправки в CMA и привести его в соответствие с современными требованиями. Первоначально принятый как не совсем безумный ответ на взлом принца Филиппа Престеля в конце 1980-х, этот закон не является популярным вариантом для полиции или прокуратуры, несмотря на то, что на первый взгляд криминализирует большинство современных компьютерных шалостей.

Эд Парсонс, старший помощник консультанта в F-Secure, которая поддерживает кампанию CyberUp по реформированию CMA, сказал The Register : «Я приветствовал бы официальный пересмотр Закона о неправомерном использовании компьютеров и призвал бы министра внутренних дел рассмотреть предлагаемые реформы, изложенные в статье. в прошлогоднем отчете сети «Реформа уголовного права».

«В обзоре следует широко рассмотреть способы борьбы с киберпреступностью, включая помощь британским компаниям в области кибербезопасности в защите людей и организаций и решении проблемы нехватки отраслевых навыков».

Все боятся нарушить его при выполнении своей работы - даже полиция

Правовая комиссия, правительственный орган по реформированию законодательства, в октябре 2020 года опубликовала отчет об ордерах на обыск, в котором подчеркиваются опасения полиции по поводу нарушения CMA при расследовании онлайн-преступлений. В этом отчете [PDF] рекомендуется реформировать закон по трем причинам:

Первая причина согласуется с наблюдением, сделанным Обществом юристов и которое мы поддержали в другом месте: как для человека, на которого распространяется ордер, так и для следователей было бы полезно иметь ясность в отношении имеющихся полномочий и их степени.

Вторая причина заключается в том, что ограничения на использование власти могут быть четко сформулированы в ее законодательной формулировке.

Третья и более конкретная причина заключается в том, что без законных полномочий следователь может совершить преступление в соответствии с Законом о неправомерном использовании компьютеров 1990 года, обыскав электронное устройство.

Патель также пообещал бороться с «сексуальным насилием над детьми в Интернете», сообщив, что только за это гнусное преступление за последний год было арестовано 800 человек. Примечательно, однако, что она не повторила свои предыдущие атаки на сквозное шифрование, чего многие ожидали, учитывая враждебное отношение британского правительства к этой технологии.

Программы-вымогатели - это плохо, и вы не должны расплачиваться с преступниками

Министр внутренних дел также предпринял прямую атаку на компании, которые платят преступникам-вымогателям в надежде расшифровать их данные и

предотвратить публикацию коммерческих секретов, личных данных сотрудников и т. Д.

«Правительство занимает твердую позицию против выплаты выкупа преступникам, в том числе в случаях, когда они становятся жертвами программ-вымогателей», - сказал сегодня Патель.

Выплата выкупа в ответ на программу-вымогатель не гарантирует успешного результата. Вы не защитите сети от будущих атак и не предотвратите возможность будущей потери данных. Фактически, выплата выкупа может способствовать дальнейшему развитию преступности.

Осуждение Пателя прозвучало вскоре после того, как многонациональная рабочая группа по программам-вымогателям, государственно-частное подразделение американского Института безопасности и технологий, указала в отчете [PDF], что средства для выкупа «могут быть использованы для распространения оружия массового уничтожения. торговля людьми и другая опасная глобальная преступная деятельность ". Тем не менее, целевая группа, в частности, не рекомендовала глобальный запрет на выплаты выкупа.

Тема горячая: многие предприятия, опасаясь нормативных актов и негативной огласки, тихо платят и надеются, что никто этого не заметит, а также молятся, чтобы преступники не вернулись за вторым кусочком вишни.

Бывший глава NCSC Кьяран Мартин оценил осуждение Пателем платежей программ-вымогателей как «значимое и желанное».

На прошлой неделе российская банда вымогателей заставила операторов крупного американского нефтепровода закрыть его в качестве меры предосторожности. Фирма Infosec Secureworks сообщила The Register, что она отследила 81 так называемую атаку "имя и позор" со стороны базирующейся в России преступной группировки, которая произвела некоторое волнение в более широком мире информационной безопасности из-за публикации сайта по связям с общественностью. Среди прочего, группа, которая называет себя DarkSide, использовала этот сайт, чтобы сегодня заявить, что его цель - «зарабатывать деньги, а не создавать проблемы для общества».

«Если злоумышленники поймут, что чистое вымогательство на основе украденных данных так же прибыльно, как сегодня шифрованные программы-вымогатели, то это кардинально меняет правила игры. Вспышка, позволяющая выбирать между первоначальным взломом и операционным успехом (для злоумышленника), теряется от нескольких дней до часов или даже минуты», - размышлял мрачный Барри Хенсли, главный разведчик по угрозам Secureworks». ***(Gareth Corfield. UK's Computer Misuse Act to be reviewed, says Home Secretary as she condemns ransomware payoffs // The Register (https://www.theregister.com/2021/05/11/computer_misuse_act_review_priti_patel/). 11.05.2021).***

***

«Президент Федерального ведомства по по безопасности в сфере информационной техники (BSI) Арне Шёнбом (Arne Schönbohm) считает, что угрозы возможных манипуляций на намеченных на сентябрь выборах в

бундестаг будут выше, чем ранее. Об этом он заявил во время онлайн-пресс-конференции во вторник, 25 мая. По его словам, это, в частности, связано и с пандемией коронавирусной инфекции, приведшей к резкому росту общения в интернете, а, следовательно, и возможности влиять на мнения людей.

Говоря о киберугрозах, он сослался на опыт других стран, например, с ситуацией вокруг взлома электронной почты предвыборной команды Эммануэля Макрона во Франции или попытками манипуляции во время президентской избирательной кампании в США. Нечто подобное «может оказаться привлекательным для реализации и в Германии как самой мощной экономической державе в Европе», - указал Шёнбом. По его словам, уже наблюдается определенные индикаторы, что заставляет BSI быть чрезвычайно бдительным. «Мы имеем дело с ситуацией комплексных угроз», - подчеркнул Шёнбом.

Глава ведомства кибербезопасности озвучил несколько возможных сценариев. Хакеры могут попытаться завладеть аккаунтами кандидатов в бундестаг и опубликовать на них ложную информацию. Некоторые похищенные данные могут быть также опубликованы, но в неподходящее время. Они также могут быть перемешаны с другой информацией, что не позволит оценить правильность тех или иных утверждений. Следовательно, подчеркнул Шёнбом, должна быть усилена интернет-безопасность будущих кандидатов.

Цель - посеять сомнения в итогах выборов

Глава федерального статистического ведомства, руководитель федеральной избирательной комиссии Георг Тиль (Georg Thiel) также готовится к возможным кампаниям дезинформации. Цель этих мероприятий, заявил он, посеять сомнения в результатах выборов. В качестве примера он привел возможные ложные сообщения о преждевременном закрытии избирательных участков. Комиссия готова к таким инцидентам и при необходимости сможет принять контрмеры.

Тиль также упомянул о более высоком числе избирателей, которые, в связи с продолжающейся пандемией, могут захотеть проголосовать по почте. Это создаст некоторые дополнительные проблемы при подготовке к выборам. Но, по его словам, нет никакой информации, что результаты голосования по почте, использующееся в стране с 1956 года, могут быть каким-либо образом подделаны». ***(Виталий Кропман. Германское ведомство кибербезопасности предупреждает об угрозах выборам в ФРГ // Deutsche Welle (https://www.dw.com/ru/germanskoe-vedomstvo-kiberbezopasnosti-preduprezhdaet-ob-ugrozah-vyboram-v-frg/a-57660332). 25.05.2021).***

***

«Законодательный процесс для Второго закона о повышении безопасности систем информационных технологий (Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, «Закон о безопасности ИТ 2.0») завершен.

После подписания Федеральным президентом Германии и публикации в Федеральном вестнике законов большая часть Закона вступит в силу завтра (28 мая 2021 года). С принятием Закона об ИТ-безопасности 2.0 был обновлен Первый акт по повышению безопасности систем информационных технологий, чтобы

повысить кибернетическую и информационную безопасность на фоне все более частых и сложных кибератак и продолжающейся цифровизации повседневной жизни.

Из-за ужесточения обязательств по обеспечению ИТ-безопасности и увеличения штрафов, в частности, многочисленных поправок к основному закону Германии об ИТ-безопасности - Закону о Федеральном ведомстве по информационной безопасности (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz), « BSI действовать") - актуальны как для операторов критической инфраструктуры, уже подпадающих под действие Закона о BSI, так и для (i) компаний, работающих в области утилизации бытовых отходов, (ii) производителей ИТ-продуктов, используемых в критических инфраструктурах, и (iii) так называемые компании, представляющие особый общественный интерес.

Кого коснутся поправки к Закону о BSI?

Расширенная сфера применения Закона о BSI является одним из основных изменений, произошедших в Законе о безопасности ИТ 2.0:

В дополнение к критическим секторам, уже закрепленным в Законе о BSI (энергетика, информационные технологии и телекоммуникации, транспорт и дорожное движение, здравоохранение, вода, продукты питания, а также финансы и страхование), в настоящее время существует еще один сектор, а именно сектор утилизации бытовых отходов. входит в сферу регулирования Закона о BSI. Важнейшей услугой в этом секторе является удаление бытовых отходов.

Поставщики, то есть производители критически важных компонентов, также будут нести определенные обязательства - это предназначено для защиты всей цепочки поставок. Критические компоненты - это ИТ-продукты (i), которые используются в критических инфраструктурах; (ii) нарушение доступности, целостности, аутентичности и конфиденциальности может привести к отказу или значительному ухудшению функциональности критически важных инфраструктур или угрозам общественной безопасности; и (iii) которые на основании закона в отношении этого положения обозначены как критический компонент или выполняют функцию, обозначенную как критическую на основании закона.

«Компании, представляющие особые общественные интересы » - это совершенно новая категория в дополнение к критически важным инфраструктурам. Сюда входят компании, которые не являются операторами критических инфраструктур и которые:

№ 1. - производят или разрабатывают товары в соответствии с Разделом 60 п. 1 шт. 1 и 3 Постановления о внешней торговле и платежах Германии (Außenwirtschaftsverordnung (AWV)) (производители оборонной продукции, а также производители ИТ-продуктов для обработки секретной государственной информации)

№ 2. - с точки зрения добавленной стоимости на внутреннем рынке, являютсясреди крупнейших компаний Германии и, следовательно, имеют большое экономическое значение для Федеративной Республики Германии, или которые имеют существенное значение для таких компаний в качестве поставщиков из-за их уникальных торговых предложений (кто явно должен подпадать под эту

категорию, будет указан - как в случае критических инфраструктур - посредством постановления) или

№ 3. - операторы предприятий высшего уровня в значении Постановления об опасных происшествиях (Störfall-Verordnung) или эквивалентны таким операторам в соответствии со статьей 1 пункт 2 Постановления об опасных происшествиях.

Какие новые обязательства по ИТ-безопасности будут введены?

Закон об ИТ-безопасности 2.0 дополняет обязательства, уже существующие в соответствии с Законом BSI, и вводит новые обязательства:

1.) Для операторов критических инфраструктур это касается, в частности, следующих новых обязательств:

Обязательство зарегистрировать критическую инфраструктуру в Федеральном ведомстве по информационной безопасности («BSI») : в дополнение к уже существующему обязательству операторов критических инфраструктур назначать контактную точку для критически важной инфраструктуры, с которой они работают, с которой можно связаться в любое время, Обязательство по регистрации критически важной инфраструктуры теперь прямо закреплено в Законе о BSI.

Обязательство использовать системы обнаружения атак : конкретизировано обязательство операторов критических инфраструктур принимать соответствующие организационные и технические меры, которые имеют решающее значение для функциональности критических инфраструктур, которыми они управляют (см. Раздел 8a Закона BSI). Это обязательство теперь также явно включает использование систем обнаружения атак, которые должны быть самыми современными.

Обязательство предоставить документы, необходимые для оценки с точки зрения BSI, и предоставить информацию: в связи с этим новым обязательством BSI может, например, запросить информацию о показателях, относящихся к соответствующим пороговым значениям, если факты оправдывают предположение, что оператор не выполняет свои обязательства по регистрации.

Обязательство раскрыть информацию, необходимую для управления нарушением : во время значительного нарушения BSI может, по согласованию с соответствующим компетентным федеральным надзорным органом, потребовать, чтобы затронутые операторы критических инфраструктур или компании, представляющие особый общественный интерес, передали информацию, включая личные данные, необходимые для управления нарушением.

Обязательства в связи с использованием критических компонентов : Оператор критической инфраструктуры также несет обязательства, связанные с использованием критических компонентов.

Закон 2.0 об ИТ-безопасности вводит, с одной стороны, обязанность операторов критически важных инфраструктур уведомлять Федеральное министерство внутренних дел, строительства и местного самоуправления (BMI) о планируемом первом использовании критически важного компонента до его использовать.

С другой стороны, оператор критической инфраструктуры обязан получить в декларацию от производителя критических компонентов ее надежности (так

называемая гарантия декларации). Только после получения такой гарантийной декларации оператор критической инфраструктуры может использовать критические компоненты. Это заявление должно быть приложено к уведомлению BMI.

На основании уведомления, описанном выше, и гарантийной декларации, ИМТ проводит априорный и экс-пост экспертизы в отношении использования критических компонентов и может запретить на плановое начальное или дальнейшее использовании критически важный компонент Vis-a- в отношении оператора критической инфраструктуры по согласованию с соответствующими министерствами, перечисленными в Законе BSI, и Федеральным министерством иностранных дел или издают приказы, « если (дальнейшее) использование может нанести ущерб общественному порядку или безопасности Федеративной Республики Германии ». Следует отметить, что запрет на дальнейшее использование важного компонента производителя может иметь дополнительные последствия для производителя.

2.) В соответствии с вышеописанным обязательством операторов критических инфраструктур использовать критические компоненты только тех производителей, которые предоставили декларацию о своей надежности оператору критической инфраструктуры, производители должны (должны) выдать соответствующие гарантийные декларации на -а-по отношению к оператору критической инфраструктуры по всей цепочке поставок.

3.) Обязательства, применимые к операторам критических инфраструктур, должны быть распространены в несколько измененной форме на другие секторы экономики, компании, представляющие особые общественные интересы. Обязательства компаний в интересах обществаразличаются в зависимости от категории, к которой принадлежит такая компания : обязательства, которые должны быть возложены на компании, подлежащие регулированию в соответствии с Постановлением об опасных инцидентах, не столь обширны, как обязательства производителей оборонной продукции и производителей ИТ-продуктов по обработке секретной государственной информации, а также компании, которые по своей внутренней добавленной стоимости входят в число крупнейших компаний в Германии и, следовательно, имеют большое экономическое значение для Федеративной Республики Германии, или которые имеют важное значение для таких компаний в качестве поставщиков из-за их уникальности. торговые предложения.

Каковы возможные последствия нарушения обязательств по ИТ-безопасности в связи с поправками к Закону о BSI?

Каталог положений о штрафах был полностью переработан : для лучшего исполнения были уточнены правонарушения, подлежащие наложению штрафов, особенно обязательства по предоставлению информации и доказательств, и были значительно расширены в соответствии с вновь введенными обязательствами, описанными выше.

Например, административное правонарушение было введено для тех операторов критически важных инфраструктур, которые не обеспечивают постоянную доступность к назначенному контактному лицу или - в случае

квалификации в качестве компании, представляющей особые общественные интересы, в соответствии с Разделом 2 пункт 14 предложение 1 шт. 1 и 2 Закона о BSI - не подавать самодекларацию, не подавать правильно, не подавать полностью или не подавать вовремя.

Сами штрафы были резко увеличены для достижения управляющего эффекта, как указано в обосновании закона. Вместо штрафов в размере до 100000 евро или до 50000 евро, возможных в соответствии с предыдущим Законом BSI, административные правонарушения теперь могут - в зависимости от случая - наказываться штрафом в размере (i) до 2000000 евро, (ii) до 1000000 евро, (iii) до 500000 евро или (iv) до 100000 евро.

Какие новые задачи будут поставлены перед BSI?

Закон о безопасности ИТ 2.0 также расширяет роль BSI. Перед BSI поставлено несколько новых задач, в том числе следующие:

Выполнение задач и полномочий BSI как национального органа по сертификации кибербезопасности в соответствии со статьей 58 Регламента (ЕС) 2019/881 от 17 апреля 2019 года будет включено в каталог задач BSI.

Чтобы принять во внимание растущее значение кибернетической и информационной безопасности для потребителей, особенно из-за растущей взаимосвязанности частных домохозяйств и распространения подключенных потребительских товаров, защита потребителей и информация для потребителей в области безопасности информационных технологий будут установлены как дополнительная задача BSI.

Кроме того, правомочность BSI по разработке спецификаций, а также окончательной оценке процедур идентификации и аутентификации с точки зрения информационной безопасности будет уточнена законом.

Учитывая растущее объединение ИТ-продуктов в сеть и необходимость соответствующих требований к ИТ-безопасности с целью защиты потребителей, компетенция BSI для разработки требований и рекомендаций вместе с тестированием и подтверждением соответствия для ИТ-продуктов, в частности, в форме технических руководств, четко указано.

Новые положения дополнительно обуславливают полномочия BSI иметь возможность запрашивать данные инвентаризации у поставщиков телекоммуникационных услуг, чтобы информировать тех, кто пострадал, об уязвимостях системы безопасности и атаках.

Для проверки наличия уязвимостей безопасности и других рисков безопасности в информационных технологиях Федерации и в информационных технологиях критических инфраструктур, цифровых услуг и компаний, представляющих особый общественный интерес, BSI имеет право проводить так называемые сканирование портов создано. Новый раздел 7b п. 4 нового закона BSI также оговаривает полномочия BSI использовать системы и процедуры для выполнения своих задач, которые имитируют успешную атаку, чтобы собирать и оценивать использование вредоносных программ или других методов атаки (так называемые приманки).

Наконец, BSI будет иметь право отдавать приказы поставщикам телекоммуникационных услуг и средств массовой информации для предотвращения конкретных угроз информационной безопасности.

Что изменилось с введением добровольного знака ИТ-безопасности?

Существующие полномочия BSI в соответствии с Законом BSI по предупреждению и консультированию пользователей продуктов в области безопасности информационных технологий дополняются новым положением о добровольном знаке безопасности ИТ. Знак безопасности ИТ наносится в виде этикетки на соответствующий продукт или на его внешнюю упаковку (если это возможно в зависимости от характера продукта) или публикуется в электронном виде и предназначен для ознакомления потребителей с ИТ-безопасностью продуктов и услуг. в сфере IT.

Знак безопасности ИТ не делает никаких заявлений о свойствах защиты данных продукта и может использоваться для продукта только в том случае, если BSI утвердил знак безопасности ИТ для этого продукта. Утверждение выдается по заявке производителя, если соблюдены требования, указанные в Законе BSI в отношении знака безопасности ИТ, и предоставляется только для продуктов тех категорий, для которых BSI уже ввел знак безопасности ИТ путем публичного объявления.

Перспективы

Закон об ИТ-безопасности 2.0 налагает ряд новых далеко идущих обязательств на операторов критически важных инфраструктур, которые требуют тщательного планирования и своевременной реализации. При оценке того, когда и как внедрить новые требования, следует также учитывать текущие события в Европейском Союзе - Директива (ЕС) 2016/1148, касающаяся мер по обеспечению высокого общего уровня безопасности сети и информационных систем по всему Союзу (Директива NIS) в настоящее время пересматривается.

Согласно Предложению о директиве о мерах по обеспечению высокого общего уровня кибербезопасности в ЕС (так называемая Директива NIS 2), опубликованном 16 декабря 2020 года, в частности, список секторов и видов деятельности, подпадающих под обязательства по кибербезопасности, должен быть расширен., а также юридические обязательства по обеспечению безопасности и отчетности должны быть в большей степени согласованы. Оба набора правил содержат похожие и связанные требования к ИТ-безопасности. Скоординированная реализация с учетом существующих и планируемых будущих требований может значительно ограничить (финансовые) усилия. Кроме того, на национальном уровне постановление об определении критических инфраструктур в настоящее время дорабатывается - в соответствии с текущим проектом, в частности, должны быть введены новые определения и пороговые значения для критических инфраструктур». ***(Natallia Karniyevich, Fabian Niemann. The German IT Security Act 2.0 comes into force – Overview of the most significant changes to the BSI Act // Bird & Bird (https://www.twobirds.com/en/news/articles/2021/germany/the-german-it-security-act-2-0-comes-into-force). 27.05.2021).***

***

«Второй проект Закона КНР о безопасности данных («Второй проект DSL») был выпущен 29 апреля 2021 года для общественного обсуждения. Период консультаций продлится до 28 мая 2021 года. Как обсуждалось в нашей предыдущей статье о первом проекте DSL («Первый проект DSL»), выпущенном в июле 2020 года, Закон о безопасности данных («DSL») вместе с Персональными данными Закон о защите («PIPL»), представляет собой два наиболее важных и долгожданных закона в области защиты данных, которые будут обнародованы. высшим законодательным органом Китая в ближайшее время.

Хотя второй проект DSL не внес радикальных изменений в первый проект DSL, некоторые изменения, тем не менее, значительны. Учитывая, что большинство китайских законов, как правило, будет проходить не более трех раундов чтения законодательным органом, Второй проект DSL будет важным индикатором того, в какой степени будут приняты положения текущего проекта. В этом информационном бюллетене мы резюмируем ключевые изменения, изложенные во втором проекте DSL.

1. Каталог "важных данных" на уровне государства

Как обсуждалось в нашей предыдущей статье, первый проект DSL представляет собой «скелет» многоуровневой системы безопасности данных, в то время как параметр «важные данные» в такой системе оставлен для рассмотрения местными регулирующими органами. В отличие от Первого проекта DSL, статьи 20-21 Второго проекта DSL предусматривают, что каталог «важных данных» должен быть составлен государством, в то время как региональные и отраслевые регулирующие органы будут выпускать конкретные каталоги важных данных, применимых к соответствующим секторам и отраслям. Этот единый подход на государственном уровне, в случае его окончательного принятия, будет приветствоваться организациями, поскольку каталоги после публикации помогут определить с потенциально большей правовой определенностью и согласованностью, будут ли их обработка данных включать "важные данные" в Китае.

2. Акцент на реализации MLPS

В статье 26 Второго проекта DSL подчеркивается, что комплексная система управления безопасностью данных должна быть создана на основе многоуровневой схемы защиты («MPLS»), которая является важным набором требований к безопасности данных, закрепленных в статье 21 Закона о кибербезопасности. («CSL»). Фактически, с момента вступления в силу CSL в 2017 году регулирующие органы выпустили ряд правил и руководств по MLPS, и компании были наказаны за несоблюдение MLPS. Делая акцент на MPLS, Второй проект DSL усиливает ужесточающуюся тенденцию в обеспечении реализации MLPS. Компаниям рекомендуется самостоятельно проверять, существует ли какой-либо пробел в соблюдении этих требований законодательства.

3. Расширены правила трансграничной передачи данных.

Что касается трансграничной передачи важных данных (которая не обсуждалась в Первом проекте DSL, несмотря на долгожданные ожидания),

недавно добавленная статья 30 Второго проекта DSL устанавливает отдельную основу для трансграничной передачи «важных данных» посредством Операторы критически важной информационной инфраструктуры («CIIO») и не-CIIO, при этом первые соблюдают правила, установленные в соответствии с CSL, а вторые - отдельные правила, которые должны быть опубликованы Администрацией киберпространства Китая («CAC») и Государственным советом.

Как поясняется в законодательной записке, расширенный объем важных ограничений на экспорт данных из CIIO в не-CIIO призван удовлетворить практические потребности в надзоре за безопасностью данных. Это перекликается с более строгими требованиями к экспорту данных в рамках проекта мер по оценке безопасности экспорта данных и проекта мер по управлению безопасностью данных, выпущенных в 2017 и 2019 годах соответственно. Однако в отсутствие каких-либо дополнительных разъяснений по важным правилам экспорта данных, относящимся к организациям, не связанным с CIIO, предприятия, скорее всего, столкнутся с правовой дилеммой, когда их экспорт важных данных может быть подвержен значительной юридической неопределенности.

4. Повышенный штраф

Статья 44 Второго проекта DSL значительно усиливает наказание за нарушение обязательств по безопасности данных в следующих трех аспектах:

во-первых, максимальный размер штрафов для предприятия за нарушение обязательств по обеспечению безопасности данных увеличился с 1 миллиона юаней (примерно 156 000 долларов США) до 5 миллионов юаней (примерно 780 000 долларов США), а максимальный размер штрафов для лиц, непосредственно ответственных за нарушение, увеличился. от 100 000 юаней (приблизительно 15 600 долларов США) до 500 000 юаней (приблизительно 78 000 долларов США);

во-вторых, в то время как Первый проект DSL налагает личную ответственность только на «непосредственно ответственных управленческих лиц», Второй проект DSL дополнительно расширяет личную ответственность на «других непосредственно ответственных лиц», предлагая не только сотрудники, занимающие руководящие должности, но и другие сотрудники также могут нести личную ответственность; а также

в-третьих, Второй проект DSL добавляет дополнительные категории штрафов за серьезное нарушение: предприятию может быть приказано приостановить его бизнес, приостановить бизнес для исправления или отозвать его разрешение или бизнес-лицензию в случае отказа принять корректирующие меры или вызвало утечка большого количества данных и другие серьезные последствия.

Помимо вышеизложенного, Второй проект DSL включает два новых подпункта в отношении штрафа за предоставление данных, но с разных точек зрения: предприятия будут наказаны за отказ сотрудничать с властями КНР в отношении запросов на доступ к данным, а также будут наказаны за несанкционированный доступ. предоставление данных в правоохранительные органы зарубежных стран без согласования с властями КНР.

Наблюдение

Во втором проекте DSL подчеркивается, что «защита данных» в Китае выходит за рамки защиты личных данных, и очень важно также учитывать защиту

«важных данных». В целом, Второй проект DSL отреагировал на некоторые ключевые и горячие вопросы и ужесточил положения Первого проекта DSL, о чем свидетельствуют, например, дальнейшие правила экспорта «важных данных» как СІІО, так и другими организациями. -СІІО, усиленные штрафы и ужесточенные ограничения на предоставление данных зарубежным правоохранительным органам. Тем не менее, остаются нерешенными некоторые вопросы, например: отсутствие правил экспорта «важных данных», в частности для не-СІІО. Хотелось бы получить дальнейшие разъяснения, которые позволят компаниям понять и соблюдать новый закон, похоже, что окончательный вариант DSL появится в ближайшее время». ***(Michelle Chan, Clarice Yue, Sharon Zhang, Tiantian Ke. Coming soon? The Second Draft of the PRC Data Security Law Released // Bird & Bird (https://www.twobirds.com/en/news/articles/2021/china/the-second-draft-of-the-prc-data-security-law-released). 15.05.2021).***

***

Російська Федерація та країни ЄАЕС

«Минцифры России сообщает об открытии киберполигона на базе Сибирского государственного университета телекоммуникаций и информатики (г. Новосибирск). Университет стал первым подведомственным вузом министерства, на базе которого создана виртуальная структура для отражения кибератак.

«Сибирский государственный университет телекоммуникаций и информатики, который является подведомственным вузом Минцифры, открыл свой киберполигон. Такие площадки уже развернуты в двух вузах: на острове Русский на базе Дальневосточного федерального университета и в Сочи на базе Научно-технологического университета «Сириус». На киберполигоне студенты изучают различные сценарии кибератак, тренируются отражать их, обеспечивая надежную защиту ИТ-инфраструктуры виртуальных предприятий. В будущем такие тренировки помогут обеспечить информационную безопасность всей страны», – сообщил врио директора департамента информационной безопасности Минцифры России Дмитрий Реуцкий.

Киберполигон СибГУТИ представляет мультифункциональный цифровой комплекс для тестирования техники и программного обеспечения, повышения грамотности в области информационной безопасности и цифровых технологий.

Планируется открытие удаленных площадок киберполигона в колледже телекоммуникаций СибГУТИ и филиалах университета в Улан-Удэ, Хабаровске и Екатеринбурге.

«Киберполигон СибГУТИ открывает новые возможности по обучению и тренировке ключевых навыков специалистов, занятых в реализации федеральных проектов национальной программы «Цифровая экономика Российской Федерации», – говорит исполняющий обязанности ректора СибГУТИ Бари Хаиров.

Национальный киберполигон – один из крупнейших проектов по информационной безопасности, реализуемых в рамках программы «Цифровая

экономика». Киберполигон представляет виртуальную копию инфраструктуры компаний различных отраслей. Он позволяет отрабатывать практические навыки по работе с современными средствами защиты информации и реагированию на кибератаки, что важно, в том числе, при подготовке молодых специалистов по информационной безопасности.

Запуск и эксплуатация сегментов киберполигона входит в список мероприятий федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика». Виртуальная площадка создается силами «Ростелекома» с привлечением экспертизы сотрудников его дочерней компании «Ростелеком-Солар».

«Развитие сети опорных центров национального киберполигона – один из важнейших аспектов проекта. Они дают будущим специалистам возможность получения практических навыков, тем самым способствуя развитию отрасли в целом и решая задачу государства по созданию кадрового резерва в сфере информационной безопасности», – подчеркнул заместитель генерального директора «Ростелеком-Солар» Александр Чечин». ***(Владимир Бахур. Подведомственный вуз Минцифры открыл киберполигон // CNews (https://www.cnews.ru/news/line/2021-05-17_podvedomstvennyj_vuz_mintsifry). 17.05.2021).***

***

«Киберпреступники с 2017 г. успешно взламывали сети федеральных органов исполнительной власти России (ФОИВ), оставаясь при этом незамеченными. Об этом CNews сообщили представители Национального координационного центра по компьютерным инцидентам (НКЦКИ) и компании «Ростелеком-Солар», дочерней структуры «Ростелекома».

Наибольшую активность, по данным НКЦКИ, хакеры развили в 2020 г. – согласно статистике, рост числа атак на субъекты критической информационной инфраструктуры (КИИ) в этом году превысил 40% по сравнению с показателями 2019 г. По данным специалистов, наиболее часто используемые этими киберпреступниками методы – фишинг, атаки через подрядчика и взлом веб-приложений.

До 2020 г. хакеры никак не выдавали себя. Обнаружить их деятельность удалось лишь при попытке проведения ими в 2020 г. атаки на один из российских ФОИВов из списка клиентов центра противодействия кибератакам Solar JSOC («Ростелеком-Солар»). Специалисты, расследовавшие этот инцидент, выяснили, что он был лишь частью цепочки атак.

На момент публикации материала хакерская группировка, годами орудовавшая в сетях российских ФОИВов, раскрыта не была, то есть пока неизвестно, кто конкретно осуществлял взломы. Однако специалистам НКЦКИ и Solar JSOC удалось заблокировать ей доступ к атакуемым сетям.

«Главная опасность проправительственных кибергруппировок в том, что, обладая мощными техническими и материальными ресурсами, они способны довольно долго скрывать свое присутствие в инфраструктуре, обходя средства защиты и мониторинга и реализуя шпионаж в интересах другого государства», –

сказал CNews директор Solar JSOC Владимир Дрюков. «Без выстроенной системы контроля привилегированных пользователей и систем удаленного доступа такие атаки могут развиваться годами – совершенно незаметно для организации-жертвы», – добавил он.

Как хакеры «жили» в сетях ФОИВов

Обнаруженная экспертами в 2020 г. хакерская атака была тщательно спланированной. У хакеров был один основной канал доступа к инфраструктуре атакуемого ими ФОИВа и более 12 запасных на случай, если основная брешь будет закрыта. В списке были лазейки через веб-сервера, коллекция учетных записей с различными уровнями привилегий для удаленного доступа и др.

Помимо этого, в арсенале киберпреступников было 120 видов вредоносного ПО, написанных ими же, притом ни один из них не определялся современными антивирусами. «Со стороны группировки была выполнена огромная работа по изучению российской ИКТ (информационно-коммуникационные технологии – прим. CNews): адаптация вредоносного ПО под работу с российскими облачными сервисами с полным изучением их API, обход российских средств защиты», – сообщили CNews представители «Ростелеком-Солар».

На получение доступа к ключевым узлам сетей российских ФОИВов хакеры тратили в среднем около месяца. За этот срок они взламывали контроллер домена, открывая себе путь к учетным записям, и проникали в почтовые сервера, где могли читать рабочую переписку. Также они получали «доступ к точкам сопряжения с другими инфраструктурами, что и позволяло развивать атаку в другие организации или органы исполнительной власти», говорится в отчете «Ростелеком-Солар».

Как итог, в среднем за 30 дней у хакеров может появиться доступ, к примеру, к личной переписке первых лиц ФОИВа. Помимо этого, они могут скомпрометировать личные данные сотрудников взламываемого учреждения. «При этом для “зачистки” федеральной информационной инфраструктуры среднего размера от злоумышленников требуется более двух недель круглосуточной работы 70 специалистов ИТ- и ИБ-служб организации, сервис-провайдера и регулятора», – рассказали CNews представители «Ростелеком-Солар».

Излюбленные методы хакеров

Почти половина всех атак на сети ФОИВов (более 45%) начинается со взлома тех или иных приложений. В большинстве федеральных российских организаций (почти в 70%) веб-ресурсы содержат различные уязвимости, которые и используют хакеры. Киберпреступники начинают «исследовать» новые ресурсы, опубликованные на правительственном домене gov.ru, спустя всего два-три дня после их публикации.

Фишинговые рассылки стоят на втором месте по популярности у хакеров, атакующих ФОИВы. Эксперты Solar JSOC утверждают, что именно в органах госвласти этот метод показывает наиболее высокую эффективность в сравнении с другими сегментами экономики. По их подсчетам, отправленное мошенником фишинговое письмо открывает каждый четвертый госслужащий (в среднем по всей России – каждый седьмой сотрудник).

Третью строчку занимают атаки через различных подрядчиков. Этот метод требует со стороны хакеров больших трудозатрат в сравнении с предыдущими. Тем

не менее, в 2020 г. злоумышленники пересмотрели свое отношение к нему – по данным Solar JSOC, его «популярность» как метода атак на субъекты КИИ выросла более чем вдвое.

ИБ-специалисты не виноваты, причина в иностранных спецслужбах

Вице-президент «Ростелекома» по информационной безопасности Игорь Ляпунов прокомментировал хакерскую атаку, позволившую обнаружить присутствие хакеров. «Однажды ночью при обеспечении мер безопасности один из наших инженеров обнаружил попытки «прикосновения» к серверу заказчика. Следы хакеров исчезли в течение нескольких минут, но этого было достаточно для понимания происходящего. <…> Мы не можем сказать, что кто-то из ИБ-специалистов плохо работал. Условно говоря, безопасники готовились к боксёрскому поединку, а когда вышли на ринг, увидели танк. Настолько неожиданны угрозы нового типа», – сообщил он порталу «Экспертный центр электронного государства».

По словам замдиректора НКЦКИ Николая Мурашова, скомпрометировавшая хакеров атака характеризовалась «высоким уровнем примененных в ней технических средств». Он добавил, что эта атака отражала «явную тенденцию последних двух лет», заключающуюся в росте активности высококвалифицированных группировок в отношении российских ФОИВов и субъектов КИИ.

«При этом уровень злоумышленника, которому приходится противостоять владельцам государственных информационных систем – иностранные спецслужбы. Их целью является, как правило, компрометация ИТ-инфраструктуры и кража конфиденциальных данных госорганов и учреждений, а мотивом – действия в интересах иностранных государств», – сообщил CNews Николай Мурашов». ***(Эльяс Касми. Коварные заграничные хакеры годами взламывали сети органов власти России и оставались незамеченными // CNews (https://www.cnews.ru/news/top/2021-05-20_kovarnye_inostrannye_hakery). 20.05.2021).***

***

Австралія

«Правительство Австралии решило ввести основы кибербезопасности в учебный план с первых классов школы…

Для начала пятилетним первоклассникам расскажут, что такой информацией, как дата рождения или полное имя, нельзя делиться с незнакомыми людьми. Также детям объяснят, что перед тем, как ввести личные данные в сеть, необходимо обсудить это с родителями или родными.

Ученики следующих двух классов освоят навыки использования логинов и паролей, их проинформируют об основных опасностях в интернете.

В четвертом и пятом классах детей будут учить определять, какая информация считается личной и может помочь идентифицировать жертву злоумышленнику.

Сейчас над образовательной программой работают». ***(Австралия вводит уроки кибербезопасности для самих младших школьников // Укринформ (https://www.ukrinform.ru/rubric-yakisne-zhyttia/3240419-avstralia-vvodit-uroki-kiberbezopasnosti-dla-samih-mladsih-skolnikov.html). 05.05.2021).***

***

«Важность того, чтобы австралийские компании были «киберподготовлены» и «киберустойчивы», чтобы защитить себя, свои информационные активы и своих клиентов от киберрисков, вызывает повышенное внимание и вызывает повышенное беспокойство. Правительство Австралии обязалось в рамках Стратегии кибербезопасности 2020 (Стратегия) Австралии инвестировать 1,67 миллиарда долларов в течение 10 лет для создания более безопасного и безопасного онлайн-мира для австралийцев. В Стратегии говорится, что эти инвестиции будут обеспечены за счет действий правительств по усилению киберзащиты от сложных угроз, со стороны бизнеса, чтобы защитить их от известных уязвимостей, и со стороны сообщества, чтобы практиковать безопасное поведение в Интернете (см. Нашу сводную статью: Стратегия кибербезопасности Австралии 2020: Что нужно знать).

Стратегия устанавливает (в параграфе 36), что для достижения этой цели рассматривается множество вариантов реформ, включая «роль законов о конфиденциальности, защите прав потребителей и данных; обязанности директоров компаний и других субъектов хозяйствования; и обязательства перед производителями и устройствами, подключенными к Интернету». В соответствии со Стратегией правительство уже предложило ряд законодательных поправок для повышения устойчивости системы конфиденциальности и кибербезопасности Австралии в отношении Закона о конфиденциальности 1988 г., Закона о безопасности критически важной инфраструктуры 2018 г. и Добровольного кодекса практики Интернета вещей. Намерено ли правительство продолжить регуляторную реформу, еще предстоит определить, однако недавнее мнениев Австралийском финансовом обзоре (AFR) сообщается, что:

эксперты по безопасности данных и рискам сформировали мнение, что реформа будет представлять собой существенные поправки к Закону о корпорациях 2001 (Cth) (Закон о корпорациях) и обязанностям директоров с введением обязательств в отношении кибербезопасности; а также форма таких поправок может обязывать все австралийские компании ASX 200 применять меры информационной безопасности, аналогичные требованиям, предъявляемым к организациям, регулируемым Австралийским органом пруденциального регулирования (APRA) в соответствии с его пруденциальным стандартом CPS 234.

Существующие обязательства в отношении кибербезопасности

Если AFR верен в этом предположении, введение обязательств по кибербезопасности, аналогичных обязательствам по CPS 234, будет иметь значительные последствия для высшего руководства, руководящих органов и советов более широкого круга компаний, а также введение минимальных требований в отношении информационной безопасности. Меры в соответствии с

Законом о корпорациях значительно увеличат обязанности директоров, особенно в отношении создания, поддержания и проверки средств защиты информации.

В настоящее время в соответствии с Законом о корпорациях директора несут ряд юридических обязанностей и обязанностей, связанных с управлением их компаниями. Большинство этих обязанностей являются широкими и касаются использования осторожности и осмотрительности, добросовестности и обеспечения того, чтобы директора не использовали информацию или свое положение ненадлежащим образом. Дополнительные обязанности, связанные с раскрытием интересов директоров и информации, недоступной рынку, также носят общий характер.

Ученые из бизнес-школы Сиднейского университета предположили, что обязательства директоров в соответствии с разделами 299, 299A и 300 Закона о корпорациях уже требуют, чтобы директора рассматривали и раскрывали киберриски своей компании в отчете своих директоров, однако эти обязательства не являются конкретно кибер-рисками. Поэтому риски, связанные с безопасностью и кибер-рисками, можно легко упустить из виду. Таким образом, для большинства крупных компаний раскрытие информации, требуемое в соответствии с приведенными выше разделами, вероятно, недостаточно для выполнения обязательств по CPS 234.

Что такое APRA CPS 234?

CPS 234 является пруденциальным стандартом и применяется к организациям, регулируемым APRA, включая банки, кредитные союзы и пенсионные фонды. Согласно CPS 234 субъекты, регулируемые APRA, должны принимать меры по управлению киберрисками для усиления своих возможностей информационной безопасности в отношении развивающихся угроз и защиты своих информационных активов.

Ключевые требования CPS 234 включают, что соответствующая организация:

внедрять и поддерживать средства защиты информации в ответ на изменения уязвимостей и угроз;

обеспечивать соблюдение CPS 234 третьей стороной, например субподрядчиками и другими организациями, которые управляют информацией от имени организации;

поддерживать структуру политики ИТ-безопасности, соизмеримую с подверженностью уязвимостям и угрозам;

внедрять и систематически тестировать соответствующие средства контроля информационной безопасности;

обеспечить надлежащее управление инцидентами, в том числе наличие надежных механизмов и планов для обнаружения инцидентов информационной безопасности и реагирования на них;

проводить внутренний аудит средств контроля информационной безопасности, включая анализ дизайна и эффективности;

внедрять процессы, обеспечивающие уведомление APRA о любых инцидентах, которые существенно влияют на клиентов, или о любых недостатках контроля, которые организация не может исправить своевременно.

Непрерывный анализ и совершенствование процедур и протоколов управления киберрисками организации лежит в основе обязательств по CPS 234 в контексте постоянно меняющегося киберпространства. CPS 234 ясно дает понять, что конечная ответственность за соблюдение нормативных требований лежит на Правлении. Для получения дополнительной информации о CPS 234 см. Наши статьи о CPS 234: 8 фактов, которые вы не знали о новом стандарте кибербезопасности APRA и Не забывайте - если у вас есть информационные активы, управляемые третьими сторонами, крайний срок для соответствия CPS 234 - 1 июля 2020 г.

Подготовка к возможным изменениям, подобным CPS 234

AFR предполагает, что, если будут предложены поправки к обязанностям директоров, они, скорее всего, будут реализованы во второй половине 2021 года.

Разработка и внедрение политик и значительных средств контроля информационной безопасности требует значительных затрат времени и инвестиций. APRA раскрыло, что многие из его регулируемых организаций все еще не в состоянии должным образом соблюдать CPS 234, несмотря на то, что прошло более 18 месяцев с момента вступления в силу стандарта, что подчеркивает необходимость значительного времени и ресурсов для адекватной реализации. Это особенно верно в отношении обязательств по обеспечению соблюдения третьей стороной CPS 234, когда информационные активы организации управляются третьей стороной, поскольку это требует согласования обязательств CPS 234 в контрактах третьей стороны с поставщиками, от которых в противном случае может не потребоваться соблюдать CPS 234.

Даже если поправки, предложенные AFR, не вступят в силу, все компании, независимо от их требований законодательства или любых возможных законодательных изменений, должны рассмотреть меры по защите себя и своих клиентов от киберрисков. Это по ряду причин. Во-первых, если у компании недостаточно мер информационной безопасности, существует значительный риск репутационного ущерба, который может возникнуть в результате серьезных утечек данных из-за снижения доверия клиентов, а во-вторых, даже если такие реформы не проводятся в соответствии с Законом о корпорациях, как это предлагается AFR, компаниям все еще может потребоваться подготовка к дальнейшим законодательным требованиям, которые могут быть наложены на них в ближайшем будущем, как указано в Стратегии.

В нынешней атмосфере повышенных киберрисков и увеличивающихся последствий инцидентов информационной безопасности все компании должны выстраивать свои процессы и процедуры кибербезопасности, чтобы эти процессы были соразмерны угрозам, с которыми сталкиваются компании. Руководствуясь передовой практикой, компаниям следует учитывать киберриски, с которыми они могут столкнуться, возможные меры по их снижению и учитывать изменения во внутренних политиках и методах, касающихся информационной безопасности, с упреждением, включая инвестирование в надежную защиту данных и средства контроля информационной безопасности, где это необходимо.

В качестве подготовительной меры крупным компаниям может быть полезно изучить CPS 234 и определить области, в которых уже достигнуто надлежащее

соответствие, выделить потенциальные области, которые необходимо улучшить, и соответствующим образом обновить свои структуры соответствия. Сейчас хорошо известно, что кибератаки и использование уязвимостей информационной безопасности коммерческих и государственных организаций становятся все более обычным явлением, а это означает, что риски безопасности для крупных компаний, таких как компании ASX 200, только возрастают. Хотя пока не известно, как правительство будет действовать в рамках Стратегии и реформировать «обязанности директоров компаний и других субъектов хозяйствования», учитывая время и инвестиции, необходимые для перехода крупных корпоративных структур к внедрению и поддержанию надежных средств контроля информационной безопасности, компаниям следует начать разработку комплексной дорожной карты кибербезопасности прямо сейчас. Будущие реформы обязанностей директоров компаний и хозяйствующих субъектов только укрепят это». ***(India Monaghan, Isobel O'Brien, Jen Bradley, Tim Gole. CPS 234-like cyber security obligations: Is your company prepared? // Gilbert + Tobin (https://www.gtlaw.com.au/insights/cps-234-cyber-security-obligations-your-company-prepared). 11.05.2021).***

***

«Постоянный комитет Австралийской столичной территории по вопросам правосудия и общественной безопасности изучает Закон о выборах 2020 года и Закон о выборах, охватывающий, среди прочего, системы электронного голосования.

Закон COVID-19 реагирования на чрезвычайные ситуации Законодательство Поправка 2020 введены временные поправки к Закону о выборах на выборах октября 2020 года. Сюда входило развертывание решения для электронного голосования за границей для правомочных избирателей ACT, которые находились за границей. Срок действия поправок истек в апреле.

На выборах 2020 года также использовалась территориальная система электронного голосования и подсчета голосов (EVACS), которая ранее использовалась на выборах 2004, 2008, 2012 и 2016 годов.

EVACS использует персональный компьютер для регистрации голоса. Эти участки для электронного голосования были также доступны на участках до голосования.

Обеспечение представления [PDF] в комитет была группа из четырех исследователей в области безопасности - с большим опытом работы в поиске дыр в избирательных системах - которые обратились в реализации, безопасность и прозрачность электронного голосования.

Они заявили, что выявили «серьезные проблемы» в точности и целостности выборов ACT, конфиденциальности голосов на выборах ACT и прозрачной демонстрации точности, честности и конфиденциальности голосов на выборах ACT.

«Секретные, неподдающиеся проверке системы, подобные тем, которые использовались на выборах ACT 2020, позволяют относительно легко изменять зарегистрированный список поданных голосов таким образом, чтобы наблюдатели

не могли этого заметить», - заявили они. «Это также увеличивает вероятность того, что случайные ошибки останутся незамеченными.

«Мы не утверждаем, что произошла коррупция или что система была разработана с учетом этой цели. Однако, конечно, были ошибки, не обнаруженные программой Elections ACT».

Доктор Эндрю Конвей, доктор Томас Хейнс, исполняющий обязанности профессора ANU Ванесса Тиг и Т. Уилсон-Браун сообщили об обнаружении трех ошибок в системе EVACS, которые потенциально могут изменить результаты выборов.

Во-первых, EVACS неправильно группирует голоса по передаваемой стоимости, не понимая, когда голоса заслуживают группировки, потому что они получили одинаковую передаваемую стоимость разными способами.

«В 2020 году это привело к тому, что некоторые подсчеты были ошибочными более чем на 20 голосов; в целом это могло вызвать гораздо большие расхождения», - добавили они.

Еще один недостаток - неправильное округление. Закон о выборах ACT прямо требует округления до шести десятичных знаков, но EVACS округляет до ближайших шести десятичных знаков.

В-третьих, группа заявила, что EVACS имеет некоторые другие неточности, которые соответствуют округлению значений перевода, несмотря на то, что это не указано в законодательстве.

«Это важно, потому что эффект трансфертной стоимости может быть умножен на тысячи голосов», - писали они. «Это вызывает ошибки порядка тысячных голосов и, возможно, может иметь значение в очень близкой гонке».

К счастью, сказали они, эти недостатки не повлияли на результат выборов 2020 года.

ACT использует четыре системы для обработки голосов: модуль электронного голосования EVACS, который работает на компьютерах на избирательных участках; Модуль сканирования бумажных бюллетеней EVACS, который сканирует и интерпретирует бумажные бюллетени, записывая результаты в электронном виде; система Интернет-голосования ACT (OSEV), которая принимает голоса из Интернета; а модуль подсчета EVACS подсчитывает голоса и выводит набор победивших кандидатов.

«Единственная система, которую мы смогли изучить, - это счетный модуль, и только потому, что мы можем сравнивать его входные данные с его выходными данными и находить ошибки, не видя кода», - заявили они.

«Мы считаем, что система Интернет-голосования является новой и что модули голосования, сканирования бумажных бюллетеней и подсчета были полностью переписаны с 2016 года. Но мы не можем быть уверены в этом, потому что не видели ни одного исходного кода 2020 года».

Группа попросила, чтобы код электронного голосования и системная документация были открыты за шесть месяцев до исследовательского сектора, чтобы можно было найти и исправить серьезные ошибки и уязвимости.

Они также попросили, чтобы у системы электронного голосования на месте была бумажная запись, подтверждаемая избирателями, чтобы избиратель мог

проверить неизменяемую запись голоса независимо от программного обеспечения; и что интернет-голосование будет прекращено из-за высокого уровня риска, связанного с нынешней технологией интернет-голосования». ***(Asha Barbaschow. Researchers found three flaws in ACT e-voting system that could affect election outcomes // ZDNet (https://www.zdnet.com/article/researchers-find-three-flaws-in-act-e-voting-system-that-could-affect-election-outcomes/). 12.05.2021).***

***

«Комиссия по уголовной разведке Австралии (ACIC) считает, что у законопослушного члена сообщества нет законных оснований для владения или использования зашифрованной коммуникационной платформы.

«Эти платформы используются почти исключительно группами SOC [серьезной и организованной преступности] и разработаны специально для сокрытия личности вовлеченных преступных групп и обеспечения возможности избежать обнаружения правоохранительными органами», - заявила ACIC. «Они позволяют пользователю общаться в закрытых сетях, чтобы облегчить изощренную преступную деятельность».

Комментарии были сделаны в представлении [PDF] в Объединенный парламентский комитет по разведке и безопасности (PJCIS) в рамках его расследования законопроекта о внесении поправок в законодательство о слежке (выявление и нарушение) 2020 года.

Он сообщил комитету, что намерен использовать полномочия, предоставленные ACIC в соответствии с законопроектом, чтобы сосредоточить усилия на понимании и сборе информации о группах SOC, которые используют зашифрованные коммуникационные платформы для сокрытия своей преступной деятельности.

В случае принятия законопроекта Федеральной полиции Австралии (AFP) и ACIC будут выданы три новых компьютерных ордера на борьбу с преступностью в Интернете.

Первый из ордеров - нарушение данных; второй - ордер на сетевую активность; и третий - ордер на захват аккаунта.

ACIC заявила, что закон позволит ей посредством сбора, оценки и распространения криминальной разведки и информации использовать национальные стратегии по борьбе с транснациональной серьезной и организованной преступностью.

«Для достижения этой цели полномочия и возможности ACIC должны идти в ногу с технологическими тенденциями и возникающими угрозами, чтобы агентство могло адекватно бороться с серьезной киберпреступностью и изощренными преступными группами с использованием зашифрованных платформ», - говорится в сообщении.

«Агентство должно иметь возможность поддерживать результаты правоохранительных органов, чтобы защитить австралийцев от наиболее изощренных и опасных субъектов, которые все чаще используют передовые коммуникационные технологии для маскировки своей преступной деятельности».

Согласно ACIC, содержащиеся в законопроекте полномочия по сбою, сбору разведывательной информации и захвату учетных записей дополняют существующие полномочия агентства, предоставляя новые возможности для сбора информации и реагирования на серьезные преступления, происходящие в Интернете, и для преступников с использованием специальных зашифрованных коммуникационных платформ.

«Меры в законопроекте основаны на том принципе, что полномочия, предоставленные парламентом органам, отвечающим за обеспечение соблюдения уголовного законодательства, не должны ослабляться достижениями в области технологий», - говорится в сообщении. «Законопроект призван предоставить ACIC и AFP возможность защищать австралийское сообщество от вреда в Интернете так же, как они защищают австралийцев в физическом мире».

ACIC считает, что законопроект устраняет пробелы в текущих полномочиях электронного наблюдения.

Предоставленные законопроектом ордера на сетевую активность «немедленно изменят способность ACIC выявлять и понимать серьезные преступные группы, использующие Dark Web и зашифрованные коммуникационные платформы для совершения серьезных преступлений и содействия их совершению».

«В настоящее время, хотя ACIC может обнаруживать преступное поведение на скрытом веб-сайте или в компьютерной сети, мы не можем идентифицировать всех лиц, участвующих в преступном поведении», - пояснил он. «По этой причине нам требуется возможность нацеливаться и проникать в сеть или класс компьютеров, в которых совершается преступление, чтобы члены преступной группы могли быть идентифицированы, а полный характер и масштабы преступности могли быть обнаружены с помощью сбор разведданных».

Между тем, ордера на нарушение данных позволят ACIC вмешиваться в данные, хранящиеся в онлайн-криминальных сетях или устройствах, чтобы помешать совершению серьезных уголовных преступлений.

«Это будет особенно действенно в контексте противодействия преступной деятельности, которая в основном происходит в Интернете», - говорится в сообщении.

Наконец, ордера на захват учетной записи, по его словам, позволят агентству взять под контроль онлайн-аккаунт в сочетании с другими следственными полномочиями, обозначив это как «эффективный метод для агентств проникновения в преступные сети онлайн».

«Это сыграет решающую роль в раскрытии личностей анонимных преступников, а также в сборе доказательств инициирования и совершения серьезных преступлений в Интернете, в том числе в Dark Web и там, где используются зашифрованные коммуникационные платформы», - говорится в сообщении». ***(Asha Barbaschow. ACIC believes there's no legitimate reason to use an encrypted communication platform // ZDNet (https://www.zdnet.com/article/acic-believes-theres-no-legitimate-reason-to-use-an-encrypted-communication-platform/). 06.05.2021).***

***

«Комиссар Австралии по электронной безопасности получил 21 миллион австралийских долларов в бюджете на 2021–2022 годы в начале этого месяца, причем финансирование будет распределено между программным обеспечением, дополнительным персоналом и продолжением его работы по борьбе с жестоким обращением с детьми с помощью технологий.

Поскольку премьер-министр Скотт Моррисон представляет недавний бюджет как «поддержку австралийских женщин», финансирование eSafety попадает под эту категорию.

«Женский онлайн-пакет» включает 15 миллионов австралийских долларов в течение двух лет для eSafety, чтобы расширить возможности расследования - наем еще 20 сотрудников в соответствии с ожидаемым принятием Закона о онлайн-безопасности - и 3 миллиона австралийских долларов на пилотное программное обеспечение.

Во время оценки сенатом в четверг комиссара по электронной безопасности Джули Инман Грант задали вопрос о сумме финансирования и попросили предоставить подробную информацию о технологии, которая еще не была оценена, учитывая, что объявление о бюджете было сделано всего за несколько недель до этого.

«3 миллиона австралийских долларов были выделены на пилотный проект… это то, о чем мы думали с 2017 года. В некоторых из самых вопиющих случаев, которые мы видели, к нам приходили люди с 400 различными URL-адресами - Если у вас есть очень решительный хищник, они могут разместить его на нескольких веб-сайтах, форумах с изображениями, мошеннических порносайтах », - объяснила она, прежде чем ее прервали.

«Прежде всего, нам нужно будет определить ряд вещей, с точки зрения законности, запроса согласия, а также того, как долго мы можем рыться в сети, как мы создадим инструмент.

«Мы не говорили, что собираемся потратить так много - мы можем решить создать технологию с нуля, если мы не найдем коммерческой версии ИИ... мы хотели бы убедиться, что любая технология, которую мы используем, и это может быть не просто программный инструмент, это может быть необходимая инфраструктура, поэтому я не готов сказать, сколько мы будем платить за технологию как таковую, потому что для этого потребуется много работы.»

Существующая система расследований Olympus, которую в настоящее время использует eSafety, была создана с нуля с использованием некоторых коммерческих продуктов многими собственными разработчиками агентства, добавила она.

«Это первый раз, когда нам предоставили финансирование, чтобы мы могли должным образом оценить это», - сказала она.

Инман Грант получит широкие полномочия с принятием Закона о безопасности в Интернете 2021 года. Среди прочего, закон расширяет действующую в настоящее время функцию кибер-уничтожения детей на взрослых.

Агентство получило 3600 запросов взрослых, связанных с киберпреступлениями, с тех пор, как оно начало их неформально принимать в 2017 году.

Только 72 из них, однако, eSafety сочла достигающими порога «реального вреда». Один из них, по словам Инмана Гранта, был «ужасающим», а некоторые из них были связаны с насилием в семье и преследованием.

«Мы использовали наши отношения с платформами социальных сетей, чтобы помочь удалить материалы по 72 наиболее серьезным случаям», - добавил глава отдела расследований eSafety Тоби Дагг.

Если бы у eSafety были формальные полномочия, то число 72 было бы выше.

«Поскольку [у нас] нет официальных полномочий в этой области и нет схемы для применения, они представляют наиболее серьезные вопросы, которые потребовали от нас координации с платформами удаления этого материала», - сказал Дагг.

«Силы нет, поэтому мы на самом деле полагаемся на добрую волю платформ, чтобы действовать, когда мы думаем, что людям грозит серьезный вред», - добавил Инман Грант.

«Мы не пытаемся использовать кувалду каждый раз… мы не заявляем никаких юридических оснований, мы говорим им, что это тот, кому, по нашему мнению, угрожает опасность и который испытывает крайние страдания из-за контента, размещенного на их сайте».

Около 70% случаев киберпреступлений среди взрослых, по мнению eSafety, неофициально содержали элемент клеветы». ***(Asha Barbaschow. eSafety prepares for Online Safety Act with AU$3m software pilot and 20 new staff // ZDNet (https://www.zdnet.com/article/esafety-prepares-for-online-safety-act-with-au3m-software-pilot-and-20-new-staff/). 28.05.2021).***

***

Інші країни

«1 апреля 2021 года Департамент связи и цифровых технологий опубликовал проект национальной политики в области данных и облачных вычислений (№ 44389). Видение политики - движение «в сторону Южной Африки, интенсивно использующей данные и управляемой данными».

В проекте национальной политики в области данных и облачных вычислений признается и подчеркивается важная роль технологий хостинга данных и облачных вычислений в современном цифровом мире, и заявленная цель - поддержать экономику Южной Африки за счет использования возможностей, которые могут быть предоставлены этими технологиями. Предлагаемые изменения нынешней среды в Южной Африке, если они будут внесены, будут широкими и будут применяться в основном по всей стране (например, к правительству, государственным предприятиям, частному сектору и широкой общественности). Предлагаемые политические меры, содержащиеся в проекте национальной политики в области данных и облачных вычислений, повлияют на ряд ключевых

областей в этом пространстве, таких как цифровая инфраструктура, меры кибербезопасности и конфиденциальность данных.

Среди других мер политики Проект национальной политики в области данных и облачных технологий предлагает регулировать трансграничную передачу данных и вводить требования по локализации данных. Проект национальной политики в области данных и облачных вычислений определяет локализацию данных как «требования к физическому хранению данных в пределах национальных границ страны, хотя иногда она используется в более широком смысле для обозначения любых ограничений на трансграничные потоки данных». Предлагаемые политические меры включают:

создание Центра высокопроизводительных вычислений и обработки данных (HPCDPC), который будет обрабатывать и размещать правительственные данные с использованием облачных вычислений;

хранение и обработка всех данных, отнесенных к критически важной информационной инфраструктуре в пределах ЮАР; а также

когда происходит трансграничная передача данных о гражданах, хранение копии таких данных в Южной Африке для целей правоохранительной деятельности.

Требование хранить копию данных о гражданах не расширяется, и было бы интересно дополнительно понять, предполагается ли, что копия всех без исключения данных о гражданах должна будет храниться в Южной Африке.

Учитывая количество компаний, использующих облачные сервисы, где информация размещается на серверах за пределами Южной Африки, возникает ряд вопросов. Например, потребуется ли для этого передача копии данных в Южную Африку, и если да, то за чей счет? Проект национальной политики в области данных и облачных вычислений признает и направлен на обеспечение более строгого соблюдения Закона о защите личной информации 2013 года (« POPIA »). Хотя в POPIA нет специального положения о локализации данных, раздел 72 POPIA ограничивает передачу личной информации за пределы Южной Африки. Однако раздел также предписывает законные способы передачи личной информации за пределы ЮАР. К ним относятся случаи, когда:

субъект данных дает согласие на передачу данных;

третья сторона-получатель информации подчиняется закону или обязательным правилам / соглашению, которое обеспечивает адекватный уровень защиты;

передача необходима для выполнения договора между субъектом данных и ответственной стороной; или же

передача осуществляется в пользу субъекта данных.

В связи с введением требований по локализации данных в проекте национальной политики в области данных и облачных вычислений возрастет потребность в создании большего числа центров обработки данных в Южной Африке. В настоящее время большинство центров обработки данных в Южной Африке расположены в крупных мегаполисах, расположенных в провинциях Гаутенг, Квазулу-Натал и Западный Кейп. В проекте национальной политики в области данных и облачных вычислений предлагается строить центры обработки

данных за пределами этих территорий, чтобы децентрализовать инвестиции и распределить возможности по всей стране.

Дополнительные социально-экономические цели включают требования о том, что все инвестиции, вложенные в развитие и строительство центров обработки данных, потребуются для достижения широких целей расширения экономических прав и возможностей чернокожих, и что в случае прямых иностранных инвестиций в инфраструктуру такие стороны должны будут предоставить для передачи цифровых навыков (которые определены в контексте проекта национальной политики в области данных и облачных вычислений для обозначения ряда возможностей использования цифровых устройств, коммуникационных приложений и сетей для доступа к информации и управления ею).

Проект национальной политики в области данных и облачных технологий все еще находится на начальной стадии, и министр в настоящее время принимает комментарии и материалы по нему до 18 мая 2021 года». ***(ISAIVAN NAIDOO, JESSICA STEELE AND NALEDI RAMOABI. The Draft National Data and Cloud Policy: possible implications for data hosting and cloud IT services // ENSafrica (https://www.ensafrica.com/news/detail/4229/the-draft-national-data-and-cloud-policy-poss). 11.05.2021).***

***

«Изменения в хранении данных в Турции

Введение и резюме

Национальная стратегия и план действий в области кибербезопасности (2020-2023 гг.) Были опубликованы Министерством транспорта и инфраструктуры 29 декабря 2020 г. Было подчеркнуто, что такие вопросы, как оставшиеся внутри страны данные, произведенные внутри страны, будут играть ключевую роль в исследованиях, которые будут проводиться в отношении защиты этих инфраструктур, связанных с критически важными инфраструктурами, и повышения их прочности.

С другой стороны, с точки зрения обязательств по хранению данных в Турции, Президентский циркуляр № 2019/12 о мерах безопасности информации и связи (« Циркуляр»") Он был опубликован в Официальном вестнике 6 июля 2019 года и вступил в силу. Циркуляр был направлен на снижение и нейтрализацию серьезных рисков безопасности, которые могут возникнуть в процессе оцифровки информации, а также на обеспечение безопасности особо важных типов данных. Одним из наиболее важных вопросов, регулируемых циркуляром, является обязательство безопасно хранить важную информацию и данные, такие как данные о населении, здоровье и коммуникации, а также генетические и биометрические данные в Турции. Это не считается запретом на передачу, это также интерпретируется как необходимость иметь резервную копию (хранилище) соответствующих данных в Турции для обеспечения большей доступности.

Хотя Циркуляр предназначен для государственных учреждений, организаций и предприятий, которые предоставляют услуги в качестве критически важной инфраструктуры, он найдет область применения, включающую юридические лица частного права, обслуживающие эти учреждения и предприятия. Таким образом,

обязательства Циркуляра в отношении хранения данных в стране косвенно применяются к государственным учреждениям и организациям, а также к поставщикам и деловым партнерам предприятий, которые предоставляют услуги в качестве критически важной инфраструктуры. Например, в соответствии со статьей 3 Циркуляра данные, принадлежащие государственным учреждениям и организациям, не должны храниться в службах облачного хранения, за исключением частных систем учреждений или внутренних поставщиков услуг, контролируемых учреждением. В контексте, Согласно циркуляру, можно сделать вывод, что лица частного права, которые предоставляют услуги любому государственному учреждению, должны иметь внутренний сервер с точки зрения облачных услуг, которые они могут предложить этому учреждению. Кроме того, в соответствии со статьей 6 Циркуляра также регулируется предпочтение использования внутренних приложений социальных сетей и коммуникационных приложений.

Однако также ведутся дискуссии о применимости и характере Циркуляра. Также можно считать, что Руководство по информационной и коммуникационной безопасности («Руководство»), подготовленное Управлением цифровой трансформации Президентства («DDO») для раскрытия реализации Циркуляра и соответствующих мер, указанных в Циркуляре, является руководством с точки зрения стандартов безопасности и не является обязательным.

Сообщается, что в рамках Национальной стратегии и плана действий в области кибербезопасности (2020-2023) в повестку дня могут быть внесены дополнительные правила для хранения данных внутри страны и ограничения их передачи. С другой стороны, слышно, что Управление по защите личных данных работает в соответствии со статьей 9 Закона о защите личных данных, которая ограничивает передачу личных данных в более жестких условиях по сравнению с Европейским регламентом защиты данных. У учреждения также может быть возможность разработать механизмы и альтернативы, такие как обязательные правила компании, которые не регулируются законом, но принимаются в Турции в рамках полномочий, предоставленных учреждению.

В дополнение к законодательству о хранении данных внутри страны с точки зрения определенных секторов, обязательство, налагаемое Циркуляром на основе категорий данных в более общем смысле, указывает на то, что в этом направлении желательна особая защита. Направление, в котором будут развиваться процессы передачи, локализации и хранения данных в Турции, вызывает серьезную озабоченность.

Текущие изменения в информационной безопасности: руководство по информационной и коммуникационной безопасности

В Циркуляре говорится, что Руководство, которое включает различные уровни безопасности, будет подготовлено и опубликовано при координации президентства DDO для применения в государственных учреждениях, организациях и предприятиях, предоставляющих услуги в качестве критически важной инфраструктуры. В этом контексте Руководство было утверждено 24.07.2020 и опубликовано на сайте DDO.

Руководство представляет собой исчерпывающее руководство с подробным описанием действий и мер предосторожности, которые необходимо предпринять для обеспечения безопасности данных, а также различных вложений и подробных шаблонов, которые компании могут использовать во время исследований соответствия. С другой стороны, большинство вопросов, упомянутых в Руководстве, связаны с техническими проблемами и административными мерами, которые обычно известны из отзывов, которые мы получаем от отрасли. Тем не менее рекомендуется, чтобы учреждения и операторы, входящие в сферу охвата, и косвенно третьи стороны, обслуживающие эти учреждения и операторов, приняли во внимание график, установленный в Руководстве, и организовали свои внутренние процессы в максимально возможной степени параллельно с Руководством.

Чтобы следовать графику, указанному в Руководстве, в течение 6 месяцев с даты публикации Руководства компании должны определить группы активов в своей структуре и выполнить оценку критичности и анализ пробелов. После этого анализа дорожная карта реализации, которая будет включать шаги, которые необходимо выполнить для соблюдения Руководящих принципов, также должна быть подготовлена в течение первых 6 месяцев. Этот период истек 31.01.2021 для государственных учреждений и организаций и предприятий, оказывающих услуги критической инфраструктуры.

Меры, относящиеся к группам активов с уровнем критичности 1 после шестимесячного периода, подлежат оценке критичности и анализу пробелов не позднее, чем в течение 12 месяцев (в течение 18 месяцев с даты публикации Руководства), а меры, относящиеся к группам активов с критичностью уровень 2. и самое позднее в течение 15 месяцев после анализа пробелов (в течение 21 месяца с даты публикации Руководства), а также меры для групп активов с уровнем критичности 3 в течение 18 месяцев после оценки критичности и анализа пробелов (из публикации дату выпуска Руководства), которое должно быть введено в действие не позднее, чем в течение 24 месяцев. В Руководстве есть подробные инструкции о мерах и о том, как они будут реализованы.

Помимо Циркуляра, в Руководстве также есть положения, касающиеся хранения и передачи данных внутри страны. Например, в Циркуляре говорится о том, что « данные, принадлежащие государственным учреждениям и организациям, не будут храниться в службах облачного хранения, за исключением их собственных частных систем или контролируемых учреждением внутренних поставщиков услуг » при использовании облачных служб для государственных учреждений и организаций. также может быть истолковано как препятствие для передачи данных за границу. При использовании облачных сервисов « обеспечение того, чтобы критически важные данные хранились внутри страны, а не за рубежом.было упомянуто требование. Это постановление, которое может иметь последствия для поставщиков, обслуживающих государственные учреждения и организации. Опять же, для операторов подчеркивается необходимость принятия мер по удержанию внутреннего коммуникационного трафика в границах страны, для предотвращения вывоза этого трафика и записей об абонентах за границу и перенаправления в страну, а также для обеспечения безопасности. облачной среды

при доступе к серверам следует принять меры для удержания трафика внутри страны.

Циркуляр также предусматривает, что учреждения и организации должны установить механизмы контроля за внедрением Руководства и проводить аудит выполнения не реже одного раза в год. Результаты аудита, а также корректирующие и предупреждающие действия должны быть представлены DDO в виде отчета в соответствии с процедурами и принципами, указанными в Руководстве. Однако указывается, что аудиторская деятельность, упомянутая в опубликованном Руководстве, будет осуществляться на основе Руководства по аудиту информационной и коммуникационной безопасности, которое будет опубликовано на веб-сайте DDO, но руководство по аудиту еще не опубликовано.

Санкции, которые могут быть применены в случае нарушения

В Циркуляре было упомянуто, что информационные системы, которые должны быть вновь созданы во всех государственных учреждениях, организациях и предприятиях, предоставляющих услуги критически важной инфраструктуры, должны соответствовать Руководству. Кроме того, DDO заявляет, что в случае слабости из-за несоблюдения указанных мер, санкции, уже определенные в соответствующем законодательстве, действуют. Циркуляр и Руководство не предусматривают отдельной санкции, и регулирование такой санкции не ожидается с юридической точки зрения.

Ясно, что Конституция Турецкой Республики и Закон № 657 о государственных служащих могут найти применение в отношении государственных служащих, работающих в государственных учреждениях и организациях. В этом контексте государственные служащие и государственные служащие могут иметь обязанности как перед государством, так и перед людьми. Эта проблема может повлиять на организацию внутренних процессов общества и его институтов, а также на обязательства, которые можно ожидать от поставщиков в отношении услуг, которые будут получены.

В отношении предприятий критической инфраструктуры могут применяться санкции в отношении информационной безопасности в рамках законодательства, которому они подчиняются. Таким образом, регулирующие и надзорные учреждения могут внести некоторые изменения в свое вторичное законодательство с учетом Циркуляра и Руководства по информационной безопасности. Кроме того, санкции за соблюдение Циркуляра и Руководства также могут регулироваться в целом. Также следует подчеркнуть, что в случае нарушения Циркуляра и Руководства в ходе аудита, который может быть проведен регулирующими и надзорными органами, ответственными за регулирование и надзор в соответствующем критическом секторе, могут быть наложены административные санкции в соответствии с с положениями об информационной безопасности и другими соответствующими положениями законодательства, подготовленными соответствующими учреждениями.

Кроме того, в Циркуляре указано, что Руководство может быть обновлено с учетом потребностей, развития технологий, меняющихся условий и изменений, которые могут быть внесены в национальную стратегию кибербезопасности и планы действий.

Что касается некоторых критических секторов, вопросы, изложенные в Циркуляре и Руководящих принципах, не новы. Например, положения, которые могут составлять основу для возможных санкций с точки зрения законодательства, которому подчиняются операторы электронной связи, Закона об электронных коммуникациях No 5809, Положения об административных санкциях в отношении информационных технологий и учреждений связи и Процедуры создания кодированных или зашифрованных сообщений. в Службе электронных коммуникаций государственных учреждений и организаций, а также физических и юридических лиц, и эти нормативные акты и другие второстепенные постановления Управления информационных и коммуникационных технологий требуют мер защиты данных, которые аналогичны или аналогичны Циркуляру и Руководству. С этой точки зрения Текущая практика компаний электронной связи в целом соответствует мерам, предусмотренным в Циркуляре и Руководстве. Тем не менее, будет полезно следить за развитием событий. Например, в Положение об обработке персональных данных и защите конфиденциальности в секторе электронных коммуникаций были внесены поправки, вступающие в силу 4 июня 2021 года. В отличие от старых правил, новые правила, как правило, не препятствуют передаче персональных данных за границу и допускают передачу с явного согласия. В Циркуляре указывается, что операторы, уполномоченные предоставлять услуги связи, обязаны создать точку обмена интернет-трафиком в Турции, и оговаривается, что будут приняты меры для предотвращения внутреннего трафика связи, который необходимо изменить в Турции. Это положение, Помимо обязательства внутреннего хранения, которое связано с критически важными данными, его также можно рассматривать как регулирование, ограничивающее передачу за границу. С другой стороны, хотя в Положении об обработке персональных данных и защите конфиденциальности в новом секторе электронных коммуникаций указано, что крайне важно не вывозить данные о трафике и местоположении за границу по соображениям национальной безопасности, ситуации, когда даже данные о трафике и местоположении могут быть переведены за границу, не игнорируются. Регулируется, что операторы могут передавать данные за границу с явного согласия подписчика, объясняя название страны, в которую данные будут переданы подписчикам, если соответствующая третья сторона находится за границей для ситуаций, когда передача трафика и данные о местоположении третьим лицам находятся под вопросом.

В финансовом секторе - другой сектор, который был определен как критический сектор, когда уровень безопасности в соответствии с Циркуляром и Руководящими принципами не предусмотрен с точки зрения информационной безопасности, как в Положении о внутренних системах банков, так и в внутреннем капитале. Процесс оценки адекватности Агентства банковского регулирования и надзора и информационных систем банков и Положение об электронных банковских услугах, а также Коммюнике по управлению и надзору за информационными системами финансовых лизинговых, факторинговых и финансовых компаний могут применяться к соответствующим предприятиям. Фактически, энергетика, которые являются другими критическими секторами. Что касается секторов транспорта и управления водными ресурсами, уполномоченным

частным юридическим лицам, работающим в этих секторах перед министерствами и соответствующими регулирующими учреждениями и организациями, будет выгодно организовать процессы информационной безопасности в соответствии с Циркуляром и Руководством. Потому что в этих секторах вторичные правила, касающиеся безопасности информации, данных и инфраструктуры в целом, можно интерпретировать как введение санкций в случае нарушения Циркуляра и Руководства.

Наконец, хотя есть некоторые сомнения в применении как Циркуляра, так и Руководства государственными учреждениями, видно, что министерства осведомлены об этой проблеме и что поставщики государственных учреждений могут принять некоторые меры для обеспечения соблюдения этого правила. Например, юридические лица частного права, к которым Циркуляр и Руководящие принципы не применяются напрямую, также могут брать на себя договорные обязательства, которые они берут на себя для соблюдения этих мер в рамках услуг, которые они предоставляют населению и своим организациям. Как мы заметили, это стало обычной практикой, такое обязательство должно быть дано в рамках тендерных процессов,

Результат

Обязательный характер Циркуляра и Руководства по лицам частного права весьма противоречив на практике и в доктрине. Как правило, циркуляры - это правила, которые выражают то, как верхняя правовая норма может быть интерпретирована или как верхняя правовая норма должна применяться администрацией по отношению к субадминистративным единицам или администраторам. Как указано в различных решениях Государственного совета, более уместно, чтобы циркуляры не добавляли новый элемент в правовой мир, имели пояснительный характер существующих правил и, что наиболее важно, не нарушали субъективные права и интересы заинтересованных сторон..

Широкое внедрение Циркуляра и Руководства с целью ограничения локализации или передачи данных может привести к различным обсуждениям в рамках этой структуры. Например, в рамках Закона о защите персональных данных, который является регулированием на уровне закона, в то время как передача за границу возможна при наличии определенных условий или с явного согласия лица, чьи персональные данные обрабатывается в любом случае, ограничивая возможности, предоставляемые этим правилом, посредством применения Циркуляра или Руководства, действительности Циркуляра и Руководящих принципов, и, опять же, он откроет для обсуждения, могут ли санкции применяться в данном контексте соответствуют закону». ***(Begüm Yavuzdoğan Okumuş ve Yalçın Umut Talay. Verilerin Türkiye'de Depolanması Yönünde Gelişmeler // Gün + Partners Avukatlık Bürosu (https://gun.av.tr/tr/goruslerimiz/makaleler/verilerin-turkiye-de-depolanmas%C4%B1-yonunde-gelismeler). 10.05.2021).***

***

«Две крупнейшие трубопроводные компании Канады заявляют, что они приняли упреждающий подход, чтобы избежать кибератак, которые

нарушили поставки бензина на юго-востоке США и способствовали повышению розничных цен на бензин в Северной Америке.

Хакеры смогли захватить контроль над компьютерными системами для Colonial Pipeline, заблокировать доступ и потребовать выкуп за их освобождение. Частичное обслуживание было восстановлено вручную поздно в понедельник, но полное восстановление ожидается не раньше выходных.

TC Energy и Enbridge, базирующиеся в Калгари, заявляют, что они регулярно принимают меры предосторожности, включая технологии и обучение, для защиты своих операций от кибератак.

Вивек Гупта, возглавляющий отдел кибербезопасности BDO Canada, говорит, что трубопроводы всегда были мишенью для кибератак из-за возможности получения высоких выплат.

«При этом, - добавляет он, - это единственная в своем роде атака с точки зрения масштаба. Насколько я могу судить, это крупнейшая атака на трубопровод, по крайней мере, за 20-25 лет ".

Он говорит, что организации обычно знают, что программы-вымогатели, использованные в атаке Colonial Pipeline, могут остановить их работу, но часто не принимают все меры предосторожности.

«Очень жаль, что подобное событие будит многих людей», - говорит Гупта.

Гупта и другие эксперты по кибербезопасности говорят, что распространенный способ проникновения хакеров в систему безопасности - обмануть сотрудников с помощью электронных писем или текстовых сообщений, которые позволяют проникнуть в корпоративные системы вредоносному ПО.

Опрос Proofpoint, проведенный среди 1400 руководителей информационной безопасности из 14 стран, показал, что мошенничество с использованием электронной почты было признано основной проблемой кибербезопасности для канадских руководителей информационной безопасности.

Другие проблемы, отмеченные канадскими респондентами в ходе опроса за первый квартал, заключались в использовании неавторизованных устройств или программного обеспечения, а также в ненадежных паролях.

Представитель Proofpoint Люсия Милица говорит, что человеческая ошибка была названа самой большой уязвимостью 51% канадских руководителей кибербезопасности.

Роберт Фальзон, канадский представитель Check Point, говорит, что компании также могут создать брешь в безопасности, когда они обращаются к удаленным серверам или облачным почтовым службам от Microsoft или Google.

Он говорит, что проблемы могут возникнуть, если эти компании также не обновят свои существующие системы аутентификации, которые хранят централизованный учет имен пользователей, паролей и других идентификационных данных.

«Хакеры знают, что делают. Они атакуют самое слабое место - эти устаревшие системы, - говорит Фальзон.

Федеральное бюро расследований США заявило, что за атакой с целью выкупа стояла группа под названием DarkSide. Colonial Pipeline мало рассказала о том, как она стала жертвой нападения.

В заявлениях TC Energy Corp. и Enbridge Inc. не упоминались какие-либо подробности атаки на Colonial Pipeline, которая доставляет около 45 процентов бензина, используемого на восточном побережье США.

TC Energy заявляет, что у нее есть «хорошо разработанная программа кибербезопасности, которую мы продолжаем продвигать и внедрять для защиты наших данных, систем и активов».

Enbridge Inc. заявляет, что «на протяжении многих лет инвестировала значительные средства в кибербезопасность», а также регулярно тестирует и контролирует свои системы.

Ни одна из компаний не раскрыла конкретных подробностей атаки на Colonial.

По сообщению Associated Press, большая часть газопровода Colonial возобновила работу в понедельник, и власти заявляют, что дефицита бензина нет, но панические закупки способствовали тому, что на более чем 1000 заправочных станциях закончилось топливо.

В понедельник ФБР заявило, что подтвердило, что программа-вымогатель Darkside была ответственна за отключение Colonial, что указывает на то, что это работа организованной преступной группы». ***(Cybersecurity experts say Canadian businesses can learn from U.S. pipeline attack // jwnenergy (https://www.jwnenergy.com/article/2021/5/13/cybersecurity-experts-say-canadian-businesses-can-/). 13.05.2021).***

***

«По сообщениям, японское правительство введет новые правила в 44 секторах для усиления национальной киберзащиты, отчасти в ответ на взлом Colonial Pipeline, произошедший на прошлой неделе.

Правительство планирует внести поправки в различные законы, регулирующие каждый сектор, путем принятия всеобъемлющего предложения и нового закона, обязывающего каждый сектор осознавать риски для национальной безопасности, говорится в отчете Nikkei.

Секторы, в которых, как ожидается, будут внесены изменения в законодательство, включают, среди прочего, телекоммуникации, электричество, финансы, железные дороги, государственные услуги и здравоохранение. В частности, как сообщается, эти секторы должны будут изучить проблемы, связанные с использованием иностранного оборудования или услуг, включая облачное хранилище данных и подключения к серверам, расположенным за рубежом.

Сообщается, что правительство также будет контролировать компании на предмет соблюдения требований и получит возможность запрещать компаниям использовать иностранное оборудование, если они обнаружат какие-либо серьезные проблемы.

Подробные стандарты, вероятно, будут также изложены в будущих постановлениях и директивах правительства.

Три года назад японские правительственные агентства согласились прекратить закупку оборудования, которое может представлять угрозу

национальной безопасности, например, от Huawei и ZTE. Обладая последним мандатом, японское правительство теперь хочет распространить этот уровень жесткости на частный сектор.

Этот шаг произошел через неделю после того, как Colonial Pipeline - один из крупнейших операторов трубопроводов Америки, который обеспечивает примерно 45% топлива на восточном побережье страны - подвергся атаке с использованием программ-вымогателей. Из-за кибератаки компании пришлось временно закрыть свои операции, заморозить ИТ-системы, чтобы изолировать заражение, и заплатить около 5 миллионов долларов за расшифровку заблокированных систем.

В течение той же недели после взлома Colonial Pipeline виновники атаки с использованием программ-вымогателей также поразили Toshiba, хотя атака с использованием программ-вымогателей оказалась в основном в Европе, а не внутри страны.

Другие страны, такие как США, уже ввели аналогичные ограничения на закупки, связанные с технологиями. В США компании - как внутренние, так и иностранные - должны получить разрешение на лицензирование, чтобы покупать технологии, созданные Huawei и ZTE, или продавать товары этим китайским компаниям, если они содержат определенные американские технологии.

К северу от границы канадские телекоммуникационные компании также эффективно заблокировали доступ Huawei к построению своих сетей 5G, подписав вместо этого сделки с конкурентами китайского гиганта. Китайский поставщик сетевого оборудования также запрещен в Австралии и Швеции, и он не вторгся в Новую Зеландию после того, как GCSB запретил Spark использовать комплект Huawei в ноябре 2018 года.

Между тем, британским мобильным сетям сказали, что они не могут больше покупать оборудование 5G у Huawei после конца этого года и что они должны удалить технологии китайской сетевой компании из своих сетей 5G к концу 2027 года». ***(Campbell Kwan. Japan to restrict private sector use of foreign equipment and tech: Report // ZDNet (https://www.zdnet.com/article/japan-to-restrict-private-sector-use-of-foreign-equipment-and-tech-report/). 18.05.2021).***

***

«Кибербезопасность находится под постоянным контролем всех государственных учреждений Ирландской Республики, заявил Таойзич (премьер-министр Ирландии) Мишель Мартин.

Он сказал, что такие атаки представляют собой очень серьезную угрозу как для государства, так и для частного сектора.

Г-н Мартин сказал, что реакция правительства будет «последовательной и методичной».

На прошлой неделе Управление здравоохранения республики (HSE) было вынуждено отключить все свои ИТ-системы после «серьезной» атаки программ-вымогателей, которые были сосредоточены на доступе к данным, хранящимся на центральных серверах.

Г-н Мартин сказал, что существует вероятность того, что данные пациентов были доступны и могут быть переданы, и что эксперты по безопасности оценивают полное влияние этой угрозы и ее последствия.

«Это отвратительное нападение, это шокирующее нападение на службу здравоохранения, но в основном на пациентов и ирландскую общественность», - сказал г-н Мартин.

«Мы советуемся с экспертами в области кибербезопасности - Национальным центром кибербезопасности (NCSC) - и мы также получаем очень значительную поддержку от экспертов из частного сектора.

«Мы разберемся с этим и будем методично работать в ответ».

'Нас не шантажируют'

По сообщению ирландской телекомпании RTÉ, NCSC идентифицировал банду, стоящую за атаками.

Считается, что это группа «Волшебный паук» из Восточной Европы.

Министр юстиции Хизер Хамфрис заявила, что правительство не будет шантажировать для выплаты преступников.

«Правительство не будет платить никаких денег. Мы будем защищать наших граждан. Нас не будут шантажировать», - сказала она.

Главный клинический директор HSE сказал, что атака с использованием программ-вымогателей оказала сильное влияние на HSE в целом и на способность оказывать медицинскую помощь, и что эти проблемы «несомненно возрастут» для большинства больниц на этой неделе.

Д-р Колм Генри сказал, что большая часть современного здравоохранения в значительной степени зависит от систем информационных технологий для безопасного оказания помощи.

Выступая на канале RTÉ «Утренняя Ирландия», доктор Генри сказал, что оказывается неотложная и неотложная медицинская помощь, но не так, как раньше.

Он сказал, что заказ тестов, сравнение и запись результатов «полностью связаны с ИТ», и в больницах есть люди, которые теперь доставляют результаты консультантам, в то время как медицинские бригады напрямую звонят терапевтам.

Он сказал, что HSE работает с внешними агентствами, и приоритетом является восстановление тех клинических систем, от которых зависят важнейшие службы.

К ним относятся материнство, радиология, лучевая терапия, новорожденные и диагностика». ***(Micheál Martin: Ireland's cyber security 'under continuous review' // BBC (https://www.bbc.com/news/world-europe-57154690). 18.05.2021).***

***

«Муниципалитет Гааги в Нидерландах позволяет взламывать себя каждый год во время Hâck The Hague. Соревнование по взлому, организованное муниципалитетом совместно с компанией Cybersprint, занимающейся кибербезопасностью. В понедельник, 27 сентября 2021 года, 200 этических хакеров из Нидерландов и из-за рубежа снова попытаются обнаружить уязвимости в цифровой инфраструктуре муниципалитета и его поставщиков. С помощью этой конкуренции Гаага хочет повысить свою устойчивость и стимулировать своих

поставщиков постоянно находиться в наилучшем цифровом состоянии, чтобы можно было гарантировать мир и безопасность.

Отобранные хакеры могут попытаться взломать муниципальные цифровые системы и системы их поставщиков 27 сентября 2021 года. Для обеспечения честной игры все участвующие хакеры заранее соглашаются сообщать об уязвимостях, которые они обнаруживают на специальном портале, чтобы предоставить доказательства того, что они выяснили, как они это обнаружили и как это можно решить, и не публиковать их. Эти условия соответствуют Скоординированному раскрытию информации об уязвимости муниципалитета. Приглашаются как профессиональные хакеры, так и студенты.

Муниципалитет Гааги стремится к тому, чтобы обработка личных данных и доступность его услуг постоянно соответствовали самым высоким требованиям безопасности. За этим также следит во время хакерского конкурса жюри, состоящее из специалистов индустрии кибербезопасности.

Существует 12 денежных призов от 500 до 2000 евро, доступных в четырех категориях:

Самый креативный хак

Самый продвинутый взлом

Самый эффективный взлом

Hâckademic Award, включая рекомендательное письмо (студенческая награда).

С помощью премии Hâckadamic Award Гаага хочет побудить студентов и других молодых специалистов делать больше в области кибербезопасности. Как вы думаете, сможете взломать муниципалитет Гааги? Зарегистрируйтесь до 1 июня на сайте Hâck The Hague». ***(Can you hack the municipality of The Hague (Nl)? // BNP Media (https://www.securitymagazine.com/articles/95254-can-you-hack-the-municipality-of-the-hague-nl). 20.05.2021).***

***

«Парламент недавно принял Закон о кибербезопасности 2020 года (Закон 1038), регулирующий деятельность в области кибербезопасности в Гане и способствующий развитию кибербезопасности в стране.

В частности, Закон создал Управление кибербезопасности для регулирования деятельности в области кибербезопасности, предотвращения, управления и реагирования на угрозы кибербезопасности, повышения осведомленности о вопросах кибербезопасности и сотрудничества с международными агентствами для продвижения кибербезопасности страны, среди других целей.

В рамках своих функций Управление кибербезопасности должно консультировать правительство и государственные учреждения по вопросам, связанным с кибербезопасностью, содействовать защите детей в Интернете, оказывать техническую поддержку правоохранительным органам и агентствам безопасности в преследовании киберпреступников, устанавливать стандарты для сертификации продуктов и услуг кибербезопасности и соответствующей сертификации, а также для выдачи лицензий и установления стандартов для предоставления услуг кибербезопасности.

Ожидается, что реализация этого закона поддержит продолжающиеся усилия по усилению борьбы правительства с киберпреступностью». ***(Ghana Introduces Cybersecurity Act // N. Dowuona & Company (https://www.ndowuona.com/news-and-updates/legal-updates/123-ghana-introduces-cybersecurity-act). 25.05.2021).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Рада Європейського Союзу 17 травня ухвалила подовження дії рамкових санкцій за кібератаки проти блоку та його членів до 18 травня 2022 року. Про це пресслужба Ради повідомила напередодні. Як пояснюють в установі, рамкове рішення дозволяє Євросоюзу запроваджувати точкові обмеження щодо людей та компаній, причетних до кібернападів, які мали значні наслідки та становили зовнішню загрозу для ЄС і його членів. Санкції також можуть бути запроваджені за напади на кібербезпеку третіх держав чи міжнародних організацій, якщо це вважатиметься необхідним згідно із Загальної зовнішньою та безпековою політикою блоку. «Санкції наразі застосовані щодо восьми людей та чотирьох установ та передбачають замороження активів та заборону на в'їзд. Крім того, громадянам та компаніям-резидентам ЄС заборонено надавати фінансування членам цього списку», – йдеться в повідомленні Ради. Подовження дії санкцій у ЄС називають «частиною підвищення стійкості та здатності запобігати, демотивувати, стримувати від та реагувати на кібератаки та зловмисну кіберактивність, аби захистити європейську безпеку та інтереси». Євросоюз створив Рамкове рішення для спільної дипломатичної відповіді на зловмисну кіберактивність у 2017 році. Механізм, як передбачалося, має дозволити блоку та державам, що до нього входять, реагувати на кібератаки, спрямовані на його цілісність і безпеку». ***(Рада ЄС вчергове продовжила дію санкцій за кібератаки // информационный портал "ua.today" (http://ua.today/news/world/rada_yes_vchergove_prodovzhila_diyu_sankcij_za_kiberataki). 18.05.2021).***

***

«Президент Джо Байден заявил в четверг, что Владимир Путин не имел отношения к преступной кибератаке в России на огромный топливопровод в США, но что он поднимет этот вопрос на ожидаемом саммите.

Вашингтон считает, что преступная группа, базирующаяся в России, нацелена на колониальный трубопровод, по которому бензин доставляется через большую часть юго-востока США, с помощью программы-вымогателя.

На вопрос, знали ли Путин или российское правительство об атаке, Байден сделал паузу, а затем сказал: «Я уверен, что я правильно прочитал отчет ФБР, и они говорят, что нет, он не знал, правительство не было».

«Мы не верим, - подчеркиваю я, - что российское правительство было причастно к этой атаке. Но у нас есть веские основания полагать, что преступники, совершившие нападение, живут в России. Вот откуда это произошло», - сказал он.

Байден сказал, что его администрация находится в «прямом контакте с Россией» и что международные стандарты необходимы для ужесточения контроля над такими преступными группировками.

«Я подозреваю, что это одна из тем, о которой я буду говорить с президентом Путиным», - сказал Байден.

Ожидается, что он впервые встретится с Путиным после того, как стал президентом, во время своего визита в Европу в июне». ***(Biden to Bring Up Russian Hackers Issue With Putin // Wired Business Media (https://www.securityweek.com/biden-bring-russian-hackers-issue-putin). 13.05.2021).***

***

«Европейский Союз прилагает слишком мало усилий для защиты от виртуальных атак со стороны России и Китая, считают немецкие политики.

Запад пережил уже массу кибератак, но как будто еще полностью не осознал всю серьезность происходящего.

Будет ли Третья мировая кибервойной?

От Германии до США

8 мая 2015 года пока канцлер Германии Ангела Меркель на торжественном мероприятии отмечала окончание Второй мировой войны, молодой хакер из России виртуально проник в ее офис в бундестаге - и взломал компьютер Меркель. Поддельные электронные письма, якобы отправленные Организацией Объединенных Наций, открыли ему доступ к IT-системам бундестага.

«Федеральному управлению уголовной полиции совместно со спецслужбами потребовалось пять лет, чтобы разоблачить хакера Дмитрия Бадина - сотрудника российской службы военной разведки ГРУ.

Недавно чрезвычайное положение объявили 17 штатов США: атака, осуществленная Dark Side, российской киберпреступной группировкой, парализовала снабжение нефтепродуктами восточного побережья через трубопровод Colonial Pipeline. На заправках для 50 млн жителей США не хватало топлива.

Практически исторической по масштабу можно назвать атаку на американского поставщика ИТ-услуг Solarwinds. Сейчас эту атаку считают крупнейшим случаем шпионажа за столетие. Об атаке стало известно лишь тогда, когда в декабре 2020 года тревогу забила частная охранная фирма - а не ведомства, отвечающие за киберзащиту. К тому времени хакеры уже проникли в сети министерства финансов и Госдепартамента США, а также ведомства, управляющего ядерным арсеналом Соединенных Штатов.

Хакеры = новые террористы

Достаточно ли хакерских атак на критическую инфраструктуру для того, чтобы Америка и НАТО объявили о необходимости совместной обороны, как они сделали это после террористической атаки на Всемирный торговый центр в Нью-Йорке в 2001 году?

«Конечно, нет, по крайней мере, пока. Но одно можно сказать наверняка: Третья мировая война будет происходить не «на суше, в море и в воздухе», а

виртуально в киберпространстве - без танков и грохота пушек», - считает немецкий политик Гюнтер Эттингер.

Среди мировых кибердержав Иран играет во второй лиге, в первой наряду с Соединенными Штатами находятся Китай, Россия и Израиль.

Россия, безусловно, является самой мощной из ведущих кибердержав, уверена Эттингер.

А что делает Европейский Союз, спрашивает политик? На период с 2021 по 2027 годы он запускает программу безопасности стоимостью всего 1,5 млрд евро. Получается, что на год выделяется 230 млн евро, что, учитывая наличие 27 государств-членов, меньше 10 млн евро на страну. Для поддержки стран-участниц предусмотрен также центр компетенции в области кибербезопасности с 57 сотрудниками.

«Секретные киберармии Москвы и Пекина, - заключает Эттингер, - должно быть, уже дрожат от страха. Или просто надрываются от хохота». ***(Валерій Литонинский. Третья мировая будет кибервойной. Силы сторон // Korrespondent.net (https://korrespondent.net/world/4359910-tretia-myrovaia-budet-kybervoinoi-syly-storon). 21.05.2021).***

***

«На саммите лидеров стран Евросоюза обсудят введение новых санкций против России, в том числе экономических. Участники соберутся на следующей неделе. Об этом заявила зампред Европейской комиссии Вера Йоурова в интервью «Чешскому радио». Она сказала, что новые санкции должны также стать ответом на взрывы в чешской Врбетице в октябре 2014 года, к которым причастны российские спецслужбы. «Законные требования Европейского союза к российской стороне повторяются: прекращение гибридных атак и кибератак, соблюдение прав человека, особенно в отношении Алексея Навального, а также выполнение Минских соглашений», - сказала Йоурова. Йоурова добавила, что разочарована подходом ряда других европейских стран и ожидает от них более резкой реакции. При этом политик утверждает, что ЕС не хочет конфронтации с Россией». ***(На саммите лидеров стран ЕС обсудят новые санкции против России // информационный портал «ua.today» (http://ua.today/news/world/na_sammite_liderov_stran_es_obsudyat_novye_sankcii_protiv_rossii). 23.05.2021).***

***

«Адміністрація президента США Джо Байдена запропонувала закласти в бюджет 2022 року 750 млн доларів на ліквідацію вразливих місць в кіберпросторі, які були виявлені при хакерській атаці на компанію SolarWinds в якій підозрюють Росію…

«$750 млн на додаткові інвестиції, необхідні для того, щоб вивчити уроки з інциденту з SolarWinds», - йдеться в опублікованому Білим домом проекті бюджету.

Додаткові $500 млн планують виділити в фонд, який використовується для просування нових технологій. Ще $110 млн - в цілому на кібербезпеку і забезпечення безпеки інфраструктури.

Укладачі бюджету вказують на необхідність витрачати гроші на протистояння Росії і Китаю.

«У бюджеті пріоритет - протистояння загрозі з боку Китаю, а також - дестабілізуючої поведінки Росії», - йдеться в документі.

У ньому наголошується, що необхідно збільшити фінансування програм, націлених на захист демократії, на захист прав людини, боротьби проти корупції в світі. Також наголошується на важливості «протистояння авторитарним силам».

Президент США Джо Байден в п'ятницю представив проект федерального бюджету на 2022 фінансовий рік, який передбачає збільшення державних витрат до $6 трлн, відповідний документ опублікований на сайті Білого дому.

Проект бюджету об'єднує великі ініціативи, про які раніше оголосив американський президент: «План підтримки американських сімей» вартістю $1,8 трлн і «Американський план зайнятості» вартістю $2,3 трлн, а також $1,5 трлн на дискреційні витрати…». ***(Дубенко Вадим. США хочуть виділити 750 млн доларів для ліквідації вразливостей від хакерів // Дзеркало тижня. Україна (https://zn.ua/ukr/WORLD/ssha-khochut-vidiliti-750-mln-dolariv-dlja-likvidatsiji-vrazlivostej-vid-khakeriv.html). 29.05.2021).***

***

«Недавно обнаруженная попытка российской разведки захватить систему электронной почты правительственного агентства Соединенных Штатов побудила ведущих демократов в пятницу призвать к более жестким действиям против Москвы за ускорение кибератак в преддверии саммита президента Байдена в следующем месяце с президентом Владимиром Путиным.

О последнем взломе стало известно поздно вечером в четверг Microsoft и другими частными фирмами. Они разоблачили, как российское агентство S.V.R., то же спецслужба, которую Вашингтон обвинил в ряде кибератак на американские сети за последнее десятилетие, проникло в коммуникационную компанию, которая распространяет электронные письма от имени Агентства США по международному развитию.

Используя этот доступ, они отправляли достоверные сообщения правозащитным группам, некоммерческим организациям и аналитическим центрам, в том числе тем, которые критиковали г-на Путина. Электронные письма содержали ссылки на вредоносные программы, которые давали россиянам доступ к компьютерным сетям получателей.

Белый дом в пятницу преуменьшил серьезность атаки, заявив, что это типичный ежедневный киберконфликт. Официальные лица заявили, что тот факт, что атака была быстро обнаружена и нейтрализована - в основном Microsoft, которая действовала, когда увидела отправку поддельных электронных писем, - свидетельствует о том, что усиленная защита, применяемая для защиты правительственных сетей, начинает давать результаты.

Но время было удачным, и это усиливало ощущение того, что масштабы исходящих из России кибератак - от самых изощренных до самых неприятных, о чем свидетельствует легкость, с которой хакеры проникли в систему электронной почты, используемую агентством по оказанию помощи, - составляет быстро расширяется, несмотря на предупреждения и ответные меры Вашингтона.

Месяц назад г-н Байден ввел экономические санкции в отношении России и выслал дипломатов в ответ на одну из самых изощренных атак, когда-либо виденных на «цепочку поставок» программного обеспечения, на которую полагаются государственные и частные сети, - атака, которая дала российской разведке широкий доступ. до 18 000 сетей. Хотя русские использовали доступ только для входа примерно в 150 государственных учреждений и компаний, атака продемонстрировала возможность искажения регулярно запланированных обновлений программного обеспечения, которые используются государственными учреждениями и компаниями для поддержания своих систем в актуальном состоянии.

Затем, в этом месяце, произошла атака с использованием программ-вымогателей на Colonial Pipeline, осуществленная преступной группой, которая, по словам Байдена, базируется в России. Трубопровод был закрыт на несколько дней, что вызвало панические закупки, длинные очереди к насосу и перекрытие бензоколонок на юго-востоке. Colonial заплатила выкуп в размере 4,4 миллиона долларов, и нападение подчеркнуло уязвимость критически важной инфраструктуры Соединенных Штатов.

Последняя атака в момент повышенной напряженности с Россией была более простой, но она привлекла дополнительное внимание к тому, почему Соединенные Штаты не смогли сдержать волну атак, заставив своих противников заплатить за них более высокую цену.

Представитель Адам Б. Шифф, демократ от Калифорнии и председатель комитета по разведке палаты представителей, заявил, что годы усилий по сдерживанию подобных атак со стороны России оказались безуспешными.

«Если ответственность несет Москва, этот наглый акт использования электронной почты, связанной с правительством США, демонстрирует, что Россия остается невосприимчивой, несмотря на санкции после атаки SolarWinds», - сказал г-н Шифф, имея в виду атаку в прошлом году на цепочку поставок программного обеспечения. «Эти санкции дали администрации возможность еще больше закрутить экономические гайки в случае необходимости - теперь это кажется необходимым».

Сенатор Марк Уорнер, демократ от Вирджинии и председатель сенатского комитета по разведке, поддержал г-на Шиффа в призыве к более серьезным последствиям. «Мы должны дать понять России и любым другим противникам, что они столкнутся с последствиями этой и любой другой злонамеренной кибератвности», - сказал он.

Г-н Байден уже сказал, что кибератрессия России будет частью напряженного разговора, который он планировал провести с г-ном Путиным 16 июня в Женеве, в момент, когда между двумя странами существуют разногласия по поводу Украины, прав человека и нового поколения России. ядерное оружие.

Некоторые аналитики высоко оценили реакцию правительства США.

«Если вы посмотрите на шаги, которые администрация предпринимает как для защиты, так и для сдерживания, которые являются двумя ключевыми вещами, которые нам здесь необходимо сделать, они движутся в правильном направлении в значительном направлении, которого мы никогда раньше не видели», - сказал Том Берт., высокопоставленный чиновник Microsoft, который работал с администрацией над несколькими недавними взломами. «Но они также сталкиваются с большей угрозой, чем мы когда-либо видели».

Но некоторые сотрудники спецслужб утверждали, что санкции и другие тайные действия - если таковые имели место - мало что говорят о сдерживании Путина. И поэтому г-н Байден видит в своем собственном Белом доме такие же энергичные дебаты по поводу того, необходимы ли более решительные меры, будь то разоблачение финансовых затруднений г-на Путина или проведение ответных кибератак.

Г-н Байден проявил осторожность, заявив в прошлом месяце, что он «решил быть соразмерным» в ответ на атаку SolarWinds, потому что не хотел «запускать цикл эскалации и конфликта с Россией».

Некоторые эксперты по кибербезопасности теперь утверждают, что г-ну Байдену следовало отреагировать более агрессивно.

«США склонны слишком зацикливаться на соразмерности», - сказал Джеймс А. Льюис, один из таких экспертов из Центра стратегических и международных исследований в Вашингтоне. «Мы слишком осторожно отреагировали на SolarWinds, и это оказалось ошибкой. Вы устанавливаете границы посредством действий, а не посылая им неприятные дипломатические записки ».

Американские официальные лица часто неохотно реагировали на кибератаки тем же, отчасти из-за того, что собственная защита страны неадекватна. «До тех пор, пока мы не будем уверены в своей способности отражать российские кибератаки, наши действия будут по-прежнему определяться опасениями по поводу того, что сделает Путин», - сказала Кирстен Тодт, управляющий директор Института кибер-готовности.

Но и правительственные чиновники, и некоторые эксперты утверждали, что захват электронной почты S.V.R. в современном мире постоянных киберконфликтных ситуаций было таким хлебом с маслом, что это не означало эскалации со стороны SolarWinds. «Для меня не очевидно, что этот тип атаки выходит за красную черту», - сказал Роберт Чесни, директор Центра Штрауса при Техасском университете в Остине.

В данном случае, как сообщает Microsoft, целью хакеров было не преследовать само агентство по оказанию помощи. Вместо этого его мотивация, по-видимому, заключалась в использовании электронных писем, якобы отправленных правительством США, для проникновения в группы, раскрывающие российские кампании дезинформации, антикоррупционные группы и тех, кто протестовал против отравления, осуждения и заключения в тюрьму самого известного лидера российской оппозиции., Алексей Алексеевич Навальный.

По данным SecureWorks, фирмы по кибербезопасности из Атланты, отслеживающей атаки, российские хакеры атаковали Атлантический совет и ЕС.

Disinfo Lab, которые разоблачили несколько российских дезинформационных кампаний.

Среди других целей - Организация по безопасности и сотрудничеству в Европе, которая вызвала гнев Путина за критику справедливости выборов в Беларуси и Украине; Украинский центр противодействия коррупции и Министерство иностранных дел Ирландии, по данным SecureWorks.

Г-н Путин ранее охарактеризовал Организацию по безопасности и сотрудничеству в Европе как «мерзкий инструмент Запада». Тот факт, что Россия нацелилась на эти цели, а не на федеральные сети, как это было с SolarWinds, наводит на мысль, что санкции, возможно, отвлекли Россию в другое место.

«Это может быть Россия и, в частности, Путин, который говорит:« Спасибо за санкции - теперь мы собираемся использовать открытые и уязвимые сети Америки для наших собственных политических целей и мести », - сказала г-жа Тодт.

Microsoft, как и другие крупные фирмы, занимающиеся кибербезопасностью, поддерживает обширную сенсорную сеть для поиска вредоносной активности в Интернете и часто сама является целью. Он был глубоко вовлечен в раскрытие атаки SolarWinds.

В самом последнем случае г-н Берт сказал, что Microsoft отслеживала хакеров, когда они взламывали систему массовой рассылки электронной почты, управляемую компанией Constant Contact, клиентом которой является Агентство международного развития.

«Им никогда не приходилось входить в правительственную систему США, - сказал г-н Берт. Вместо этого они взломали систему связи Constant Contact и проникли в аккаунт агентства. Это позволило им отправлять электронные письма, которые, по всей видимости, были от агентства.

В своем заявлении Constant Contact, не подтверждая личность своего клиента, предположил, что хакеры использовали украденные учетные данные для взлома учетных записей электронной почты агентства Constant Contact. «Это единичный инцидент, - говорится в заявлении, - и мы временно отключили затронутые аккаунты, пока работаем в сотрудничестве с нашим клиентом, который работает с правоохранительными органами».

Но российские хакеры воспользовались многими такими возможностями, говорят представители спецслужб. Помощники г-на Байдена заявили, что тот факт, что хакеры были пойманы так быстро, подчеркивает необходимость того, чтобы правительственные учреждения и поставщики придерживались новых стандартов, предусмотренных указом, изданным две недели назад. Это включает в себя требования к мониторингу, которые, скорее всего, вызовут тревогу в случаях, когда вредоносное ПО передается по электронной почте, и требования к отчетности в случае атак.

Представляя новый порядок в этом месяце, Энн Нойбергер, заместитель советника г-на Байдена по вопросам кибербезопасности и новых технологий, сказала, что новый порядок «поднимет игру» для всех, кто хочет вести дела с федеральным правительством, и что более высокие стандарты безопасности будет

распространяться через частный сектор. Есть некоторые признаки того, что это уже происходит.

Но противники тоже улучшаются. Microsoft отметила, что российская атака использовала новые инструменты и уловки, явно пытаясь избежать обнаружения. «Некоторые люди назвали бы это «шпионажем, как обычно», и это было так, - сказал г-н Берт. «Но ни одно правительство не хочет, чтобы какое-то другое правительство проживало в их сетях в течение трех месяцев». ***(David E. Sanger, Nicole Perlroth. Russia Appears to Carry Out Hack Through System Used by U.S. Aid Agency // The New York Times Company (https://www.nytimes.com/2021/05/28/us/politics/russia-hack-usaid.html?smtyp=cur&smid=tw-nytimes). 28.05.2021).***

***

«За прошедшие годы Москва столкнулась с многочисленными обвинениями в кибератаках, которые привели к множественным санкциям и высылке ее дипломатов. Термин «хакер» стал почти синонимом России.

Вот обзор мира российских киберпреступлений: от «фабрик троллей» до хакеров, предположительно контролируемых службами безопасности страны:

- *Навыки и умения* -

Россия на протяжении десятилетий была рассадником компьютерных экспертов. В советские времена правительство стремилось к развитию науки и технологий и - с появлением первых компьютеров - в программировании.

После распада СССР в 1991 году некоторые из талантливых, но малооплачиваемых программистов обратились к киберпреступности, что вскоре сделало россиян печально известными кражами кредитных карт по всему миру.

«В 90-е годы окружающая среда процветала благодаря культуре находчивости и тенденции обходить правила», - сказал Кевин Лимонье из Французского института геополитики.

- *Армия и службы безопасности* -

Эксперты говорят, что в своем непрекращающемся противостоянии с Западом Россия в значительной степени полагается на свои возможности кибернетической и информационной войны.

Несколько известных хакерских групп подозреваются в работе на службы безопасности страны, а в 2012 году российское министерство обороны создало собственные «кибер-подразделения».

Первая крупномасштабная атака, которую приписывают России, относится к 2007 году, когда балтийское государство Эстония столкнулось с волной кибератак на свои газеты, банки и правительственные министерства.

Соединенные Штаты заявляют, что хакеры российской военной разведки (ГРУ) пытались манипулировать президентскими выборами 2016 года, взломав Национальный комитет Демократической партии и кампанию Хиллари Клинтон.

Самая известная группа кибершпионажа, замешанная в десятках дел, известна как Fancy Bear или APT28. Считается, что его спонсирует правительство России.

По словам Вашингтона, атака на американского разработчика программного обеспечения SolarWinds была осуществлена Службой внешней разведки России и скомпрометировала правительственные учреждения и сотни частных компаний.

- *Информация и саботаж* -

«Кибератаки, осуществляемые российскими спецслужбами, являются частью многолетних международных операций, направленных на получение стратегической информации», - заявила немецкая разведка в 2016 году, имея в виду шпионские и диверсионные операции.

Список предполагаемых атак со стороны России длинный: хакерская атака на парламент Германии в 2015 году; нацелены на украинские артиллерийские подразделения в период с 2014 по 2016 год; взлом французской телесети в 2015 году; вмешательство в выборы в США в 2016 и 2020 годах и нацеливание на исследовательские институты вакцины против коронавируса на Западе в 2020 году.

Эксперты говорят, что атаки становятся все более изощренными.

«Уровень российских кибератак растет по сравнению с тем, что было три или четыре года назад», - сказал эксперт по разведке Андрей Солдатов.

«Мы знаем об операциях, которые были раскрыты, но многое еще остается эффективным».

- *Дезинформация* -

Россию также обвиняют в проведении крупномасштабных кампаний дезинформации с целью повлиять на демократические процессы на Западе и разжечь социальную рознь в Интернете.

Считается, что в стране действуют онлайн-«фабрики троллей», которые придумывают фальшивую вирусную информацию в попытке повлиять на пользователей Интернета.

Обвинения были направлены как против государственных СМИ, включая RT (бывшая Russia Today), так и против союзников Кремля, таких как Евгений Пригожин, бизнесмена, подозреваемого в том, что он стоял у истоков «фабрик троллей» в России и Африке.

Вашингтон обвинил союзника президента Владимира Путина в финансировании Internet Research Agency, компании из Санкт-Петербурга, которая стремилась повлиять на электорат США в 2016 году.

- *Отказ* -

Осознавая, что природа кибератак затрудняет отслеживание их происхождения, Кремль всегда отрицал свою причастность и обвинял Запад в ведении дезинформационной войны против России.

Россия также неоднократно заявляла о своем желании сотрудничать в киберсфере.

В преддверии президентских выборов в США 2020 года Путин предложил пакт о невмешательстве в выборы и глобальное соглашение против неправомерного использования коммуникационных технологий.

Предложение осталось без ответа.

Солдатов сказал, что Россия может использовать хакерские атаки, чтобы заставить Запад сотрудничать.

Он не исключил, что перед лицом российской угрозы и из-за отсутствия лучшей альтернативы «полиция Европы и США может захотеть вернуться к сотрудничеству с Россией по вопросам кибербезопасности». ***(Hack, disinform, deny: Russia's cybersecurity strategy // Microsoft News (https://www.msn.com/en-us/news/world/hack-disinform-deny-russia-s-cybersecurity-strategy/ar-AAKldXb). 25.05.2021).***

***

«По данным компании SentinelOne, связанной с безопасностью конечных точек, за последний год связанный с Ираном злоумышленник по имени Agrius под видом атак программ-вымогателей совершал разрушительные атаки на израильские цели.

Группа угроз, вероятно, спонсируемая государством, первоначально участвовала в кибершпионажных атаках, но затем попыталась вымогать у жертв, утверждая, что они перехватили и зашифровали данные. Однако восстановить поврежденные файлы не удалось из-за разрушительного характера атаки.

Вайпер, получивший название Apostle, позже был дополнен возможностями шифрования и превратился в полнофункциональную программу-вымогатель.

«Сходство с его версией Wiper, а также характер цели в контексте региональных споров заставляют нас думать, что операторы, стоящие за ним, используют программы-вымогатели для их разрушительных возможностей», - говорит SentinelOne.

Для вторжения используются уязвимости в приложениях с выходом в Интернет, включая CVE-2018-13379, уязвимость обхода пути высокой степени серьезности на веб-портале FortiOS SSL VPN и различные ошибки безопасности в других веб-приложениях.

Исследователи говорят, что Agrius использует службы VPN для подключения к средам жертв и использует веб-оболочки (в основном разновидности ASPXSpy) для туннелирования трафика RDP и использования скомпрометированных учетных записей для бокового перемещения.

Злоумышленники также используют общедоступные инструменты для сбора учетных данных и расширения своих позиций в скомпрометированной среде. Они также развертывают свой собственный бэкдор.NET, получивший название IPsec Helper, на интересующие цели, чтобы украсть данные и при необходимости развернуть дополнительные полезные нагрузки.

Помимо Apostle, группа угроз наблюдалась с помощью дворника DEADWOOD, который ранее использовался при атаке на цель в Саудовской Аравии в 2019 году. Однако большинство целей противника из Израиля и, вероятно, выбраны случайно. SentinelOne считают исследователи.

Кодекс Apostle схож с IPsec Helper, вероятно, потому, что они оба разработаны собственными силами. Первоначальная версия вредоносного ПО содержала только возможности очистки, но не выполняла ожидаемое действие, что привело к развертыванию очистителя DEADWOOD.

В этом году злоумышленник представил второй вариант Apostle, который обладает возможностями вымогателя, но использует старый метод очистки для удаления исходных файлов после шифрования.

В ходе своего расследования исследователи SentinelOne не обнаружили связей между методами, инструментами и инфраструктурой Agrius и известными субъектами угроз, но выявили доказательства, свидетельствующие о том, что злоумышленник действует за пределами Ирана.

«Agrius - это новая группа угроз, которую мы со средней степенью уверенности оцениваем как иранское происхождение, занимающуюся как шпионажем, так и подрывной деятельностью. Группа использует свой собственный набор инструментов, а также общедоступные средства защиты для атак на различные организации на Ближнем Востоке», - отмечает SentinelOne.

Исследователи также отмечают, что группа может быть частью более крупной скоординированной иранской стратегии, которая также включает недавно обнаруженные атаки Pay2Key. Однако разрушительный характер атак Agrius, которые продолжались до мая 2021 года, предполагает, что у группы нет финансовой мотивации». ***(Ionut Arghire. New Iranian Group 'Agrius' Launches Destructive Cyberattacks on Israeli Targets // Wired Business Media (https://www.securityweek.com/new-iranian-group-agrius-launches-destructive-cyberattacks-israeli-targets). 27.05.2021).***

***

«Военные Великобритании опасаются, что авианосная группа с кораблем Queen Elizabeth во время 28-недельного похода может быть атакована хакерами.

По информации газеты Times, подобные опасения были высказаны после того, как генсек НАТО Йенс Столтенберг заявил о масштабе киберугроз и отработке противодействия им в ходе учений, передает РИА «Новости».

По словам командира авианосной группы Стива Мурхауза, на кораблях британской группы присутствует команда экспертов в сфере цифровых технологий, которые должны отслеживать аномалии в этом вопросе.

Специалисты считают, что кибератака наиболее вероятна осенью, когда корабль подойдет к берегам Японии. Тогда всем членам экипажа прикажут отключить мобильные телефоны и даже вынуть из них SIM-карты. Пользоваться электронной почтой разрешат только командиру авианосца.

Также британские военные считают, кто Queen Elizabeth могут взломать во время прохода мимо берегов Сирии, где размещены российские военные». ***(Британцы боятся взлома "Королевы Елизаветы" // SecurityLab.ru (https://www.securitylab.ru/news/520671.php). 28.05.2021).***

***

«Пресс-секретарь президента России Дмитрий Песков назвал абстрактными и голословными обвинения компании Microsoft в том, что новые кибератаки на госструктуры США якобы совершили российские хакеры.

Таким образом он ответил на антироссийское заявление представителя компании Microsoft о «русских» хакерах, якобы «причастных» к киберпреступлениям. Песков счел слова достаточно абстрактными, он сравнил его голословность с вымышленным обвинением корпорации в распространении угроз от программного обеспечения.

Инцидент не повлияет на ход развития двустороннего саммита президента РФ Владимира Путина и главы Белого дома Джозефа Байдена, уверен пресс-секретарь лидера государства.

Говоря о возможном росте напряжённости между РФ и США из-за «атаки хакеров», представитель Кремля отметил, что сначала нужны данные о хакерской группе, её якобы связях с Россией, деталях нападения и прочем…». ***(Кремль отреагировал на обвинения Microsoft в кибератаках // SecurityLab.ru (https://www.securitylab.ru/news/520678.php). 30.05.2021).***

***

Кіберзахист критичної інфраструктури

«Администрация Байдена взяла на себя обязательство сделать кибербезопасность своим главным приоритетом и теперь обращает внимание на энергетическую инфраструктуру, которая широко признана уязвимой для кибератак из-за систем управления энергосистемой. Министерство энергетики США (DOE) запустило 100-дневную инициативу по «продвижению технологий и систем, которые обеспечат кибер-видимость, обнаружение и возможности реагирования для промышленных систем управления электроэнергетическими предприятиями».

Сообщается, что с тех пор, как эта инициатива была объявлена 20 апреля 2021 года, Colonial Pipeline стала жертвой атаки вымогателей, в результате которой трубопровод был остановлен в качестве меры предосторожности. Colonial Pipeline поставляет почти пятьдесят процентов бензина, дизельного топлива и авиационного топлива Восточного побережья. Атака была одной из самых успешных кибератак на нефтяную инфраструктуру в США на сегодняшний день и подчеркивает уязвимость критически важной инфраструктуры США.

Инициатива Министерства энергетики выделяет четыре основных направления: (1) поощрение реализации мер, которые повышают «возможности обнаружения, смягчения последствий и судебной экспертизы; (2) установление «конкретных этапов», разработанных для «обеспечения возможности ситуационной осведомленности и реагирования в режиме, близком к реальному времени»; (3) поддержка и повышение «кибербезопасности критически важных инфраструктурных информационных технологий (ИТ) сетей»; и (4) создание добровольной программы «по развертыванию технологий для повышения видимости угроз в системах ICS и OT»… ***(Leah Kaiser. Cybersecurity Focus Shifts to Energy Infrastructure // Husch Blackwell LLP (https://www.contractorsperspective.com/cybersecurity/cybersecurity-focus-shifts-to-energy-infrastructure/). 18.05.2021).***

***

«Министерство торговли, энергетики и инфраструктуры Южной Кореи приказало провести обзор готовности к кибербезопасности энергетической инфраструктуры страны.

Министр торговли, промышленности и энергетики Мун Сын Ук созвал вчера встречу, заявив, что это необходимо с учетом атаки программ- вымогателей на колониальный трубопровод, закрывшего один из основных объектов транспортировки нефти в США.

«После сбоя необходимо тщательно изучить, правильно ли приняты меры по обеспечению кибербезопасности и меры противодействия нашей энергетической инфраструктуре», - сказал министр, прежде чем обратиться к операторам нефтепроводов, электросетей, газопроводов и системы аварийного реагирования, чтобы проверить состояние своих систем и сообщить о своих выводах.

Также в повестке дня на поспешно созванном заседании было обсуждение правительственных мер противодействия нападениям, подобным тем, которые поразили колониальный трубопровод.

Зимой в Южной Корее очень холодно, при этом среднесуточные температуры ниже нуля с декабря по февраль. Перебои в энергоснабжении могут оказаться катастрофическими.

В Америке, тем временем, Colonial Pipeline заявляет, что могла проводить ручные операции на небольших участках своей инфраструктуры, но панические закупки привели к нехватке топлива, и цены на топливо выросли. Несколько штатов США приняли меры, чтобы либо разрешить автомобильную перевозку топлива, либо предотвратить взвинчивание цен.

Colonial установила пятницу как день, в который надеется восстановить полный спектр услуг. Южная Корея, похоже, надеется, что ей никогда не придется принимать такие меры». ***(Simon Sharwood. South Korea orders urgent review of energy infrastructure cybersecurity // The Register (https://www.theregister.com/2021/05/12/south_korea_security_review/). 12.05.2021).***

***

Захист персональних даних

«13 мая Окружной суд США Северного округа Калифорнии предварительно одобрил мировое соглашение, разрешив обвинения в том, что базирующаяся в Калифорнии торговая площадка онлайн-дизайнеров не смогла защитить личную информацию клиентов от группы компьютерных хакеров в результате утечки данных в мае 2020 года. Истцы заявили о халатности и подали иски в соответствии с Законом Калифорнии о конфиденциальности потребителей и Законом о недобросовестной конкуренции после того, как истцы начали расследование инцидента, связанного с кибербезопасностью. Предварительное урегулирование требует, чтобы компания

учредила расчетный фонд в размере 5 миллионов долларов, который «обеспечит выплату примерно 43 долларов США на каждого участвующего члена группы, двухлетний кредитный мониторинг и услуги по восстановлению личности». Компания также должна внести несколько изменений в бизнес-практику для повышения безопасности, включая усиление защиты паролем и реализацию политики, направленной на минимизацию сохранения информации, позволяющей установить личность клиентов. В соглашении также отмечается, что «участники, ставшие жертвами кражи личных данных, могут также получить помощь в разрешении мошенничества для оспаривания транзакций, посредничества при звонках с продавцами и реализации предупреждений о мошенничестве». Члены группы, которые не согласны с мировым соглашением, могут отказаться от него до 16 сентября». ***(District Court approves online marketplace data breach settlement // Buckley LLP (https://buckleyfirm.com/blog/2021-05-18/district-court-approves-online-marketplace-data-breach-settlement#page=1). 18.05.2021).***

***

«11 мая 2021 года сенаторы Эдвард Марки (D-MA) и Билл Кэссиди (R-LA) представили Закон о защите конфиденциальности детей и подростков в Интернете («Законопроект»). Законопроект, который внесет поправки в существующий Закон о защите конфиденциальности детей в Интернете (COPPA), запретит компаниям собирать личную информацию от детей в возрасте от 13 до 15 лет без их согласия.

Стандарт расширенного согласия будет применяться в тех случаях, когда компании «обоснованно знают», что на их платформах присутствуют дети. Этот стандарт конструктивных знаний отличается от стандарта «фактических знаний» в соответствии с COPPA, согласно которому согласие родителей требуется только в том случае, если оператор веб-сайта действительно знает, что платформу используют дети младше 13 лет. В частности, законопроект потребует согласия пользователя, если ему от 13 до 15 лет (а не согласия родителей, которое требуется для сбора информации от детей младше 13 лет в соответствии с COPPA).

Законопроект содержит ряд других положений, в том числе (1) запрет на целевую рекламу, ориентированную на детей; (2) определенные требования к уведомлениям, относящиеся к сбору, использованию и раскрытию личной информации детей для операторов веб-сайтов и производителей подключенных устройств; (3) требования к кибербезопасности для подключенных к Интернету устройств, предназначенных для детей; (4) создание «кнопки-ластика» для родителей и детей, требующей от компаний разрешать пользователям удалять личную информацию ребенка или подростка, если это технически возможно; и (5) создание отдела молодежного маркетинга и конфиденциальности при Федеральной торговой комиссии». ***(Senate Bill Would Expand Federal Children's Privacy Protections // Hunton Andrews Kurth LLP (https://www.huntonprivacyblog.com/2021/05/12/senate-bill-would-expand-federal-childrens-privacy-protections/#page=1). 12.05.2021).***

***

«Калифорнийский университет (UC) на этой неделе подтвердил, что личная информация была украдена в результате кибератаки с использованием службы Accellion File Transfer Appliance (FTA).

Инцидент, произошедший в конце декабря 2020 года после обнаружения критической уязвимости в сервисе обмена файлами, которому уже несколько десятилетий, затронул десятки компаний, государственных учреждений и университетов.

Первоначально UC подтвердил влияние инцидента в начале апреля, после того как операторы программы-вымогателя Clop, которая организовала атаку на сервис Accellion, опубликовали на своем веб-сайте утечек на базе Tor информацию, предположительно украденную у университета и других организаций.

На этой неделе университет подтвердил, что злоумышленники действительно смогли получить доступ к большому количеству личной информации, относящейся к «сотрудникам (нынешним и бывшим) и их иждивенцам, пенсионерам и бенефициарам, а также нынешним студентам, а также другим лицам, которые участвовали в программах UC.»

Украденная информация может включать имена и адреса, номера социального страхования, номера телефонов, водительские права и паспортные данные, финансовые данные (включая банковские маршруты и номера счетов), даты рождения, сведения о состоянии здоровья и связанных с ними льготах, информацию об инвалидности и другие данные.

Университет, который также подтвердил, что часть украденной информации была размещена в Интернете, заявляет, что сотрудничает с ФБР в расследовании инцидента.

Кроме того, в то время как он уведомляет пострадавших лиц, университет «работает над выявлением членов сообщества, чья личная информация была затронута, и их контактной информации» и ожидает, что пострадавшие люди получат уведомление в течение следующих 45-60 дней.

«Мы также отдельно уведомляем лиц, которые начали или заполнили заявки на 2021-22 учебный год, чья контактная информация (имя, адрес электронной почты и номер телефона) была затронута. В их уведомлении будет содержаться информация, касающаяся этих лиц», - отмечают в университете.

Нарушение данных затронуло только Accellion FTA, никакие другие системы не пострадали. Университет заявляет, что он уже списал службу обмена файлами, что он переходит на более безопасное решение и что он предпринимает шаги для повышения общей безопасности своей сети». ***(Ionut Arghire. University of California Confirms Personal Information Stolen in Cyberattack // Wired Business Media (https://www.securityweek.com/university-california-confirms-personal-information-stolen-cyberattack). 11.05.2021).***

***

«В пятницу город Чикаго заявил, что электронные письма сотрудников были скомпрометированы в результате взлома данных Jones Day, связанного с файловым сервисом Accellion FTA.

Кибератака началась в декабре 2020 года, когда критическая уязвимость была обнаружена в 20-летнем сервисе передачи больших файлов, срок службы которого истек 30 апреля 2021 года.

Около 50 клиентов все еще использовали FTA, когда произошел инцидент с безопасностью, но только некоторые из них испытали значительную потерю данных, утверждает Accellion.

В феврале 2021 года крупная американская юридическая фирма Jones Day подтвердила, что на нее повлияла атака, после того как киберпреступники, стоящие за вымогателем Clop, опубликовали на своем веб-сайте утечек на базе Tor документы, предположительно украденные у компании.

В пятницу город Чикаго сообщил, что в ходе инцидента были скомпрометированы электронные письма некоторых сотрудников, которые были отправлены Jones Day «в рамках независимого расследования, проводимого фирмой».

Нарушение данных затронуло только службу Accellion FTA и было связано с «электронными письмами, отправленными или полученными от четырех бывших сотрудников City в течение двухлетнего периода», - заявили в городе.

Городской департамент активов, информации и услуг (AIS) Чикаго уже уведомил ФБР и офис генерального прокурора Иллинойса об утечке и предпринял необходимые действия, чтобы гарантировать, что электронные письма были удалены из службы передачи файлов.

«Хотя городу не известно о каком-либо мошенничестве, которое могло произойти в результате этого события, он очень серьезно отнесся к этому вопросу и отреагировал соответствующим образом», - говорят в городе.

Кроме того, город заявляет, что смог определить количество пострадавших людей и что он уже предпринял шаги для уведомления лиц, у которых могла быть личная информация, включенная в скомпрометированные файлы электронной почты, либо напрямую, либо через уведомление на своем веб-сайте и общегосударственное оповещение СМИ». ***(Ionut Arghire. City of Chicago Hit by Data Breach at Law Firm Jones Day // Wired Business Media (https://www.securityweek.com/city-chicago-hit-data-breach-law-firm-jones-day). 10.05.2021).***

***

«Исследователи, анализирующие приложения для Android, обнаружили серьезные неправильные конфигурации облака, которые потенциально могут привести к раскрытию данных, принадлежащих более чем 100 миллионам пользователей.

В отчете, опубликованном в четверг Check Point Research, компания, занимающаяся кибербезопасностью, сообщила, что не менее 23 популярных мобильных приложений содержат различные «неправильные конфигурации сторонних облачных сервисов».

Облачные сервисы сегодня широко используются онлайн-сервисами и приложениями, возможно, даже в большей степени из-за быстрого перехода на удаленную работу, вызванного пандемией коронавируса. Хотя это полезно для

управления, хранения и обработки данных, требуется только один контроль доступа или авторизации для раскрытия или утечки хранимых записей.

В частности, приложения часто интегрируются с базами данных в реальном времени для хранения и синхронизации данных на разных платформах. Однако разработчики некоторых исследованных приложений не смогли убедиться в наличии механизмов аутентификации.

Согласно CPR, из 23 исследованных приложений для Android, включая приложение для такси, средство создания логотипов, устройство записи экрана, службу факсов и астрологическое программное обеспечение, произошла утечка данных, включая записи электронной почты, сообщения чата, информацию о местоположении, идентификаторы пользователей, пароли и изображения.

В 13 случаях конфиденциальные данные были общедоступными в незащищенных облачных установках. На каждое из этих приложений было загружено от 10 000 до 10 миллионов загрузок.

Например, при исследовании приложения службы такси команда смогла отправить один простой запрос в базу данных приложения и получить сообщения, отправленные между водителями и клиентами, с именами, номерами телефонов, а также с пунктами посадки и высадки.

Облачные службы, обеспечивающие внутреннее управление данными для приложений записи с экрана и факсов, также не были должным образом защищены. CPR смог восстановить ключи для предоставления доступа к сохраненным записям и факсимильным документам, проанализировав файлы приложений.

Ключи push-уведомлений также были обнаружены в приложениях, оставшись открытыми для злоупотреблений. Если используются push-сервисы, их можно использовать для отправки злонамеренных предупреждений пользователям приложения.

Исследователи говорят, что эти сбои в системе безопасности вызваны тем, что разработчики не следуют «лучшим практикам при настройке и интеграции сторонних облачных сервисов в свои приложения».

«Эта неправильная конфигурация баз данных реального времени не нова, но [..] масштаб проблемы все еще слишком широк и затрагивает миллионы пользователей», - говорит CPR. «Если злоумышленник получит доступ к этим данным, это может потенциально привести к служебному смахиванию (попытка использования той же комбинации имени пользователя и пароля в других службах), мошенничеству и краже личных данных».

CPR проинформировал разработчиков приложений о неправильных настройках до раскрытия информации, и некоторые ужесточили свои меры контроля.

Ранее в этом месяце исследователи опубликовали рекомендации по службам данных Qualcomm MSM и обнаружению уязвимости, которая теоретически может быть использована для взлома и внедрения вредоносного кода в модемы телефонов Android». ***(Charlie Osborne. Android apps exposed data of millions of users through cloud authentication failures // ZDNet (https://www.zdnet.com/article/cloud-services-used-by-android-apps-exposed-data-of-millions-of-users/). 20.05.2021).***

***

«Британский железнодорожный оператор West Midlands Trains отправил электронное письмо 2500 сотрудникам, чтобы поблагодарить их за тяжелую работу во время COVID и пообещал разовый бонус в качестве награды, но эта прекрасная новость оказалась обучением фишингу. Излишне говорить, что все прошло не очень хорошо.

В заведомо недостоверном электронном письме сначала поблагодарили сотрудников за их усердную работу, а затем добавили: «Мы понимаем, что в результате COVID-19 на большое количество наших сотрудников возникла огромная нагрузка... и мы хотели бы предложить вам одно - выплата, чтобы поблагодарить вас за всю вашу тяжелую работу за последние 12 месяцев или около того».

Читателям было предложено щелкнуть ссылку, чтобы зарегистрироваться для получения бонуса, но тем, кто следовал инструкциям, были отправлены новости об их сбоях в информационной безопасности и предложены полезные советы на будущее, такие как «будьте бдительны со всеми ссылками и вложениями» и «никогда не переходите по ссылке». это выглядит подозрительно».

Электронное письмо сотрудникам West Midland Trains рационализировало тест следующим текстом:

Этот тест был специально разработан, чтобы точно имитировать тактику, которая, к сожалению, ежедневно используется опытными преступными организациями, чтобы попытаться получить доступ к данным и системам компании.

Ассоциация наемных работников транспорта (TSSA) опубликовала заявление, в котором генеральный секретарь Мануэль Кортес назвал неудачные попытки учений по кибербезопасности «циничным и шокирующим трюком». Профсоюз охарактеризовал такое поведение как «абсолютно грубое и предосудительное» и сослался на многочисленные случаи COVID и одну смерть среди основных сотрудников компании как на свидетельство бесчувственности руководства.

Мероприятие может дорого обойтись британской железнодорожной компании, поскольку Кортес потребовал, чтобы компания выполнила обязательства и предоставила обещанные бонусы.

Более того, хотя «тест», возможно, облегчил ИТ-отделу поиск недостатков безопасности, похоже, что он заставил много работать антикризисную группу по связям с общественностью West Midland Trains, хотя, похоже, они еще не прижились.

West Midlands Railway предложила, если вас не устраивает их ответ на данный момент или его отсутствие, вы можете подать официальную жалобу в Интернете.

Письмо с проверкой фишинга утверждалось, что оно пришло со стола недавно назначенного управляющего директора West Midland Trains Джулиана Эдвардса.

Что просто подтверждает старую поговорку о том, что фишинг гниет из головы». ***(Laura Dobberstein. Train operator phlunks phishing test by teasing***

employees with non-existent COVID bonus // The Register (https://www.theregister.com/2021/05/11/west_midlands_trains_phishing_drill_goes_off/). 11.05.2021).

***

«Платформа электронной коммерции Mercari раскрыла крупный инцидент с утечкой данных, произошедший из-за атаки на цепочку поставок Codecov.

Mercari - это публичная японская компания и онлайн-торговая площадка, которая недавно расширила свою деятельность на Соединенные Штаты и Соединенное Королевство.

По состоянию на 2017 год приложение Mercari было загружено более 100 миллионов раз по всему миру, и компания первой в Японии достигла статуса единорога.

Как ранее сообщал BleepingComputer, популярный инструмент покрытия кода Codecov стал жертвой атаки цепочки поставок, которая длилась два месяца.

В течение этого двухмесячного периода злоумышленники модифицировали законный инструмент Codecov Bash Uploader для извлечения переменных среды (содержащих конфиденциальную информацию, такую как ключи, токены и учетные данные) из сред CI / CD клиентов Codecov.

Сообщается, что используя учетные данные, полученные из подделанного Bash Uploader, злоумышленники Codecov взломали сотни клиентских сетей.

Крупная утечка данных раскрывает тысячи финансовых записей клиентов

Сегодня гигант электронной коммерции Mercari раскрыл серьезное влияние атаки на цепочку поставок Codecov на данные своих клиентов.

Компания подтвердила, что десятки тысяч клиентских записей, включая финансовую информацию, были раскрыты внешним субъектам из-за нарушения Codecov.

Завершив расследование сегодня, 21 мая, Mercari заявляет, что скомпрометированные записи включают:

17 085 записей, связанных с переводом выручки от продаж на счета клиентов, произошедшим в период с 5 августа 2014 г. по 20 января 2014 г.

Доступная информация включает код банка, код отделения, номер счета, владельца счета (кана), сумму перевода.

7 966 записей о деловых партнерах «Mercari» и «Merpay», включая имена, дату рождения, принадлежность, адрес электронной почты и т. Д., Доступны для некоторых.

2615 записей о некоторых сотрудниках, включая сотрудников дочерней компании Mercari

Имена некоторых сотрудников по состоянию на апрель 2021 года, адрес электронной почты компании, идентификатор сотрудника, номер телефона, дата рождения и т. д.

Подробная информация о бывших сотрудниках, некоторых подрядчиках и сотрудниках сторонних компаний, которые взаимодействовали с Mercari.

С ноября 2015 г. по январь 2018 г. зарегистрировано 217 обращений в службу поддержки клиентов.

Доступные данные включают имя клиента, адрес, адрес электронной почты, номер телефона и содержание запроса.

6 записей, связанных с событием, произошедшим в мае 2013 года…

Mercari полностью отказывается от Codecov после месячного расследования

Mercari стало известно о последствиях взлома Codecov вскоре после того, как Codecov впервые раскрыла свою информацию в середине апреля.

23 апреля GitHub также уведомил Mercari о подозрительной активности, связанной с инцидентом, замеченным в репозиториях Mercari.

В тот же день Mercari начал копать глубже и запросил у GitHub подробные журналы доступа.

В конце концов, сотрудники Mercari определили, что третья сторона-злоумышленник приобрела и неправильно использовала их учетные данные для аутентификации, получила доступ к частным репозиториям Mercari (включая исходный код) и получила дальнейший несанкционированный доступ к его системам в период с 13 по 18 апреля.

Обнаружив эту атаку, Mercari немедленно деактивировал скомпрометированные учетные данные и секреты и продолжил исследование всех последствий взлома.

27 апреля Mercari обнаружила, что некоторая информация о клиентах и исходный код были незаконно доступны неавторизованным сторонам.

Компания заявляет, что ей пришлось ждать раскрытия утечки данных до сегодняшнего дня, потому что ее расследование продолжалось. И пока какие-либо слабые места в системе безопасности не будут полностью выявлены и устранены, компания рискует подвергнуться дальнейшим атакам и ущербу.

Mercari завершила расследование и, следовательно, представила подробное раскрытие информации сегодня…

Mercari индивидуально связалась с людьми, чья информация была скомпрометирована, а также уведомила соответствующие органы, включая Комиссию по защите личной информации Японии, об этой утечке данных:

«Одновременно с этим объявлением мы незамедлительно предоставим индивидуальную информацию тем, кто стал объектом утечки информации по этому поводу, и мы также создали специальный контактный пункт для запросов по этому поводу».

«В будущем мы продолжим внедрять дополнительные меры по повышению безопасности и расследовать этот вопрос, используя знания внешних экспертов по безопасности, и будем незамедлительно сообщать о любой новой информации, которая должна быть объявлена».

«Мы искренне приносим извинения за любые неудобства и беспокойство, вызванные этим вопросом», - говорится в приблизительном переводе оригинального пресс-релиза Меркари.

Сегодняшнее раскрытие информации произошло после того, как несколько компаний недавно заявили о воздействии атаки цепочки поставок Codecov на их частные репозитории. К ним относятся производитель программного обеспечения

HashiCorp, платформа облачных коммуникаций Twilio, поставщик облачных услуг Confluent, страховая компания Coalition, американская фирма по кибербезопасности Rapid7 и платформа управления рабочими процессами Monday.com.

В прошлом месяце Codecov также начал рассылать дополнительные уведомления пострадавшим клиентам и раскрыл подробный список индикаторов взлома (IOC), то есть IP-адресов злоумышленников, связанных с этой атакой цепочки поставок.

Пользователи Codecov должны сканировать свои CI / CD-среды и сети на предмет каких-либо признаков взлома и в качестве меры предосторожности чередовать все секреты, которые могли быть раскрыты». ***(Ax Sharma. E-commerce giant suffers major data breach in Codecov incident // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/e-commerce-giant-suffers-major-data-breach-in-codecov-incident/). 21.05.2021).***

***

«Компания по страхованию здоровья студентов guard.me отключила свой веб-сайт после того, как уязвимость позволила злоумышленнику получить доступ к личной информации страхователей.

guard.me - одна из крупнейших в мире страховых компаний, специализирующаяся на страховании здоровья студентов во время поездок или учебы за границей в другой стране.

12 мая Guard.me обнаружил на своем веб-сайте подозрительную активность, которая вынудила их закрыть свой веб-сайт. При посещении веб-сайта посетители автоматически перенаправляются на страницу обслуживания с предупреждением о том, что сайт не работает, в то время как страховая компания увеличивает безопасность на сайте.

«Недавняя подозрительная активность была направлена на веб-сайт guard.me, и мы, проявив большую осторожность, немедленно удалили этот сайт. Наши ИТ-специалисты и специалисты по информационной безопасности пересматривают меры по обеспечению повышенной безопасности сайта, чтобы вернуть его в полную работоспособность. как можно быстрее». - сообщает сайт guard.me.

Сегодня guard.me начал рассылать студентам уведомление об утечке данных, обнаруженное BleepingComputer, в котором говорится, что уязвимость веб-сайта позволяет посторонним лицам получить доступ к личной информации страхователей.

«Поздним вечером 12 мая 2021 года наша команда информационных систем обнаружила необычную активность на нашем веб-сайте, и в качестве меры предосторожности они немедленно отключили веб-сайт и предприняли немедленные шаги для защиты наших систем. Уязвимость устранена. Наши специалисты проводят тщательное расследование дело дальше», - говорится в уведомлении Guard.me о взломе данных.

Эта уязвимость позволяла злоумышленнику получить доступ к дате рождения, полу и зашифрованным паролям учащихся. Для некоторых студентов

также были раскрыты их адреса электронной почты, почтовые адреса и номера телефонов.

guard.me заявляет, что они устранили уязвимость и что она выдержала дальнейшие попытки их команды по кибербезопасности обойти дополнительные меры безопасности.

Страховая компания также заявляет, что они вводят новые политики для повышения безопасности, включая сегментацию базы данных и двухфакторную аутентификацию.

Поскольку компания является канадской, неясно, сообщил ли guard.me о нарушении уполномоченному по конфиденциальности Канады и не ответил на запросы BleepingComputer о предоставлении дополнительной информации». ***(Lawrence Abrams. Student health insurance carrier Guard.me suffers a data breach // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/student-health-insurance-carrier-guardme-suffers-a-data-breach/). 17.05.2021).***

***

«Киберпреступники используют вымогательство с целью кражи данных, создавая темные торговые площадки, которые существуют исключительно для продажи украденных данных.

Задолго до того, как банды вымогателей начали вымогать жертв с помощью украденных данных, другие злоумышленники уже использовали эту практику.

Одним из известных и широко известных хакеров, которые выполнили эту практику, был The Dark Overlord, который украл данные и потребовал выкуп от Disney, Netflix и страховых компаний.

Группа Maze Ransomware произвела революцию в операциях с программами-вымогателями в 2019 году, приняв стратегию двойного вымогательства. Используя сайты утечки данных программ-вымогателей, Maze предупредил жертв, что они публично утекут украденные данные, если жертвы не заплатят выкуп.

Другие банды быстро взяли на вооружение эту тактику вымогательства.

Некоторые злоумышленники сообщили BleepingComputer, что практика кражи данных и угроз их разглашения часто приводит к большему количеству выкупа, чем потеря зашифрованных файлов.

Этот сдвиг в тактике можно увидеть в недавнем заявлении программ-вымогателей Babuk о том, что они больше не будут шифровать устройства и переходят исключительно к вымогательству кражи данных.

Рост рынка украденных данных

Поскольку нарушения происходят почти каждый день, а правительства налагают большие штрафы за раскрытие личной информации, злоумышленники теперь извлекают выгоду из этих опасений, используя специальные торговые площадки, на которых продаются украденные данные.

Хотя темные веб-площадки для незаконных товаров не новы и использовались для продажи украденных данных в прошлом, они не были предназначены исключительно для вымогательства кражи данных.

Недавно BleepingComputer обнаружил две новые торговые площадки под названием Marketo и File Leaks, созданные для продажи данных другим

злоумышленникам или обратно самим жертвам. Кроме того, есть одна торговая площадка под названием Dark Leak Market, которая, похоже, была создана в 2019 году.

Рынок Dark Leak

Самая старая из этих торговых площадок - Dark Leak Market, которая продает украденные данные с 2019 года.

Объем данных, продаваемых на этом сайте, варьируется от 100 до 9000 долларов, и они были собраны с сайтов утечки данных банд вымогателей и хакерских форумов, таких как RaidForums.

Используя интеллектуальную платформу KELA DarkBeast, BleepingComputer обнаружил сообщение Unknown REvil Ransomware, подтверждающее, что данные перепродаются из-за других утечек данных.

Торговая площадка Marketo

В прошлом месяце злоумышленники запустили новую торговую площадку под названием Marketo, владелец которой связывается с журналистами и исследователями безопасности для продвижения сайта.

«Мы хотели бы представить новую торговую площадку Marketo, которая вскоре станет лучшим местом для поиска, покупки и продажи любой информации о любой компании», - написал BleepingComputer злоумышленник, стоящий за Marketo.

Когда мы спросили, были ли эти данные украдены в результате их собственных или других атак, они ответили: «Это торговая площадка для людей, у которых есть информация для продажи, мы не взламываем компании».

Они также утверждали, что выступают против программ-вымогателей и не связаны с «теми, кто блокирует сети и вымогает деньги».

Хотя большая часть данных, найденных на сайте, похоже, не связана с известными атаками программ-вымогателей, это не означает, что они не размещают данные от этих типов атак.

BleepingComputer недавно был предупрежден кем-то из индустрии автомобильной кибербезопасности, который видел данные о Marketo для дилерского центра, который, как известно, недавно пострадал от атаки вымогателя.

Торговая площадка утечек файлов

Торговая площадка File Leaks была запущена в апреле 2021 года и сразу сбрасывает все украденные данные, предлагая жертвам связаться с ними и заплатить за их удаление.

Торговая площадка утечек файлов - самый маленький из сайтов: две жертвы из Италии и один из Индии.

Выплата выкупа - это выбрасывание денег

Как мы сообщали в ноябре, жертвы никогда не должны платить выкуп за украденные данные, поскольку нет гарантии, что их данные будут удалены и не проданы другим злоумышленникам.

Компания Coveware, занимающаяся переговорами о программах-вымогателях, сообщила BleepingComputer, что киберпреступники все чаще не выполняют свои обещания после выплаты выкупа.

В некоторых случаях у жертв, которые заплатили, позже снова вымогали деньги, используя те же данные, или злоумышленники все равно слили данные.

Кроме того, как показывает рынок Dark Leak Market, после утечки данных невозможно сдержать их, поскольку они распространяются между различными хакерскими форумами и сайтами, посещаемыми злоумышленниками.

Помня об этом, Coveware советует жертвам всегда ожидать следующего, если они решат заплатить банде программ-вымогателей за предотвращение утечки данных:

Данные не будут удалены. Жертвы должны предполагать, что он будет продан другим субъектам угрозы, продан или удержан для второй / будущей попытки вымогательства.

Хранение украденных данных осуществлялось несколькими сторонами и не защищалось. Даже если злоумышленник удаляет объем данных после платежа, другие стороны, имевшие к нему доступ, могли сделать копии, чтобы они могли вымогать у жертвы в будущем.

Данные могут быть опубликованы по ошибке или намеренно, прежде чем жертва сможет даже ответить на попытку вымогательства.

Вместо этого жертвы кражи данных всегда должны рассматривать атаку как нарушение данных и должным образом сообщать о нарушении всем клиентам, сотрудникам и деловым партнерам, чтобы предотвратить нанесение им ущерба в результате кражи данных». ***(Lawrence Abrams. Data leak marketplaces aim to take over the extortion economy // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/data-leak-marketplaces-aim-to-take-over-the-extortion-economy/). 07.05.2021).***

***

«Группа хакеров получила доступ к конфиденциальным данным и учетным записям, связанным с десятками миллионов клиентов, водителей и сотрудников испанского приложения для доставки Glovo, как сообщила компания Yarix, занимающаяся кибербезопасностью.

Во вторник было объявлено, что злоумышленники пытаются продать архив с клиентской базой данных в даркнете - части Интернета, недоступной для обычных веб-браузеров - с примерно 160 гигабайтами имен, телефонных номеров, паролей и данных, связанных с платежными системами клиентов. Сообщается, что лот выставлен на продажу примерно за 85000 долларов.

«Несмотря на то, что неавторизованная третья сторона могла получить доступ к номерам IBAN и Tax ID в течение короткого периода времени, мы можем подтвердить, что к данным кредитной/дебетовой карты не было доступа», - сказал представитель Glovo.

Ранее 4 мая издание Forbes сообщало, что данные приложения Glovo были взломаны. Пока неизвестно, какие именно данные продаются в даркнете и имеют ли они отношение к недавнему взлому, который Glovo подтвердил Forbes.

Мирко Гатто, генеральный директор Yarix, сказал, что его компания смогла получить выдержки из украденной базы данных, которые включали платежные реквизиты и учетные данные для доступа к Glovo.

«Пользователям Glovo настоятельно рекомендуется изменить свой пароль и следить за своими кредитными картами, чтобы убедиться, что нет аномальных платежей», - порекомендовал Гатто». ***(Романов Роман. Конфиденциальные данные пользователей сервиса Glovo выставлены на продажу в даркнете // Internetua (http://internetua.com/konfidencialnye-dannye-polzovatelei-servisa-glovo-vystavleny-na-prodaju-v-darknete). 12.05.2021).***

***

«Національна авіакомпанія Індії Air India заявила, що кібератака на її сервери даних торкнулася близько 4,5 мільйонів клієнтів по всьому світу. Про це інформує УНН з посиланням на BBC.

Деталі

Про злам компанії вперше повідомили в лютому. Деталі, включаючи паспортні дані та інформацію про квитки, а також дані кредитних карток, були скомпрометовані.

Але Air India повідомила, що дані безпеки для кредитних карт - номери CVV або CVC - не зберігалися на цільовому сервері.

Хто стояв за атакою досі не зрозуміло.

Авіакомпанія, що входить в мережу Star Alliance, заявила, що порушення стосується всієї інформації, зареєстрованої в період з 26 серпня 2011 року по 20 лютого 2021 року.

Компанія попросила усіх своїх клієнтів змінити паролі до своїх облікових записів на своєму веб-сайті.

Air India повідомила, що ніяких подальших несанкціонованих дій виявлено не було.

Доповнення

У минулому році British Airways була оштрафована на 26 мільйонів доларів за витік даних, який торкнувся особистих даних і даних кредитних карт більш 400 тис. клієнтів в 2018 році.

Також в минулому році EasyJet визнала, що адреси електронних пошт і дані про поїздки приблизно дев'яти мільйонів клієнтів були вкрадені в результаті кібератаки». ***(Кібератака Air India: зламані дані мільйонів клієнтів // Голос України (http://www.golos.com.ua/news/136217). 22.05.2021).***

***

«На этой неделе министерство иностранных дел Японии и министерство земли, инфраструктуры, транспорта и туризма подтвердили влияние утечки данных у поставщика услуг Fujitsu Limited.

Ранее на этой неделе японский многонациональный поставщик ИТ-услуг и продуктов подтвердил, что подвергся кибератаке, которая привела к несанкционированному доступу к ProjectWEB, инструменту, который позволяет организациям обмениваться данными в своей среде и за ее пределами.

Компания заявила, что остановила службу, чтобы предотвратить дальнейший несанкционированный доступ, но подтвердила, что «некоторая информация,

доверенная нам нашими клиентами, была украдена», не предоставив дополнительной информации по этому поводу.

«Масштабы и причины этого инцидента в настоящее время расследуются, и работа ProjectWEB приостановлена для предотвращения дальнейшего несанкционированного доступа», - сказали в Fujitsu.

В среду министерство иностранных дел Японии объявило, что на него повлиял инцидент, заявив, что учебные материалы были украдены, а также могла быть затронута некоторая личная информация.

Министерство отмечает, что пострадавшие были проинформированы об утечке данных и что информация об исследовании не влияет на его системы или операции.

Также в среду министерство земли, инфраструктуры, транспорта и туризма заявило, что в результате инцидента, вероятно, были скомпрометированы около 76 000 адресов электронной почты лиц как внутри министерства, так и за его пределами.

«Несанкционированный доступ к системе министерства не подтвержден», - заявили в министерстве, добавив, что не было никаких перебоев в результате утечки данных. Министерство также сообщило о планах связаться с людьми, адреса электронной почты которых были скомпрометированы». ***(Ionut Arghire. Japanese Ministries Confirm Impact from Fujitsu Data Breach // Wired Business Media (https://www.securityweek.com/japanese-ministries-confirm-impact-fujitsu-data-breach). 27.05.2021).***

***

«Всякий раз, когда вы покупаете что-то на Amazon, данные ваших клиентов автоматически обновляются и хранятся на тысячах виртуальных машин в облаке. Для таких компаний, как Amazon, крайне важно обеспечить безопасность данных миллионов клиентов. Это верно как для больших, так и для малых организаций. Но до сих пор не было возможности гарантировать, что программная система защищена от ошибок, хакеров и уязвимостей.

Исследователи Columbia Engineering могли решить эту проблему безопасности. Они разработали SeKVM, первую систему, которая гарантирует - с помощью математического доказательства - безопасность виртуальных машин в облаке. В новом документе, который будет представлен 26 мая 2021 года на 42-м симпозиуме IEEE по безопасности и конфиденциальности, исследователи надеются заложить основу для будущих инноваций в проверке системного программного обеспечения, которые приведут к новому поколению киберустойчивого системного программного обеспечения.

SeKVM - первая официально проверенная система для облачных вычислений. Формальная проверка является критическим шагом, так как это процесс доказательства того, что программное обеспечение является математически правильным, что код программы работает должным образом и нет никаких скрытых ошибок безопасности, о которых следует беспокоиться.

«Это первый случай, когда реальная многопроцессорная программная система была показана математически правильной и безопасной», - сказал Джейсон

Ние, профессор компьютерных наук и содиректор Лаборатории программных систем. «Это означает, что данные пользователей правильно управляются программным обеспечением, работающим в облаке, и защищены от ошибок безопасности и хакеров».

Создание правильного и безопасного системного программного обеспечения было одной из величайших задач вычислительной техники. | Ние работал над различными аспектами программных систем с тех пор, как присоединился к Columbia Engineering в 1999 году. Когда Ронгхуэй Гу, доцент кафедры компьютерных наук семьи Тан и эксперт по формальной проверке, присоединился к отделу компьютерных наук в 2018 году, он и Ние решили сотрудничать по изучению формальной проверки программных систем.

Их исследования вызвали большой интерес: оба исследователя выиграли премию Amazon Research Award, несколько грантов Национального научного фонда, а также многомиллионный контракт Агентства перспективных исследовательских проектов в области обороны (DARPA) на дальнейшую разработку проекта SeKVM. Кроме того, за эту работу Ние был удостоен стипендии Гуггенхайма.

В течение последних десяти лет формальной проверке уделялось много внимания, включая работу по проверке многопроцессорных операционных систем. «Но все эти исследования проводились на маленьких игрушечных системах, которые никто не использует в реальной жизни», - сказал Гу. «Проверка многопроцессорной системы массового потребления, широко используемой системы, такой как Linux, считалась более или менее невозможной».

Экспоненциальный рост облачных вычислений позволил компаниям и пользователям перемещать свои данные и вычисления за пределы площадки в виртуальные машины, работающие на узлах в облаке. Поставщики облачных вычислений, такие как Amazon, развертывают гипервизоры для поддержки этих виртуальных машин.

Гипервизор - это ключевая часть программного обеспечения, которая делает возможными облачные вычисления. Безопасность данных виртуальной машины зависит от правильности и надежности гипервизора. Несмотря на свою важность, гипервизоры сложны - они могут включать в себя всю операционную систему Linux. Всего лишь одно слабое звено в коде, которое практически невозможно обнаружить с помощью традиционного тестирования, может сделать систему уязвимой для хакеров. Даже если гипервизор написан правильно на 99%, хакер все равно может проникнуть в эту конкретную настройку на 1% и получить контроль над системой.

Работа Ние и Гу - первая проверка серийной системы, в частности широко используемого гипервизора KVM, который используется для запуска виртуальных машин такими облачными провайдерами, как Amazon. Они доказали, что SeKVM, представляющий собой KVM с небольшими изменениями, безопасен и гарантирует изоляцию виртуальных компьютеров друг от друга.

«Мы показали, что наша система может защищать и защищать частные данные и вычисления, загруженные в облако, с математическими гарантиями», -

сказал Сюпэн Ли, аспирант Гу и соавтор статьи. «Это никогда не было сделано раньше».

SeKVM был проверен с помощью MicroV, нового фреймворка для проверки свойств безопасности больших систем. Он основан на гипотезе о том, что небольшие изменения в системе могут значительно упростить проверку, новый метод, который исследователи называют микроверификацией. Этот новый метод наслоения модернизирует существующую систему и выделяет компоненты, обеспечивающие безопасность, в небольшое ядро, которое проверяется и гарантирует безопасность всей системы.

Изменения, необходимые для модернизации большой системы, довольно скромны - исследователи продемонстрировали, что если небольшое ядро более крупной системы не повреждено, то система безопасна, и утечка личных данных не произойдет. Так они смогли проверить большую систему, такую как KVM, что раньше считалось невозможным.

«Подумайте о доме - трещина в гипсокартоне не означает, что целостность дома находится под угрозой», - пояснил Ние. «Он по-прежнему структурно прочен, а ключевая структурная система в хорошем состоянии».

Ши-Вей Ли, аспирант Ние и соавтор исследования, добавил: «SeKVM будет служить защитой в различных областях, от банковских систем и устройств Интернета вещей до автономных транспортных средств и криптовалют».

Как первый проверенный товарный гипервизор, SeKVM может изменить способ проектирования, разработки, развертывания и доверия к облачным сервисам. В мире, где кибербезопасность вызывает растущую озабоченность, эта отказоустойчивость очень востребована. Крупные облачные компании уже изучают возможности использования SeKVM для удовлетворения этого спроса». ***(Columbia Engineering Team Builds First Hacker-resistant Cloud Software System // Newswise, Inc (https://www.newswise.com/articles/columbia-engineering-team-builds-first-hacker-resistant-cloud-software-system). 24.05.2021).***

***

Кібербезпека Інтернету речей

«Многие устройства умного дома и Интернета вещей (IoT) редко обновляются, а средства обеспечения безопасности Wi-Fi остаются для них последней линией защиты от атак. Которую, к сожалению, теперь можно обойти.

Исследователь безопасности Мэти Ванхоф (Mathy Vanhoef) написал об этом в своем блоге, где представил под коллективным именем FragAttacks десяток уязвимостей устройств, использующих Wi-Fi.

«Эксперименты показывают, что каждый продукт Wi-Fi имеет как минимум одну, а большинство продуктов — несколько из этих уязвимостей, — сказал он. — Противник, находящийся в пределах радиуса действия жертвы, может

использовать эти уязвимости для кражи пользовательской информации или атак на устройства».

Ванхоф практически продемонстрировал эксплуатацию FragAttacks, пробив брешь в брандмауэре и захватив уязвимый компьютер с Windows 7.

CVE, зарегистрированные в связи FragAttacks, получили средний рейтинг серьезности с оценками CVSS от 4,8 до 6,5. Многие из них сложны в использовании и требуют взаимодействия с пользователем, но другие достаточно тривиальны.

Детали FragAttacks не разглашаются согласно правилам девятимесячного эмбарго, чтобы дать поставщикам время для создания исправлений.

Microsoft разослала свои патчи 9 марта, а соответствующие исправление для ядра Linux проходит через систему подготовки к публикации. Некоторые сетевые поставщики, такие как Cisco и Juniper, тоже начали продвигать исправления в некоторые из своих затронутых продуктов, другие, как Sierra планируют обновить ряд своих продуктов в течение следующего года.

По информации Wi-Fi Alliance., нет никаких доказательств злонамеренного использования этих уязвимостей, и все проблемы устраняются регулярными программными обновлениями устройств, которые «позволяют обнаруживать подозрительные передачи или улучшать соблюдение рекомендуемых практик реализации безопасности».

«К сожалению, не все продукты (в частности интеллектуальные или IoT-устройства) регулярно получают апдейты, в этом случае сложно (если не невозможно) должным образом защитить их, — пишет Ванхоф. — В зависимости от вашей конфигурации Wi-Fi, вы можете смягчить атаки (но не полностью предотвратить их), отключив фрагментацию, парные смены ключей и динамическую фрагментацию в устройствах Wi-Fi 6 (802.11ax)». Предотвратить кражу данных с непропатченных устройств также можно, если использовать HTTPS-соединения». ***(FragAttacks — тотальная угроза для всего, подключенного к Wi-Fi // Компьютерное Обозрение (https://ko.com.ua/fragattacks_totalnaya_ugroza_dlya_vsego_podklyuchennogo_k_wi-fi_137335). 13.05.2021).***

***

«В июле 2020 года правительство Великобритании объявило, что планирует изменить закон, чтобы сделать умные продукты более безопасными, и опубликовало призыв высказаться по поводу его предложений. Получив 110 ответов от организаций и частных лиц, правительство опубликовало свой ответ.

Правительство заявляет, что когда позволит парламентское время, оно примет законодательный акт о создании новой надежной схемы регулирования для защиты потребителей от небезопасных подключенных продуктов. Регламент будет применяться ко всем подключенным к потребителю продуктам (например, интеллектуальным колонкам, смарт-телевизорам, подключенным дверным звонкам и смартфонам). Различные устройства, в том числе настольные компьютеры и ноутбуки, будут освобождены из-за конкретных обстоятельств их конструкции и

защиты. Требования безопасности будут соответствовать международным стандартам и, по мнению правительства, знакомы всем производителям и другим заинтересованным сторонам в отрасли. Правоприменительный орган будет наделен полномочиями расследовать утверждения о несоблюдении и принимать меры для обеспечения соблюдения.

Ключевые политические позиции

Предполагаемый подход правительства к регулированию подкреплен 12 ключевыми политическими позициями:

определение продуктов в области применения - предусмотренное законодательство будет применяться ко всем устройствам, подключаемым к сети, и связанным с ними службам, которые предоставляются в первую очередь потребителям, за исключением продуктов, которые обозначены как выходящие за рамки;

освобожденные классы продуктов - определенные классы продуктов, которые в противном случае подпадали бы под действие этого законодательства, но для которых его применение было бы неуместным, будут исключены из законодательной базы;

адаптируемый объем - там, где изменения в более широких нормативных, технологических или угрожающих ландшафтах делают это целесообразным, предполагаемое законодательство позволит министрам, при условии согласия парламента, скорректировать объем связанных с потребителем продуктов, охватываемых этим правилом, путем обновления списка исключенных классов продуктов;

функциональная совместимость - правительство гарантирует, что предполагаемое законодательство совместимо с другими существующими или планируемыми государственными вмешательствами, которые охватывают смежные или перекрывающиеся классы продуктов (например, обязательства Министерства бизнеса, энергетики и промышленной стратегии по регулированию интеллектуальных устройств);

обязательства экономических субъектов - законодательство налагает соразмерные обязательства на соответствующих экономических субъектов, участвующих в передаче товаров, подпадающих под действие охвата, потребителям, чтобы гарантировать, что небезопасные товары не будут доступны потребителям Великобритании;

требования безопасности - законодательство будет препятствовать тому, чтобы соответствующие экономические субъекты могли предлагать подключенные к потребителю продукты на рынке Великобритании, если они не соответствуют определенным требованиям безопасности или установленным стандартам;

адаптируемые требования безопасности - если изменения в более широких нормативных, технологических или угрожающих ландшафтах делают это целесообразным, предполагаемое законодательство позволит министрам обновлять требования безопасности и установленные стандарты, которым соответствующие экономические субъекты должны обеспечивать соответствие продуктов, представленных на рынке Великобритании;

гарантия продукта - там, где изменения в более широком технологическом ландшафте или ландшафте угроз делают это целесообразным, предполагаемое законодательство позволит министрам требовать гарантии продукта для определенных категорий продуктов, подключенных к потребителю;

правоохранительный орган - правоприменительный орган будет расследовать и принимать меры в отношении несоблюдения и оказывать поддержку соответствующим экономическим субъектам, чтобы они могли выполнять свои обязательства;

роль и обязанности правоприменения - чтобы обеспечить соразмерное правоприменение в различных контекстах, законодательство наделяет правоприменительный орган необходимыми полномочиями, а также способностью принимать соответствующие корректирующие меры и наказания и потенциально возбуждать уголовное дело в наиболее серьезных обстоятельствах;

апелляции - соответствующие субъекты экономической деятельности будут иметь право обжаловать любые санкции или корректирующие меры, примененные против них, в соответствии с процессами, используемыми в существующем законодательстве о безопасности продукции; а также

соразмерные переходные положения - после королевского согласия правительство предоставит соответствующим экономическим субъектам соответствующий льготный период для корректировки их деловой практики до того, как предполагаемый закон полностью вступит в силу.

Примеры новых требований

Ниже приведены примеры новых требований, которым должны соответствовать интеллектуальные устройства:

В точке продажи покупатели должны быть проинформированы о продолжительности времени, в течение которого интеллектуальное устройство будет получать обновления программного обеспечения безопасности.

Производители не должны использовать легко угадываемые универсальные пароли по умолчанию (например, «пароль» или «администратор»), которые часто предварительно устанавливаются в заводских настройках устройства.

Производители должны предоставить общедоступные контактные данные, чтобы всем было проще сообщить об уязвимости». ***(Alan Owens. Government publishes response to call for views on consumer smart product cybersecurity regulation proposals // Law Business Research (https://www.internationallawoffice.com/Newsletters/Tech-Data-Telecoms-Media/United-Kingdom/Wiggin-LLP/Government-publishes-response-to-call-for-views-on-consumer-smart-product-cybersecurity-regulation-proposals).07.05.2021).***

***

«Технологии, подключенные к Интернету, которые используются для питания умных городов, являются очень заманчивой целью для кибератак, и местные власти должны осознавать риски, с которыми они - и их граждане - могут столкнуться, если злоумышленники смогут вмешаться в инфраструктуру или услуги.

Городская инфраструктура, включая службы экстренной помощи, транспорт, управление светофорами, видеонаблюдение и многое другое, все чаще использует датчики и подключается к Интернету вещей, чтобы собирать данные и предоставлять более качественные и эффективные услуги.

Однако Национальный центр кибербезопасности Великобритании (NCSC) - кибер-подразделение разведывательного агентства GCHQ - предупредил, что киберфизические системы в умных городах могут быть скомпрометированы кибер-злоумышленниками, если они не будут должным образом защищены.

Огромный объем конфиденциальных данных, собираемых и хранимых умными городами, подключенными к Интернету вещей, плюс способность нарушать работу «делают эти системы привлекательной мишенью для ряда злоумышленников», - предупреждает новое руководство NCSC по обеспечению безопасности умных городов.

«Эти подключенные физические среды только появляются в Великобритании, поэтому сейчас самое время убедиться, что мы проектируем и строим их должным образом. Поскольку эти« связанные места »становятся все более объединенными, повсеместность предоставляемых ими услуг, вероятно, будет сделать их мишенью для злоумышленников», - сказал Ян Леви, технический директор NCSC.

Чтобы помочь местным властям и защитить инфраструктуру, организации и людей от угрозы кибератак, которые могут быть нацелены на умные города, NCSC опубликовал ряд принципов, которых следует придерживаться, чтобы обеспечить этим сетям максимально возможный уровень кибербезопасности.

Для начала местным властям следует понимать роль своего связанного места. Определив, кто отвечает за подключенное место, как будет выглядеть сеть IoT, какие данные будут собираться, обрабатываться, храниться и передаваться, а также какие операционные технологии уже используются, власти могут начать подключать умные города с учетом безопасности от начало.

Властям также рекомендуется понимать потенциальные риски для подключенного места. Эти риски варьируются от точного знания того, какие устройства и программное обеспечение используются для подключения места - обеспечение того, что оно от надежного, уважаемого поставщика - до обеспечения достаточной защиты этих устройств, когда дело доходит до аутентификации.

Например, город не должен развертывать устройства IoT в сети, если у этих продуктов все еще есть имя пользователя и пароль по умолчанию, так как это сделало бы их легкой мишенью для кибер-злоумышленников, особенно если данные «собираются или обрабатываются бессистемно. - сказал Леви.

Предполагается, что умные города помогут улучшить услуги для людей, но безответственное отношение к хранению данных может привести к нарушениям конфиденциальности, а плохо реализованная система безопасности может позволить кибератакам вмешиваться в службы и системы, которые нужны людям.

«Мы надеемся, что эти принципы помогут разработчикам, владельцам и менеджерам подключенных систем размещения сделать осознанный выбор кибербезопасности», - сказал Леви.

Хотя руководство NCSC не относится к какому-либо конкретному потенциальному субъекту киберугроз, директор GCHQ недавно предупредил, что появление Китая в качестве производителя технологий означает, что Великобритания и другие страны могут столкнуться с проблемами, если организации или местные власти станут зависимыми. на устройствах и программном обеспечении отечественного производства.

«Государства, не разделяющие наших ценностей, выстраивают свои собственные нелиберальные ценности в стандарты и технологии, на которые мы можем полагаться. Если это произойдет, и окажется, что это будет небезопасно, сломано или недемократично, каждый столкнется с очень трудным будущее», - сказал Джереми Флеминг». ***(Danny Palmer. Smart cities are a tempting target for cyberattacks, so it's time to secure them now // ZDNet (https://www.zdnet.com/article/smart-cities-are-a-tempting-target-for-cyberattacks-so-its-time-to-secure-them-now/). 07.05.2021).***

***

Кіберзлочинність та кібертерроризм

«Компания Ardagh Group, занимающаяся производством металлической и стеклянной упаковки, объявила, что столкнулась с инцидентом в области кибербезопасности, который привел к тому, что группа активно закрыла некоторые ИТ-системы и приложения.

Группа выпустила заявление, в котором говорится, что ее ИТ-команда при поддержке внешних специалистов по кибербезопасности «работает над решением этой проблемы, продолжая при этом безопасную эксплуатацию объектов группы».

Судебно-медицинское расследование

Ardagh Group проведет судебно-медицинское расследование инцидента с помощью ряда специалистов.

Несмотря на то, что производственные мощности группы продолжают работать, у упаковочного гиганта возникают задержки в цепочке поставок.

Ardagh Group также объявила, что кибератака, вероятно, «приведет к некоторой отсрочке или потере доходов, а также к дополнительным расходам».

В заявлении добавлено, что группа «имеет соответствующее страхование в отношении широкого спектра рисков».

Усиленная безопасность

После инцидента Ardagh Group внедрила новые инструменты защиты в свою сеть, чтобы обеспечить повышенный уровень безопасности.

Группа пересмотрит свою технологическую дорожную карту и ускорит ряд запланированных инвестиций для дальнейшего повышения эффективности возможностей группы в области ИТ-безопасности.

Тем не менее, группа не ожидает, что инцидент повлияет на полный прогноз на 2021 год для группы, и что инвестиционные проекты по развитию бизнеса, реализуемые Ardagh Group, не пострадали от этого инцидента и продолжаются.

В настоящее время группа работает над постепенным, поэтапным и безопасным возвращением ключевых систем в режим онлайн.

Это идет по плану и, как ожидается, будет в значительной степени достигнуто к концу этого месяца». ***(Ardagh Group Confirms 'Cybersecurity Incident' // Checkout (https://www.checkout.ie/packaging-design/ardagh-group-confirms-cybersecurity-133172). 18.05.2021).***

***

«Производитель устройств сетевого хранения (NAS) QNAP Systems заявляет, что расследует сообщения о злонамеренных атаках, нацеленных на устройства NAS.

Известная во всем мире своими решениями NAS и профессиональных сетевых видеорегистраторов (NVR), тайваньская компания в пятницу выпустила два предупреждения, чтобы предупредить о новой волне атак, нацеленных на своих пользователей, и призвав их обеспечить, чтобы их устройства NAS не подвергались воздействию Интернет.

В первом сообщении компания сообщает, что расследует кампанию атаки, в которой злоумышленники нацелены на уязвимость в Roon Server. Компания заявляет, что все устройства QNAP NAS, на которых работает Roon Server 2021-02-01 и ранее, могут быть уязвимы для атак.

Предоставляемый Roon Labs сервер Roon Server предоставляет пользователям QNAP NAS полный спектр возможностей, которые они ожидают от музыкального сервера, включая простой способ навигации по музыке и доступ к биографии артистов, датам концертов, текстам песен и многому другому.

«Мы уже уведомили Roon Labs о проблеме и тщательно расследуем дело. Мы выпустим обновления безопасности и предоставим дополнительную информацию в кратчайшие сроки», - сообщает QNAP.

Тем временем пользователи должны убедиться, что их NAS не подключен к Интернету, а также отключить Roon Server, чтобы убедиться, что они не подвержены потенциальным атакам.

Во-вторых, QNAP заявляет, что расследует сообщения о том, что устройства NAS по-прежнему становятся жертвами вымогателя eCh0raix.

«Устройства, использующие слабые пароли, могут быть уязвимы для атак. Мы настоятельно рекомендуем пользователям действовать немедленно, чтобы защитить свои данные», - говорится в сообщении компании.

Чтобы снизить риски, пользователям рекомендуется использовать надежные пароли для своих учетных записей администраторов, включить защиту IP-доступа, чтобы обеспечить защиту учетных записей от атак методом грубой силы, и избегать использования номеров портов по умолчанию 443 и 8080.

Это не первый случай, когда устройства QNAP NAS становятся жертвами вымогателя eCh0raix. В апреле компания предупредила о нападениях с участием семейств программ-вымогателей Qlocker и eCh0raix, призвав пользователей немедленно выполнить операции обнаружения и очистки». ***(Ionut Arghire. QNAP Investigating New Attacks Targeting NAS Devices // Wired Business Media***

(https://www.securityweek.com/qnap-investigating-new-attacks-targeting-nas-devices). 17.05.2021).

***

«Федеральное бюро расследований сообщает, что его Центр жалоб на преступления в Интернете (IC3) получил более миллиона жалоб на киберпреступления за последние 14 месяцев.

Основанная в 2000 году как Центр жалоб на мошенничество в Интернете и переименованная в 2002 году, IC3 на сегодняшний день получила в общей сложности 6 миллионов жалоб. Первый миллион жалоб был зарегистрирован почти через семь лет. В марте прошлого года, всего за несколько недель до своего 20-летия, на Центр поступило 5 миллионов жалоб.

В дополнение к сбору и представлению этих данных, IC3 также выдает оповещения общественности о новых мошенничествах или всплеске конкретных преступлений. Он также обеспечивает доступ к собранным данным федеральным и другим государственным учреждениям.

За последние несколько лет в Центре наблюдается устойчивый рост числа зарегистрированных киберпреступлений. В период с 2019 по 2020 год количество жалоб выросло почти на 70%, но рост заявленных убытков был не таким резким.

В течение 2020 года IC3 получил около 800000 жалоб на киберпреступления, в результате чего убытки составили около 4,2 миллиарда долларов. В 2019 году в Центр поступило около 467000 жалоб, заявленные убытки составили 3,5 миллиарда долларов.

Фишинг-мошенничество, мошенничество с неплатежами / недоставкой и вымогательство были главными зарегистрированными киберпреступлениями в 2020 году, при этом наибольшие убытки были нанесены мошенничеством с взломом деловой электронной почты (BEC), схемами романтики и доверия, а также инвестиционным мошенничеством.

Глобальная пандемия привела к появлению мошенничества, использующего темы COVID-19, но также привела к общему увеличению количества жалоб, связанных с киберпреступлениями - в основном из-за увеличения активности и торговли в Интернете, - и IC3 считает, что 2021 год может быть успешным. рекордный год.

Ссылаясь на массовый рост зарегистрированных жалоб, руководитель IC3 Донна Грегори отметила, что большее количество отчетов помогает ФБР более эффективно бороться с киберпреступлениями.

«С одной стороны, в этой цифре есть положительные новости. Люди знают, как нас найти и как сообщить о происшествии. Но с другой стороны, эти цифры указывают на то, что больше людей страдают от онлайн-преступлений и мошенничества», - говорит Грегори». ***(Ionut Arghire. BI: IC3 Received 6 Million Cybercrime Complaints Since Inception // Wired Business Media (https://www.securityweek.com/fbi-ic3-received-6-million-cybercrime-complaints-inception). 18.05.2021).***

***

«Во вторник судебная система Аляски заявила, что восстановила возможности электронной почты почти через две недели после атаки кибербезопасности.

Судебная система в своем заявлении заявила, что не знает, кто стоял за атакой, почему судебная система стала мишенью и сколько времени пройдет, прежде чем службы полностью вернутся в онлайн. Он заявляет, что не считает, что личные или конфиденциальные данные были получены из компьютерных систем судов, и заявляет, что не было доступа к информации о кредитных картах.

Джоэл Болджер, председатель Верховного суда Аляски, на прошлой неделе сообщил Associated Press, что судебная система не получала требований о выкупе или каких-либо прямых сообщений от лиц, причастных к атаке на кибербезопасность.

В заявлении говорится, что кто-то вне сети 29 апреля разместил в системе вредоносное ПО, что вынудило суды отключить онлайн-сервисы 1 мая. Судебная система в четверг начала то, что она называет «этапом исправления процесса восстановления», который включает в себя проверку отсутствия вредоносных программ и обеспечение «достаточных мер безопасности в будущем», - говорится в сообщении.

В заявлении говорится, что во вторник была восстановлена служба электронной почты, которая позволит отправлять по электронной почте и рассылать уведомления или заказы электронными средствами». ***(Alaska Courts Restore Email, Lack Answers on Cyber Attack // Wired Business Media (https://www.securityweek.com/alaska-courts-restore-email-lack-answers-cyber-attack). 12.05.2021).***

***

«Официальные лица заявили, что сайт министерства здравоохранения Аляски стал целью атаки вредоносного ПО.

Подобная атака ранее была направлена на судебную систему штата.

В заявлении министерства здравоохранения во вторник вечером говорится, что его веб-сайт был отключен в понедельник, пока идет расследование. В заявлении не говорится, когда была обнаружена кибератака, а Клинтон Беннетт, официальный представитель департамента, в электронном письме в среду заявила, что департамент не может раскрыть эту информацию «по соображениям безопасности, и поэтому мы не ставим под угрозу расследование».

Точно так же он ответил на вопрос о том, требовали ли участники выкупа.

В ведомстве заявили, что следователи пытались определить, была ли скомпрометирована какая-либо личная или конфиденциальная информация.

По сообщению департамента, онлайн-расписание приема вакцины против COVID-19 и информационные панели размещаются во внешних источниках, и к ним можно получить доступ через covid19.alaska.gov.

«В настоящее время нет подробностей о том, кто инициировал атаку, почему они нацелены на DHSS, связана ли эта атака с какими-либо другими недавними атаками или как долго веб-сайт может быть недоступен», - говорится в сообщении Министерства здравоохранения и социальных служб. свое заявление.

В этом месяце председатель Верховного суда Аляски заявил, что атака кибербезопасности, в результате которой судебная система отключила свои онлайн-сервисы, была впервые обнаружена 29 апреля и что требования о выкупе не поступало. Судебная система возвращается в онлайн, объявляя на этой неделе, что общественность снова может получить доступ к онлайн-системе судебных дел и записей, а также оплачивать штрафы и сборы онлайн.

Во вторник судебная система заявила, что возможность вносить залог онлайн еще не восстановлена». ***(Alaska Health Department Website Targeted in Malware Attack // Wired Business Media (https://www.securityweek.com/alaska-health-department-website-targeted-malware-attack). 20.05.2021).***

***

«Огромный радиус взрыва от атаки на цепочку поставок Codecov остается окутанным тайной, поскольку службы безопасности продолжают оценивать последствия взлома, но горстка жертв начинает публично признавать возможное раскрытие конфиденциальных секретов разработчиков.

Компрометация скрытой цепочки поставок программного обеспечения Codecov Bash Uploader оставалась незамеченной с января этого года и раскрыла конфиденциальные секреты, такие как токены, ключи и учетные данные, от организаций по всему миру.

Первой компанией, публично признавшей свою уязвимость, была HashiCorp, компания, которая продает средства разработки с открытым исходным кодом и средства безопасности для инфраструктуры облачных вычислений. HashiCorp заявила, что расследование после взлома обнаружило, что часть ее конвейеров CI использовала затронутый компонент Codecov.

В частности, был раскрыт закрытый ключ GPG, используемый для подписи хэшей, используемых для проверки загрузки продукта HashiCorp. «Хотя расследование не выявило доказательств несанкционированного использования открытого ключа GPG, он был изменен, чтобы поддерживать надежный механизм подписи», - говорится в сообщении компании в опубликованном уведомлении о безопасности.

После заявления HashiCorp компания Twilio из Сан-Франциско выпустила уведомление, подтверждающее, что она использует скомпрометированный компонент Bash Uploader в небольшом количестве проектов и конвейеров CI.

«Наше последующее расследование последствий этого события показало, что небольшое количество адресов электронной почты, вероятно, было украдено неизвестным злоумышленником в результате этого разоблачения. Мы уведомили этих пострадавших лиц в частном порядке и устранили дополнительную потенциальную уязвимость, тщательно проверив и изменив любые потенциально уязвимые учетные данные», - добавил Твилио.

«Как только нам стало известно о событии, мы определили все потенциально раскрытые учетные данные или секреты и поменяли их. Это удалило любую способность плохого актера получить доступ к нашему окружению. Кроме того, мы

исследовали объем этих учетных данных и в меру своих возможностей подтвердили, что ими не было злоупотреблений», - добавили в компании.

Codecov удалила со своего сайта веб-страницу, на которой утверждалось, что более 29 000 компаний полагаются на ее продукты для защиты кода. На странице клиента перечислены известные компании, такие как GoDaddy, Proctor & Gamble, Lululemon, RBC, Mozilla и Elastic.

В Твиттере и на некоторых форумах общественной безопасности разработчики сообщества Mozilla обсуждали ротацию секретов разработчиков, подтверждая, что степень нарушения еще не была должным образом оценена.

Взлом Codecov был обнаружен клиентом Codecov утром 1 апреля 2021 года, когда компания заявила, что узнала, что кто-то получил несанкционированный доступ к скрипту Bash Uploader, и изменил его без разрешения.

«Актер получил доступ из-за ошибки в процессе создания образа Docker Codecov, которая позволила актеру извлечь учетные данные, необходимые для изменения нашего сценария Bash Uploader», - сказал Кодеков, предупредив, что атаки начались в конце января и оставались незамеченными, пока клиент не заметил. несоответствие между shasum на Github и shasum, вычисленным из загруженного Bash Uploader.

Codecov сказал, что нарушение позволило злоумышленникам экспортировать информацию, хранящуюся в средах непрерывной интеграции (CI) ее пользователей. Затем эта информация была отправлена на сторонний сервер за пределами инфраструктуры Codecov». ***(Ryan Naraine. Twilio, HashiCorp Among Codecov Supply Chain Hack Victims // Wired Business Media (https://www.securityweek.com/twilio-hashicorp-among-codecov-supply-chain-hack-victims). 10.05.2021).***

***

«В период между 2019 и 2020 годами количество мобильного фишинга среди финансовых служб и страховых организаций увеличилось вдвое. Кибератаки намеренно атакуют телефоны, планшеты и Chromebook, чтобы повысить свои шансы найти уязвимую точку входа.

Согласно новому отчету исследовательской группы Lookout, опубликованному 6 мая, одна успешная фишинговая или мобильная атака с использованием программ-вымогателей может дать злоумышленникам доступ к собственным исследованиям рынка, финансовым данным клиентов, инвестиционным стратегиям и денежным средствам или другим ликвидным активам.

Отчет об угрозах финансовых услуг показал, что почти половина всех попыток фишинга пытались украсть корпоративные учетные данные. Другие результаты заключаются в том, что около 20 процентов клиентов мобильного банкинга имели троянское приложение на своих устройствах при попытке войти в свою личную учетную запись мобильного банкинга.

Несмотря на 50-процентный рост внедрения управления мобильными устройствами (MDM) с 2019 по 2020 год, среднеквартальная подверженность

фишингу выросла на 125 процентов. Риск вредоносного ПО и приложений увеличился более чем на 400 процентов.

Спустя семь месяцев после выпуска iOS 14 и Android 11 21 процент устройств iOS все еще был на iOS 13 или более ранней версии, а 32 процента устройств Android все еще работали на Android 9 или более ранней версии. Согласно отчету, такая задержка с обновлением мобильных устройств пользователями создает для злоумышленника возможность получить доступ к инфраструктуре организации и украсть данные.

«Вредоносные приложения, которые доставляются с помощью фишинговых кампаний с использованием социальной инженерии, всегда будут проблемой, с которой придется иметь дело службам безопасности. Злоумышленники знают, что могут атаковать людей через личные каналы, такие как SMS, сторонние платформы обмена сообщениями, социальные сети и даже приложения для знакомств. для установления связи и укрепления доверия ", - сказал TechNewsWorld Хэнк Шлесс, старший менеджер по решениям безопасности в Lookout.

Более высокие риски безопасности, больше мобильных пользователей

Эта цифровая среда подвергает данные как предприятий, так и их клиентов новым рискам, поскольку теперь данные перемещаются туда, где они необходимы. Отрасль финансовых услуг находится в процессе ускорения цифровой трансформации.

Еще до того, как пандемия вынудила организации переходить на облачные сервисы и мобильные устройства, в 2019 году в финансовой отрасли наблюдалось увеличение внедрения мобильных приложений на 71 процент. Планшеты, Chromebook и смартфоны теперь являются ключевым компонентом работы финансовых учреждений.

К постоянным мобильным пользователям относятся сотрудники, выполняющие работу дома, или клиенты, управляющие своими финансами с помощью приложения. Учитывая стремительный рост популярности Chromebook как одного из самых популярных мобильных устройств для образовательных учреждений и предприятий за последние 18 месяцев, это значительная канарейка в угольной шахте.

Хотя многие организации обратились к MDM как к способу контролировать ситуацию, этого недостаточно. Lookout подчеркивает в своем отчете, что управление устройством не защищает его от сложных мобильных угроз.

Когда сотрудники были вынуждены работать удаленно почти всю ночь, им приходилось использовать свои смартфоны и планшеты, чтобы оставаться продуктивными. По словам Шлесса, злоумышленники осознали этот сдвиг и начали более активно атаковать людей с помощью вредоносных программ для мобильных устройств и фишинговых атак.

«Это мгновенное изменение также вынудило группы безопасности и ИТ-специалистов резко изменить свои стратегии и политики. Чтобы сохранить некоторое подобие контроля над мобильным доступом к корпоративной инфраструктуре, группы безопасности расширили возможности своих корпоративных сетей VPN и развернули MDM для больше мобильных пользователей», - добавил он.

Несколько бесполезные усилия

Несмотря на обращение к управлению мобильными устройствами, все же произошел значительный скачок в уязвимостях мобильных угроз, отметил Шлесс.

«Это доказывает, что MDM следует использовать только для управления устройствами, а не для их защиты. Эти решения не могут защитить устройства от киберугроз, таких как мобильный фишинг», - сказал он.

Финансовые организации должны использовать современные технологии и стратегии безопасности, чтобы оставаться безопасными, конкурентоспособными и актуальными на устройствах, которые сотрудники и клиенты используют чаще всего, - убеждены исследователи Lookout.

Lookout обнаружил, что рост среднего ежеквартального уровня подверженности мобильному фишингу на 125% был значительно выше, чем в любой другой отрасли. Первая проблема заключается в том, что MDM не могут защитить мобильные устройства. По словам Шлесса, VPN также не проверяют наличие каких-либо угроз на устройстве, прежде чем разрешить ему доступ к корпоративным ресурсам и инфраструктуре.

«Злоумышленники очень быстро сообразили. Они создали вредоносные программы и фишинговые кампании, которые могли легко обойти основные политики управления, предлагаемые решениями MDM. Вот почему мы продолжаем видеть рост уязвимостей мобильных угроз, несмотря на то, что организации более активно используют MDM», - сказал он.

По его мнению, единственный способ защититься от этих атак - это реализовать по-настоящему интегрированное решение для обеспечения безопасности конечных точек в облаке. Это решение может проверить степень риска устройства и пользователя, чтобы гарантировать, что вредоносные программы или неавторизованные пользователи не получат доступ к инфраструктуре.

Бизнес должен действовать в целях безопасности

Исследователи предупреждают, что для предотвращения мошенничества и захвата аккаунтов финансовые организации и другие предприятия должны подумать о том, как обезопасить мобильные приложения для своих клиентов. При создании потребительских приложений безопасность должна быть интегрирована с нуля.

Благодаря интеграции сервисов в процесс разработки мобильных приложений, возможности мобильной безопасности изначально доставляются клиентам, не требуя от них установки какого-либо дополнительного программного обеспечения.

«При нацеливании на финансовые услуги киберпреступники имеют возможность преследовать как сотрудников, так и клиентов. Это означает, что службы безопасности должны охватывать невероятно широкий спектр угроз. По этой причине никогда не бывает слишком удивительно видеть, что финансовые услуги входят в число наиболее распространенных угроз. целевые отрасли», - сказал Шлесс из Lookout.

Почему фишинг ловит жертв

Фишинговые письма часто содержат личную информацию и могут выглядеть очень достоверно. Часто они выглядят как законная услуга от известного поставщика, - предложил Джозеф Карсон, главный специалист по безопасности и консультант по информационной безопасности ThycoticCentrify.

«Фишинговые электронные письма почти всегда представляют собой срочное сообщение от органа, требующее быстрых действий, таких как щелчок по ссылке или открытие прикрепленного файла, чтобы избежать дальнейших проблем, штрафов за просрочку платежа и т. Д. Эти электронные письма обычно содержат несколько гиперссылок - некоторые из них законно замаскировать одну вредоносную ссылку между ними», - сказал он TechNewsWorld.

Электронные письма с адресным фишингом нацелены на вас лично, притворяясь от кого-то, кого вы знаете и которому доверяете, например друга, коллеги или начальника. Эти электронные письма содержат гиперссылку или вложение, например PDF-файл, документ Word, электронную таблицу Excel или презентацию PowerPoint.

Наиболее частые целевые фишинговые атаки исходят от высшего руководства вашего работодателя или от кого-то из представителей власти, которые просят вас выполнить важное действие - либо открыть вложение, либо, в некоторых случаях, срочно перевести деньги на ссылку в электронном письме, Карсон объяснил.

Обнаружение попыток атаки

Ограничьте то, чем вы делитесь в социальных сетях, и включите настройки конфиденциальности и безопасности в своих учетных записях Facebook, Twitter или других социальных сетях, Карсон рекомендовал в качестве стандартов безопасности.

«Не принимайте просьбы о дружбе, если вы не знаете человека хорошо», - добавил он.

Как и в случае с известным спамом, помечайте отправителей подозрительных писем на фишинг как спам или нежелательную почту. Затем немедленно сообщите о них в отдел ИТ-безопасности, если они появятся прямо в вашем рабочем почтовом ящике.

Еще одна тактика безопасности - никогда не пересылать фишинговые письма. Кроме того, убедитесь, что вы предприняли основные шаги для защиты своих устройств и проверили свою систему и электронную почту на наличие вредоносных программ.

«Необычно высокий объем мобильных данных и использования Интернета может указывать на то, что устройство было взломано, и что данные извлекаются и крадутся. Всегда проверяйте ежемесячные тенденции использования Интернета, обычно доступные у вашего интернет-провайдера или домашнего маршрутизатора, как для загрузки, так и для выгрузки для отслеживания вашей ежемесячной активности в Интернете», - предложил он.

Обычно вы можете установить ограничения на использование, которые будут предупреждать вас о подозрительных уровнях. При срабатывании этих сигналов тревоги немедленно проверьте уровни использования». ***(Jack M. Germain. Mobile***

Devices Under Siege by Cyberattackers // ECT News Network, Inc. (https://www.technewsworld.com/story/87132.html). 18.05.2021).

***

«Австралийский бизнес в области цифровой недвижимости Domain Group подтвердил, что его платформа стала жертвой фишинг-атаки.

«Мы выявили мошенничество, которое использовало фишинговую атаку для получения доступа к административным системам Domain для взаимодействия с людьми, которые обращались с запросами об аренде недвижимости», - заявил генеральный директор компании Джейсон Пеллегрино в заявлении для ZDNet.

«Насколько мы понимаем, мошенники затем связались с некоторыми из этих людей по электронной почте, чтобы предложить им внести «депозит», чтобы обеспечить аренду собственности на веб-сайте, указанном мошенником».

Домен заявил, что, хотя атака является серьезным вопросом, на данный момент ее расследование показало, что лишь небольшое количество людей могло участвовать в мошенничестве.

«Очевидно, что люди становятся более осведомленными о том, как определять подозрительное поведение в Интернете и принимать меры защиты, чтобы не участвовать в такой деятельности», - добавил Пеллегрино.

«К сожалению, со времен Covid количество подобных мошенничеств стало расти. Нам очень досадно узнать, что после столь трудных для многих из нас последних двенадцати месяцев некоторые видят в этом возможность воспользоваться другими».

По словам генерального директора, после того, как компания Domain узнала о мошенничестве, она внедрила несколько дополнительных мер безопасности и еще больше повысила уровень мониторинга.

«Мы продолжаем внедрять дальнейшие способы выявления и предотвращения фишинга и привлекли внешних консультантов по безопасности, чтобы предоставить дополнительные знания в области управления и предотвращения онлайн-мошенничества», - сказал он.

Domain Group примерно на 65% принадлежит Nine Entertainment Co в результате слияния Fairfax и Nine. В начале этого года девять служб были нарушены в результате кибератаки, из-за которой они были отключены от эфира. Домен сказал, что последний инцидент не был связан с инцидентом, с которым столкнулась Девять.

Окружной совет здравоохранения Новой Зеландии Вайкато работает над тем, чтобы вернуть свои системы в оперативный режим после того, как во вторник в нем полностью отключились информационные службы. Stuff сообщает, что инцидент был вызван программой-вымогателем, а глава Waikato DHB заявил, что киберпреступникам «выкуп не будет выплачиваться».

В обновлении, опубликованном в среду днем, Waikato DHB сообщила, что добилась «хороших успехов» в восстановлении зараженных систем и в процессе исправления.

«В настоящее время мы работаем с другими правительственными ведомствами над расследованием причины, но работаем над теорией, согласно

которой первоначальное вторжение произошло через вложение электронной почты. Судебно-медицинское расследование продолжается», - говорится в сообщении.

Это означает, что на этой неделе пострадало обслуживание в больницах Вайкато, Темзы, Те Куити, Токороа и Таумаруноуи. В больнице Вайкато отложены некоторые плановые операции, а количество амбулаторных клиник сокращено.

Из 102 плановых операций, запланированных для стационарных пациентов в больнице Вайкато в среду, 73 все еще продолжаются, шесть плановых операций отменены во вторник, а 95 все еще выполнены.

Плановые операции в больнице Темзы были отложены, а вся амбулаторная деятельность в сельских больницах Waikato DHB была отложена». ***(Asha Barbaschow. Domain Group says phishing attack targeted site users // ZDNet (https://www.zdnet.com/article/domain-group-says-phishing-attack-targeted-site-users/). 20.05.2021).***

***

«2020 год был непохожим на другие. Первая настоящая глобальная пандемия в нашу современную эпоху потрясла мир, нарушив наш образ жизни и ведение бизнеса. Организации были вынуждены адаптироваться в удивительно короткие сроки, как и их сотрудники. Однажды мы ехали на работу в обычном режиме, а потом почти на ночь нам сказали, что мы не можем прийти в офис. Нам сказали, что мы не можем пойти поесть, нам даже сказали, что мы не можем достать туалетную бумагу.

Как бы трудно ни было справиться с первоначальным потрясением, настойчивость была совсем другим делом. В условиях продолжающейся экономической борьбы, политических потрясений и общего чувства неуверенности это было поистине трудное время для людей как в профессиональном, так и в личном плане.

А это благодатная почва для мошенников.

Видите ли, аферы получают свою силу от эмоций и обмана, и в этом нет ничего нового. На самом деле, хотя термин «мошенничество» является довольно новым для мира, вероятно, возникшим совсем недавно, в 1963 году, концепция намного старше. Я говорю о концепции «против». «Обман» был описан как «уверенность с чувством уверенности, основанной на недостаточных основаниях» и восходит к концу 1500-х годов. Я предполагаю, что практика желания чего-то, что есть у кого-то другого, и обмана, заставляющего их отказаться от этого, вероятно, восходит к временам наскальных рисунков или даже раньше.

Основной рецепт мошенничества или мошенничества почти всегда один и тот же. Мошенник заставляет жертву доверять им, а затем использует это доверие, чтобы убедить их сделать что-то, что не в их интересах. Это действие исторически было связано с потерей денег или собственности, но в наше время расширилось, чтобы включить информацию или доступ к чему-либо.

За прошедшие годы мошенники отточили свое мастерство, и эти мошенники даже без промедления перешли от традиционного пути к цифровому миру. Например, общепризнанная «Мошенничество с принцем Нигера» начиналось с использования традиционных почтовых служб для распространения. Еще до этого

была афера с испанским узником, вероятно, предшественник нигерийского. Переход на цифровое распространение через электронную почту не только устранил неприятную задачу облизывания и наклеивания штампов на бумажные конверты, но и значительно снизил стоимость организации атак. В моих недавних проверках в даркнете стоимость отправки 50 000 фишинговых писем через криминальную службу составила 65 долларов. Стоимость одной марки для отправки писем 50 000 человек составит 27 500 долларов США. Неудивительно, что фишинг по электронной почте так популярен.

За прошедшие годы эти мошенники выяснили, какие эмоциональные ловушки работают лучше всего, и знают, как противостоять практически любым возражениям или подозрительным вопросам. Они используют психологические уловки, чтобы цель оставалась в состоянии сильных эмоций. Будь то страх, возмущение, гнев, услужливость или любой другой набор эмоций, результат один и тот же. Это заставляет людей принимать неверные решения.

Вспомните время, когда вы испытали сильное беспокойство или страх. Теперь подумайте, насколько комфортно вы будете принимать важные решения в этом состоянии, особенно те, которые требуют сложных вычислений или критического мышления. Как правило, в состоянии сильных эмоций наша способность концентрироваться значительно снижается, и наши решения подвержены ошибкам. Это психическое состояние, при котором мошенники хотят своих целей. Если вы когда-либо попадали на место жульничества, когда вы оглядываетесь на цепочку событий, часто очень ясно, где вы пропустили, казалось бы, очевидные признаки обмана. Это типично, когда мы оглядываемся назад и удаляем эмоциональный фактор, омрачающий наши суждения.

Теперь давайте посмотрим, как пандемия повлияла на мир киберпреступности. Вначале переход на работу из дома был быстрым: организации закрывались, а персонал отправлялся на работу домой без предупреждения или с минимальным предупреждением. Люди начали накапливать предметы, и даже такие предметы первой необходимости, как туалетная бумага, стали дефицитным товаром. Когда школы закрылись, ученики были вынуждены начать занятия онлайн, к чему многие семьи не были готовы. Многие оказались в затруднительном финансовом положении. Для тех, кто все еще работает, с закрытием детских садов, уход за детьми стал проблемой, и у многих людей не было ноутбуков или компьютеров, установленных дома, чтобы поддерживать эти изменения. Даже веб-камеры стало почти невозможно получить, если вы не готовы платить цену скальперам.

Этот вид стресса - золотая жила для мошенников.

В течение нескольких недель после отключений, связанных с COVID-19, киберпреступники не отдыхали. Вместо этого они сосредоточились на создании новых атак…

Фишинговые электронные письма различались по своим сообщениям, темам и целям, однако почти все они были сосредоточены на неопределенности новой пандемии. Они включали электронные письма, якобы отправленные правительством или глобальными организациями, такими как Всемирная организация здравоохранения (ВОЗ), предлагающие недавно обновленные

инструкции, но вместо этого ведущие к зараженным вредоносным программам документам или поддельным порталам, требующим конфиденциальной информации для «подтверждения» личности жертвы. Другие использовали скудную информацию о пакетах стимулов для нацеливания на банковскую информацию или конфиденциальную личную информацию, такую как номера социального страхования, отправляя жертв на поддельные веб-сайты, утверждая, что они являются порталом для подтверждения информации о предстоящих платежах. Даже другие использовали поддельные мобильные приложения, утверждающие, что они созданы правительством, приложения отслеживания контрактов COVID-19 для распространения программ-вымогателей. Очевидно,

Помимо фишинга, процветало мошенничество. Поскольку частные лица и организации всех размеров изо всех сил пытаются получить средства индивидуальной защиты (СИЗ) и основные продукты, такие как дезинфицирующее средство для рук и отбеливатель, поле было готово для сбора. Поскольку нормальная цепочка поставок была растянута до предела, люди и организации были вынуждены обращаться за помощью к новым поставщикам. Как следствие, ряд организаций лишились денег из-за того, что мошенники продавали им СИЗ, которых у них не было. В число этих организаций входили больницы и исследовательские центры, а также традиционные предприятия и даже отдельные лица.

Со временем проблемы с поставками СИЗ и сопутствующих материалов уменьшились, однако некоторые по-прежнему трудно найти. По мере того как мы преодолеваем годичную отметку отключений от пандемии, мы по-прежнему сталкиваемся с некоторыми серьезными проблемами. Цены на нефть и газ растут, пластмассы дорожают, сталь и другие металлы быстро растут в цене, а импорт и экспорт застревают в доках, ожидая погрузки или разгрузки. Нехватка микрочипов сказывается даже на производстве новых автомобилей.

Продолжая бороться с этой пандемией, мы также должны работать, чтобы помочь людям лучше распознавать эти мошенничества. Независимо от того, является ли цель кражей данных, личных данных или денег, последствия будут значительными на организационном или личном уровне. Информирование людей об этих опасностях, а также о методах выявления мошенничества и защиты себя никогда не было так важно, как сейчас». ***(Erich Kron. The pandemonium of the pandemic: How working from home has changed the cybersecurity formula // BNP Media (https://www.securitymagazine.com/articles/95253-the-pandemonium-of-the-pandemic-how-working-from-home-has-changed-the-cybersecurity-formula). 20.05.2021).***

***

«Ранее в этом году Tesla обнаружила, что сотрудник украл более 6000 файлов, содержащих конфиденциальный код. Инженер-программист, проработавший всего две недели, был нанят как один из немногих, кто мог получить доступ к этим файлам.

Этот инцидент подчеркивает опасность, которую инсайдерские угрозы представляют для предприятий. Это проблема не только Tesla или какой-либо

одной отрасли. Сотрудники в результате неосторожных или злонамеренных действий могут представлять значительный риск для любой организации. Опрос, проведенный Институтом Ponemon, недавно показал, что внутренние угрозы увеличились на 47 процентов с 2018 по 2020 годы. Стоимость инцидентов с внутренними угрозами также выросла на 31 процент с 8,76 до 11,45 миллиона долларов за тот же период.

Если данные компании попадут в чужие руки, они могут нанести реальный вред людям и поставить компании в невыгодное положение с точки зрения конкуренции, способствуя потере внешнего доверия со стороны клиентов и других жизненно важных заинтересованных сторон. Вот почему организации должны вооружиться правильными инструментами для обнаружения и предотвращения внутренних угроз и утечки данных в ИТ-экосистеме.

Понимание различных форм внутренних угроз

В большинстве случаев внутренние угрозы включают злонамеренных внешних пользователей, которые получили доступ к законным учетным данным и, как следствие, могут проникнуть внутрь организации. Хотя чаще принято думать об этих злонамеренных хакерах, проникающих извне, реальность такова, что значительная утечка данных вызвана внутренними угрозами.

Приведенный выше пример Tesla прекрасно показывает, что может произойти, когда сотрудник со злым умыслом решит злоупотребить использованием своих аутентичных учетных данных для кражи данных, чтобы они могли продать их с целью получения финансовой выгоды, отомстить компании за любую предполагаемую несправедливость или помочь конкуренту.

Однако более распространенная форма внутренней угрозы исходит из неосторожных ошибок сотрудников, таких как решение обойти указанные процедуры безопасности, что приводит к неправильным решениям, таким как хранение конфиденциальных данных на незащищенных личных устройствах для удобства при работе из дома, а также стать жертвой фишинга. схемы.

Достижение более быстрой идентификации и профилактики

ИТ-экосистема в большинстве организаций за последний год значительно изменилась, чтобы приспособиться к изменениям, связанным с COVID-19, включая переход на удаленную работу, ускоренный перенос операций в облако и разрешение сотрудникам использовать личные устройства для доступа к корпоративным ИТ-ресурсам. Все это сделало защиту данных от внутренних угроз еще более сложной и доказало, что инструменты и стратегии реактивной безопасности, созданные для предшествующей эпохи, не могут идти в ногу с сегодняшней динамичной бизнес-средой.

Чтобы оставаться успешными в этом новом мире, предприятия должны получать и поддерживать постоянный контроль над конфиденциальными данными, которые больше не могут регулироваться локальными инструментами безопасности. Компании также должны обладать способностью обнаруживать и блокировать внутренние угрозы из любого места и в любое время, для чего требуются решения, которые могут блокировать, шифровать, применять управление цифровыми правами (DRM) и редактировать.

Организации также должны выбрать полнофункциональное решение с аналитикой поведения пользователей и сущностей (UEBA), которое использует машинное обучение для разработки базовых показателей поведения каждого сотрудника, чтобы можно было обнаруживать и устранять подозрительные отклонения от нормы по мере необходимости.

Максимизация бюджета и результатов

Команды безопасности должны решать все более сложные задачи, не выходя за рамки бюджета. Следовательно, они получат значительную выгоду от наличия простой в управлении платформы, которая может удовлетворить широкий спектр сценариев использования безопасности, включая описанные выше. Тем не менее, многие организации по-прежнему полагаются на ряд разрозненных инструментов безопасности. В результате получается серия неинтегрированных продуктов, из-за которых командам не хватает комплексных мер безопасности, необходимых для адекватной защиты от угроз.

Сложно управлять разрозненными инструментами безопасности, и они создают слепые зоны, которые тратят время и деньги и приводят к непоследовательным результатам, которые, несомненно, повлияют на скорость и точность программы безопасности. Вот почему компаниям необходимо решение, которое предлагает консолидированную простоту управления и комплексную защиту, эффективно защищает данные путем блокировки угроз и расширяет возможности бизнес-процессов без каннибализации финансовых ресурсов.

Ключевым моментом является внедрение унифицированной платформы вместо множества разрозненных продуктов, поэтому все популярнее становятся предложения для облачных сервисов безопасного доступа (SASE). Такие платформы предоставляют любым сотрудникам в любом месте безопасный доступ к любым данным или системам организации в облаке, в Интернете или в сети. Они делают это, не требуя каких-либо локальных аппаратных устройств (например, VPN), что позволяет группам безопасности обходить расходы на такие архитектуры, оптимизируя при этом их состояние безопасности.

Приоритет комплексного решения безопасности

Компании должны активно искать и внедрять правильные инструменты, чтобы уберечь группы безопасности от широкого спектра дорогостоящих неудач, в том числе тех, которые часто сопровождаются инсайдерскими атаками. Матрица взаимодействий внутри корпоративной ИТ-экосистемы становится все более сложной. Использование платформы SASE дает командам безопасности доступ к единой всеобъемлющей панели инструментов для настройки данных и политик защиты от угроз, которые применяются автоматически везде, где данные передаются, обеспечивая тем самым безопасность, непрерывность и рост бизнеса». ***(Anurag Kahol. It's Time to Prepare for a Rise in Insider Threats // Threatpost (https://threatpost.com/prepare-rise-insider-threats/166272/). 18.05.2021).***

***

«Кибератаки перешли от обычных ограблений типа «разбей и захвати» к более скрытным кампаниям, в которых хакеры тихонько разбивают лагерь в сетях на длительные периоды, воруя все, что попадает в их руки. Это

называется временем ожидания злоумышленника и является частью состязательного подхода, который стал еще более популярным среди хакеров, когда речь идет об атаках программ-вымогателей и утечках данных в 2021 году.

Рассмотрим недавние атаки программ-вымогателей, совершенные кибергангами Ryuk и Maze, когда злоумышленники прятались в тени центра обработки данных и в уязвимостях конечных точек, собирая контрразведку, крадя учетные данные и распространяя вредоносное ПО. Только после кражи всех цифровых товаров компании преступники, наконец, зашифруют файлы и потребуют выкуп, что становится все более распространенной атакой с «двойным вымогательством».

Согласно недавнему опросу института SANS, 14 процентов фирм указывают, что время между взломом и обнаружением составляет от одного до шести месяцев. Из тех, кто обнаружил вторжение, почти 10 процентов заявили, что на его локализацию и изгнание киберпреступников ушло до трех месяцев.

Борьба с временем ожидания с помощью EDR

Даже один день - это слишком много, когда речь идет о злоумышленниках, которые разбили лагерь в вашей сети, но их искоренение может оказаться сложной задачей для компаний с ограниченными ресурсами и ограниченным бюджетом. Вот почему уделяется повышенное внимание автоматизации обнаружения угроз и поиска вредоносных программ, скрывающихся в сетях организаций (включая ранее не обнаруженные угрозы), с использованием таких решений, как платформы расширенного обнаружения и реагирования на конечные точки (EDR).

Исследование, проведенное «Лабораторией Касперского», показало, что 28% компаний, внедривших решения EDR, смогли сократить время ожидания до нескольких часов.

В то время как EDR был основным продуктом для групп безопасности более десяти лет, для малых и средних организаций это относительно ново, когда им необходимо укрепить свой центр безопасности с помощью круглосуточного мониторинга.

Майкл Саби, вице-президент IDC по исследованиям, отмечает в недавнем отчете, что компании все чаще сталкиваются с более изощренными и агрессивными атаками. По его словам, это подтолкнуло службы безопасности к внедрению более проактивной защиты и принятию таких решений, как EDR, которые могут быстро реагировать на новые и неизвестные угрозы.

Натиск атак способствует принятию EDR

Этот переход от громких атак к скрытным злоумышленникам подталкивает защитников к тому, чтобы также немного изменить тактику от сосредоточения внимания на защите периметра до усиления EDR и поиска внутренних угроз.

Хакеры- невидимки, прячущиеся внутри конечных точек сети, были зафиксированы в недавних эксплойтах прошивки, атаках Active Directory и продолжающихся взломах, связанных с SolarWinds.

По словам исследователей, безотлагательность защитников усугубляется резким ростом не только кибератак, но и новых разновидностей вредоносных программ.

«Изощренное вредоносное ПО - новое оружие преступников и национальных государств», - говорится в отдельном отчете Института SANS. «Развитие таких угроз, как безфайловые вредоносные программы, программы-вымогатели, вредоносные программы нулевого дня и сложные вредоносные программы, в сочетании с обойденными средствами безопасности, представляет собой серьезный риск для предприятий», - говорится в отчете.

Несмотря на то, что атаки вредоносных программ в целом имеют тенденцию к снижению, их варианты становятся все более изощренными, а цели - более разнообразными. ФБР отметило в февральском отчете, что вредоносная программа Emotet семилетней давности оставалась серьезным противником на протяжении многих лет.

«Вредоносная программа Emotet претерпела существенные изменения с тех пор, как ее впервые заметили в отрасли», - написала специальный агент Джессика Най, руководитель киберотряда ФБР. «Он становился все более скрытным в своей способности получать доступ к вашему компьютеру, что затем открывало дверь для дополнительных вредоносных программ».

EDR может помочь идентифицировать даже неизвестные угрозы в режиме реального времени с помощью поведенческого анализа в сочетании со снятием отпечатков пальцев пользователя и сети. С помощью этих данных EDR может обнаруживать потенциально вредоносную активность и сообщать о ней. И, коррелируя временные рамки и используя передовые алгоритмы, EDR помогает командам безопасности работать в обратном направлении, чтобы определить вероятные точки взлома.

Оптимальные группы безопасности

Проблемы сохраняются для многих организаций с ограниченными ресурсами, у которых может быть персонал службы безопасности, но практически отсутствуют операционные центры безопасности (SoC). Но для обнаружения давно существующих злоумышленников требуется круглосуточный мониторинг сетей, особенно в эпоху удаленной работы.

«В прошлом году типичное предприятие было вывернуто наизнанку, - сказал Питер Ферстбрук, вице-президент и аналитик Gartner. «По мере формирования новой нормы всем организациям потребуется постоянная защитная позиция и ясность в отношении того, какие бизнес-риски [повышаются] удаленными пользователями».

EDR позволяет компаниям усилить защиту с помощью видимости в реальном времени на всех ваших конечных точках. Это позволяет группам безопасности отслеживать действия злоумышленников, даже если они пытаются проникнуть в вашу среду.

Kaspersky Optimum Security: оптимизация вашей защиты

Расширенный EDR лежит в основе решения Kaspersky для киберзащиты, которое называется Kaspersky Optimum Security. В решении используется свежий и инновационный подход к решению проблем безопасности во время ожидания и автоматизированному поиску сетевых угроз без разрушения бюджета.

Kaspersky Optimum Security обеспечивает автоматический поиск угроз, анализ первопричин и отслеживание угроз через единую облачную консоль, что позволяет небольшим командам осуществлять мониторинг, подобный SoC.

Kaspersky Optimum Security ориентирован на группы ИТ-безопасности с ограниченными ресурсами, которые управляют инфраструктурами малого и среднего размера.

Endpoint Protection - это защита конечных точек, серверов и шлюзов - наиболее распространенных точек входа и укрытий для злоумышленников.

Threat Hunting включает в себя упреждающее преследование сетевых угроз и угроз устройств, которые могут оставаться незамеченными и все еще активными в корпоративных инфраструктурах.

Advanced EDR включает в себя автоматизированные службы и единую облачную панель управления, что дает командам безопасности малого и среднего бизнеса стабильную рентабельность инвестиций…». ***(2021 Attacker Dwell Time Trends and Best Defenses // Threatpost (https://threatpost.com/2021-attacker-dwell-time-trends-and-best-defenses/166116/). 20.05.2021).***

***

«DBIR - отчет Verizon об утечках данных за 2021 год - показывает всплески изощренного фишинга, финансово мотивированных кибератак и криминального внимания к серверам веб-приложений.

…Последнее издание давно действующего DBIR не могло не вызывать сожаления по поводу прошедшего года, когда наблюдался резкий всплеск кибератак, поскольку COVID-19 привел к целевому фишингу на тему пандемии, атакам методом грубой силы на удаленных сотрудников и сосредоточиться на использовании или злоупотреблении платформами для совместной работы.

Многие другие наблюдали то же самое: например, в марте Касперский опубликовал отчет, в котором говорится, что атаки методом перебора (когда злоумышленники пробуют случайные имена пользователей и пароли для учетных записей) на соединениях по протоколу удаленного рабочего стола (RDP) увеличились во всем мире, увеличившись на 197 процентов. с 93,1 миллиона во всем мире в феврале до 277,4 миллиона в марте.

DBIR этого года проанализировал 5 258 нарушений от 83 участников из 88 стран: это примерно на треть больше нарушений, чем было проанализировано в прошлом году. Атаки фишинговых программ и программ-вымогателей на удаленных сотрудников выросли на 11% и 6% соответственно. Тем временем веб-приложения были нацелены на 39% взломов, что отражает стремительное распространение облачных сервисов, поскольку сотрудникам внезапно было приказано вернуться домой и остаться там.

Что касается мотивов кибератак, здесь нет ничего удивительного: как и в предыдущие годы, большинство злоумышленников участвовало в финансово мотивированных кампаниях. Что касается того, кто делает грязную работу, то злоумышленники, отнесенные к категории организованной преступности, несомненно, являются преступниками №1.

Учетные данные снова были главным разнообразием данных, которые они искали. Однако DBIR отмечает, что с 2015 года спонсируемые государством субъекты также преследовали el dinero: за последние шесть лет финансовые мотивы этих субъектов колебались между 6 и 16 процентами зарегистрированных нарушений. Неудивительно, что два наиболее распространенных термина киберпреступности, встречающиеся на криминальных форумах, связаны с банковскими счетами и кредитными картами.

Это было фишинговое шоу-фрик-шоу

В прошлогоднем отчете DBIR прогнозировалось возможное увеличение фишинга, использования украденных учетных данных, программ-вымогателей и нарушений конфигурации. Как это (обогащенное данными) инстинктивное чувство оправдывало себя?

Не так уж и плохо, заключил DBIR 2021 года: фишинг по-прежнему остается одной из основных разновидностей взломов, как и в последние два года. Однако он стал амбициозным, или, говоря языком DBIR, фишинг не ограничивался лишь тем, чтобы «почивать на чешуйчатых лаврах».

Например, целевые фишеры набросились на людей, находящихся в карантине, чтобы увеличить объем: частота фишинга в прошлом году сыграла свою роль в 36 процентах взломов, по сравнению с 25 процентами в прошлом году.

«Это увеличение коррелирует с нашими ожиданиями, учитывая первоначальный всплеск фишинга и фишинговых приманок, связанных с COVID-19, когда вступили в силу всемирные приказы о домохозяйствах», - говорится в сообщении DBIR. «Фишинг - это ответ

Это невозможно для подавляющего большинства нарушений в этой схеме, поскольку предпочтительной целью являются облачные почтовые серверы».

Джеймс Маккуигган, защитник осведомленности о безопасности в KnowBe4, отметил, что фишинг или другие кампании социальной инженерии стали исходным вектором атаки для взломов в течение последних нескольких лет. К тому же, все становится все сложнее, сказал он Threatpost по электронной почте в четверг.

«Киберпреступники творчески развивают свои атаки социальной инженерии», - сказал он. «Будь то сброс пароля к учетной записи в социальной сети или наличие комплектов, которые могут автоматически вставлять логотип целевой компании, или даже дезинформация о нехватке газа и о том, где его найти, - все это привело к тому, что люди попались на фишинговые приманки. любопытства, страха или жадности».

Мартин Маккий, исследователь безопасности и редакторский директор Akamai - одного из многих партнеров, которые предоставляют данные в DBIR - сказал Threatpost в четверг, что никого не должно удивлять, что Akamai соглашается с Verizon в том, что произошло «огромное увеличение» по количеству фишинговых компромиссов во время пандемии. Сам Akamai неоднократно анализировал влияние пандемии на трафик и модели атак за последний год, отметил он в электронном письме в четверг. Сам Akamai выпустил SOTI / исследовательский отчет о том, как это повлияло на собственные системы Akamai.

Кража учетных данных не прекращается

Типичный способ фишинга - это, конечно, подделка учетных данных. Вполне понятно, что команда DBIR ожидала увидеть скачок в использовании украденных учетных данных при взломах из-за вызванного пандемией роста удаленной рабочей силы. Было ли это верным предсказанием? Оказывается, не так уж и много: на самом деле количество украденных учетных данных, используемых для взломов, стабильно составляет около 25 процентов взломов, хотя, как отметила команда, это все еще значительное число.

Совместное использование рабочего стола кибер-мошенникам

Тим Эрлин, вице-президент по управлению продуктами и стратегии в Tripwire, указал на то, что он назвал «значимым» ростом использования совместного использования рабочего стола в качестве вектора атаки в 2020 году. Это тенденция, на которую организациям следует обратить внимание, сказал он Threatpost по электронной почте. в четверг.

«Если вы собираетесь использовать приложения для общего доступа к рабочему столу, вам следует убедиться, что вы можете провести точную инвентаризацию их использования, оценить их конфигурации и выявить в них уязвимости», - сказал Эрлин.

Что касается целевых ресурсов, серверы - в частности, серверы веб-приложений - доминировали в этой области с точки зрения целевых ресурсов. «Если вы собираетесь сосредоточить средства контроля безопасности на одном типе активов, вы получите наибольшую отдачу от своих веб-серверов», - сказал он.

Еще больше денег: внимание к старым ошибкам

Эрлин сказал, что это говорит о том, что злоумышленники продолжают использовать старые уязвимости, но новые уязвимости представляют меньшую проблему. «Если вы отвечаете за управление уязвимостями в своей организации, стоит изучить, как ваша тактика расстановки приоритетов согласуется с данными об эксплойтах», - предложил он.

«Неправильная конфигурация составляет самый большой процент различных ошибок, вызывающих нарушения. Возможно, было бы интереснее потратить ресурсы на новейший инструмент для поиска угроз, основанный на искусственном интеллекте, но внедрение управления конфигурацией и обнаружения изменений будет иметь большое значение для поддержания целостности ваших цифровых активов», - сказал Эрлин.

Вот еще несколько выводов из DBIR этого года:

85 процентов нарушений связаны с человеческим фактором.

61% нарушений касались учетных данных.

13% инцидентов, не связанных с отказом в обслуживании (non-DoS), связаны с программами-вымогателями.

3 процента нарушений связаны с эксплуатацией уязвимости…» ***(Lisa Vaas. Verizon: Pandemic Ushers in ⅓ More Cyber-Misery // Threatpost (https://threatpost.com/verizon-pandemic-cyber-misery/166168/). 14.05.2021).***

***

«Бельгийский интернет-провайдер Belnet восстановил свои услуги после масштабной распределенной атаки типа «отказ в обслуживании» (DDoS) в

начале этой недели, в результате которой был отключен доступ в Интернет для многочисленных правительственных, общественных, научных и образовательных учреждений, включая парламент Бельгии и некоторые правоохранительные органы.

Атака произошла во вторник в 11:00 (GMT) в Европе и затронула «все учреждения, подключенные к сети Belnet», которых насчитывается около 200, согласно заявлению, опубликованному в среду на веб-сайте Belnet.

Более того, после расследования выяснилось, что атака - скоординированные усилия, нацеленные на правительство Бельгии - также затронула других интернет-провайдеров, что, по сообщениям, было самой крупной DDoS-атакой, которую видела страна. Бельгия является штаб-квартирой Европейского Союза (ЕС) и, следовательно, ключевым центром деятельности и принятия решений, влияющих на глобальный политический и социально-экономический ландшафт.

Белнет восстановил обслуживание своей сети и веб-сайта к вечеру вторника, однако, по словам Белнета, атака продолжает иметь постоянные последствия: некоторые клиенты по-прежнему не могут подключиться к веб-сайтам и онлайн-сервисам.

«Мы полностью осознаем влияние на организации, подключенные к нашей сети, и их пользователей, и мы осознаем, что это серьезно нарушило их работу», - сказал в заявлении технический директор Belnet Дирк Хэкс.

Однако атака была «такого масштаба, что вся наша сеть была переполнена», - сказал он. «Тот факт, что исполнители атаки постоянно меняли тактику, еще более затруднял ее нейтрализацию», - сказал Хаекс.

Нет признаков вторжения

На данный момент нет никаких признаков того, что киберпреступники проникли в сеть какого-либо из затронутых учреждений или организаций, поскольку похоже, что атака была направлена исключительно на насыщение сетей с целью нарушения трафика, добавил он.

Действительно, Belnet сообщил новостному агентству VRT, работа которого также была нарушена из-за атаки, что это был первый случай, когда поставщик услуг столкнулся с таким «гигантским потоком данных».

Масштабность атаки указывает на то, что злоумышленники не держали Belnet в поле зрения, а были нацелены на то, чтобы вывести из строя сеть бельгийского правительства, сказал VRT Герт Баудевейнс, генеральный директор охранной компании Secutec. Secutec предоставляет услуги безопасности правительству Бельгии.

«Это было сделано через всех операторов связи», - сказал он в отчете VRT. «Провайдеры, такие как Telenet и Proximus, также подверглись этой атаке».

Согласно отчетам, поток трафика, который затопил сети при атаке, поступил примерно из 29 стран, хотя первоначальный источник или исполнитель атаки еще не идентифицирован, согласно Belnet.

Правоохранительные органы, заседания парламента сорваны

В среду The Brussels Times сообщила о некоторых конкретных и продолжающихся последствиях атаки на государственные учреждения Бельгии.

Согласно сообщению, парламенту Бельгии пришлось отложить несколько заседаний из-за нападения.

В результате инцидента также был заблокирован доступ к онлайн-сервисам столичной полиции, например, в Брюсселе и Антверпене, а также к веб-сайту Брюсселя. По состоянию на утро четверга в Европе все восстановлено.

Атака также вызвала проблемы с дистанционным обучением в нескольких университетах и колледжах, которые продолжают предлагать онлайн-услуги из-за продолжающейся пандемии коронавируса, а также вызвала проблемы с покупкой билетов у брюссельской транспортной компании STIB.

Belnet, Центр кибербезопасности Бельгии и другие органы власти и организации безопасности продолжают отслеживать и расследовать ситуацию, и Belnet подала жалобу в Федеральное управление по компьютерным преступлениям Бельгии». ***(Elizabeth Montalbano. Massive DDoS Attack Disrupts Belgium Parliament // Threatpost (https://threatpost.com/ddos-disrupts-belgium/165911/). 06.05.2021).***

***

«Toyota призналась в паре кибератак.

Первый пришелся на европейские операции ее дочерней компании Daihatsu Diesel Company, принадлежащей Toyota компании, которая разрабатывает двигатели. В заявлении [PDF] от 16 мая Daihatsu сообщила, что «14 мая 2021 года у компании возникла проблема с доступом к файловому серверу во внутренней системе».

«После непродолжительного расследования причина этой проблемы была подтверждена кибератакой путем несанкционированного доступа третьей стороны», - говорится в заявлении. Daihatsu остановил распространение информации в других офисах, начал расследование и пообещал обновить информацию. На момент написания этого сообщения не поступало.

Между тем, многочисленные японские СМИ сообщают, что дочерняя компания Toyota Auto Parts Manufacturing Mississippi раскрыла атаку с использованием программ-вымогателей. В отчетах говорится, что некоторые финансовые данные и данные о клиентах были извлечены и разоблачены - тактика, которую поставщики программ-вымогателей используют, чтобы получить рычаги для удовлетворения своих финансовых потребностей. В сообщениях говорится, что производство автозапчастей в Миссисипи не заплатило и не прервалось.

Технические проблемы Toyota усугубляются ее решением остановить на несколько дней в июне три производственные линии на двух заводах из-за нехватки запчастей. Хотя в заявлении автопроизводителя не упоминается о нехватке кремния, это широко признано.

Toyota Japan извинилась за производственные проблемы, но также указала, что у нее 29 производственных линий на 14 заводах, так что это замедление не является серьезным сокращением производства». ***(Simon Sharwood. Toyota rear-ended by twin cyber attacks that left ransomware-shaped dents // The Register (https://www.theregister.com/2021/05/21/toyota_cyber_attacks/). 21.05.021).***

***

«Monday.com недавно раскрыл последствия атаки на цепочку поставок Codecov, которая затронула несколько компаний.

Monday.com - это онлайн-платформа для управления рабочим процессом, используемая менеджерами проектов, специалистами по продажам и CRM, маркетинговыми командами и различными другими организационными отделами.

Среди клиентов платформы такие известные имена, как Uber, BBC Studios, Adobe, Universal, Hulu, L'Oreal, Coca-Cola и Unilever.

Как сообщал BleepingComputer в прошлом месяце, популярный инструмент покрытия кода Codecov стал жертвой атаки цепочки поставок, которая длилась два месяца.

В течение этого двухмесячного периода злоумышленники модифицировали законный инструмент Codecov Bash Uploader для извлечения переменных среды (содержащих конфиденциальную информацию, такую как ключи, токены и учетные данные) из сред CI / CD клиентов Codecov.

Сообщается, что используя учетные данные, полученные из подделанного Bash Uploader, злоумышленники Codecov взломали сотни клиентских сетей.

Доступ к исходному коду Monday.com при атаке Codecov

Клиент Codecov Monday.com недавно объявил, что подвергся атаке на цепочку поставок Codecov.

В форме F-1, поданной на этой неделе в Комиссию по ценным бумагам и биржам США (SEC) для предлагаемого первичного публичного предложения (IPO) Monday.com, компания поделилась подробностями о масштабах нарушения Codecov.

После расследования взлома Codecov Monday.com обнаружил, что неавторизованные участники получили доступ к копии их исходного кода, доступной только для чтения.

Однако компания заявляет, что на сегодняшний день нет никаких доказательств того, что исходный код был изменен злоумышленниками или что какой-либо из ее продуктов был затронут.

Кроме того, «злоумышленник действительно получил доступ к файлу, содержащему список определенных URL-адресов, указывающих на публично транслируемые формы и представления клиентов, размещенные на нашей платформе, и мы связались с соответствующими клиентами, чтобы сообщить им, как восстановить эти URL-адреса», - заявляет компания.

В настоящее время также нет никаких указаний на то, что данные клиентов Monday.com были затронуты этим инцидентом, хотя компания продолжает расследование.

До раскрытия информации в документации SEC на этой неделе, Monday.com ранее заявляла, что после инцидента с Codecov они удалили доступ Codecov к своей среде и полностью прекратили использование сервиса:

«Узнав об этой проблеме, мы приняли незамедлительные меры по ее устранению, в том числе отозвали доступ Codecov, прекратили использование службы Codecov, ротацию ключей для всех производственных сред и сред разработки monday.com, а также привлекли ведущих судебных экспертов по

кибербезопасности для помощи в нашем расследовании», - сказала служба безопасности Monday.com в сообщении в блоге на прошлой неделе.

Monday.com - одна из многих жертв взлома Codecov

Monday.com - не первая и не единственная компания, пострадавшая от атаки на цепочку поставок Codecov.

Хотя атака Codecov оставалась незамеченной в течение двух месяцев, полный масштаб атаки продолжает разворачиваться даже после ее обнаружения.

Как сообщает BleepingComputer на этой неделе, американская компания по кибербезопасности Rapid7 сообщила, что злоумышленники Codecov получили доступ к некоторым из их репозиториев исходного кода и учетным данным.

В прошлом месяце HashiCorp объявила, что их закрытый ключ GPG был раскрыт в результате атаки.

Этот ключ использовался для подписания и проверки выпусков программного обеспечения, поэтому его пришлось ротации.

Платформа облачных коммуникаций Twilio, поставщик облачных услуг Confluent и страховая компания Coalition также сообщили, что злоумышленники Codecov получили доступ к их частным репозиториям.

С тех пор нескольким другим клиентам Codecov пришлось поменять свои учетные данные. Были ли они затронуты или нет, и в каком качестве, остается загадкой.

До того, как Codecov обнаружил нарушение, Bash Uploader использовался тысячами проектов с открытым исходным кодом…

Поскольку нарушение Codecov сравнивается с атакой на цепочку поставок SolarWinds, федеральные следователи США вмешались, чтобы полностью исследовать ее последствия.

«На дату этого проспекта мы не обнаружили никаких доказательств каких-либо несанкционированных модификаций нашего исходного кода или какого-либо воздействия на наши продукты», - сообщает Monday.com, добавляя мелкий шрифт в файл SEC: «Однако обнаружение новой или иной информации о кибератаке Codecov, в том числе в отношении ее масштабов и любого потенциального воздействия на нашу ИТ-среду, в том числе в отношении потери, непреднамеренного раскрытия или несанкционированного распространения служебной информации или конфиденциальных или конфиденциальных данных о нас или наших клиентов, либо уязвимости в нашем исходном коде могут привести к судебным разбирательствам и потенциальной ответственности за нас, нанести ущерб нашему бренду и репутации, негативно повлиять на наши продажи или иным образом нанести ущерб нашему бизнесу. Любые претензии или расследования могут привести к серьезным внешним и внутренним юридические и консультационные расходы, а также отвлечение внимания руководства от ведения нашего бизнеса».

В прошлом месяце Codecov начал рассылать дополнительные уведомления пострадавшим клиентам и раскрыл подробный список индикаторов взлома (IOC), то есть IP-адресов злоумышленников, связанных с этой атакой цепочки поставок.

Пользователи Codecov должны сканировать свои CI / CD-среды и сети на предмет каких-либо признаков взлома и в качестве меры предосторожности

чередовать все секреты, которые могли быть раскрыты». ***(Ax Sharma. Codecov hackers gained access to Monday.com source code // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/codecov-hackers-gained-access-to-mondaycom-source-code/). 18.05.2021).***

***

«Центр рассмотрения жалоб на Интернет-преступления (IC3) ФБР за последние 14 месяцев получил 100% жалоб на киберпреступления.

Когда IC3 впервые начала регистрировать жалобы в 2000 году, потребовалось семь лет, чтобы собрать 1 миллион жалоб. С тех пор на каждый дополнительный миллион жалоб уходило в среднем 29,5 месяцев.

За период с марта 2020 года по май 2021 года в IC3 всего за 14 месяцев произошел значительный рост жалоб на 1 миллион.

ФБР объясняет рост жалоб киберпреступниками, которые пользуются людьми, работающими из дома, из-за пандемии и роста тематических атак COVID-19.

«В 2020 году, когда американская общественность была сосредоточена на защите наших семей от глобальной пандемии и помощи другим нуждающимся, киберпреступники воспользовались возможностью извлечь выгоду из нашей зависимости от технологий, чтобы заняться Интернет-преступностью», - говорится в сообщении IC3. Отчет о преступности в Интернете за 2020 год.

«Эти преступники использовали фишинг, спуфинг, вымогательство и различные виды интернет-мошенничества для нацеливания на наиболее уязвимые слои нашего общества - медицинские работники, ищущие средства индивидуальной защиты, семьи, ищущие информацию о стимулирующих проверках для оплаты счетов, и многие другие.

В рамках отчета ФБР заявляет, что тремя основными преступлениями, зарегистрированными в 2020 году, были фишинг, мошенничество с неплатежами / недоставкой и вымогательство.

Тем не менее, жертвы потеряли больше всего денег из-за мошенничества с BEC (убытки 1,8 миллиарда долларов), мошенничества в романтических отношениях (убытки на 600 миллионов долларов) и мошенничества с инвестициями (336 миллионов долларов)». ***(Lawrence Abrams. FBI says cybercrime complaints more than doubled in 14 months // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-says-cybercrime-complaints-more-than-doubled-in-14-months/). 18.05.2021).***

***

«Каждый час злоумышленник начинает новое сканирование общедоступной сети на предмет уязвимых систем, продвигаясь более быстрыми темпами, чем глобальные предприятия, когда пытается выявить серьезные уязвимости в своих сетях.

Усилия злоумышленников значительно возрастают, когда появляются критические уязвимости, и новые сканирования в Интернете происходят в течение нескольких минут после раскрытия.

Обратите внимание на разрыв

Злоумышленники неутомимы в поисках новых жертв и стремятся выиграть гонку за исправлением уязвимых систем. Хотя компании стремятся выявить проблемы в своих сетях, пока не стало слишком поздно, они действуют гораздо медленнее.

Данные получены от исследовательской группы Palo Alto Networks Cortex Xpanse, которая в период с января по март этого года отслеживала сканирование с 50 миллионов IP-адресов 50 глобальных предприятий, некоторые из которых входят в список Fortune 500.

Исследователи обнаружили, что компаниям требуется в среднем 12 часов, чтобы найти новую серьезную уязвимость. Почти треть всех выявленных проблем связана с протоколом удаленного рабочего стола, который является общей целью программ-вымогателей, поскольку они могут использовать его для получения административного доступа к серверам.

Неверно настроенные серверы баз данных, уязвимости нулевого дня в критически важных продуктах от таких поставщиков, как Microsoft и F5, и небезопасный удаленный доступ (Telnet, SNMP, VNC) завершают список высокоприоритетных недостатков.

По данным Palo Alto Networks, компании выявляли одну такую проблему каждые 12 часов, что резко контрастировало со средним временем, затрачиваемым злоумышленниками на инвентаризацию всего за один час.

Однако в некоторых случаях злоумышленники увеличивали частоту сканирования до 15 минут, когда появлялись новости о критической ошибке, доступной для удаленного использования, в сетевом устройстве; и скорость упала до пяти минут после обнаружения ошибок ProxyLogon в Microsoft Exchange Server и проблемах Outlook Web Access (OWA).

Palo Alto Networks рекомендует группам безопасности изучить следующий список служб и систем, чтобы ограничить поверхность атаки.

Исследователи отмечают, что они составили список, основываясь на двух принципах: определенные вещи не должны быть открыты для публичного доступа (плохие протоколы, порталы администрирования, VPN), а защищенные активы могут стать уязвимыми со временем.

Сервисы удаленного доступа (например, RDP, VNC, TeamViewer)

Небезопасные службы обмена / обмена файлами (например, SMB, NetBIOS)

Системы без исправлений, уязвимые для публичных эксплойтов и систем с истекшим сроком эксплуатации (EOL)

Порталы систем ИТ-администрирования 5. Приложения для важных бизнес-операций (например, Jenkins, Grafana, Tableau)

Незашифрованные логины и текстовые протоколы (например, Telnet, SMTP, FTP)

Устройства с прямым доступом к Интернету вещей (IoT)

Слабая и небезопасная / устаревшая криптовалюта

Открытая инфраструктура разработки

Небезопасные или заброшенные маркетинговые порталы (которые, как правило, работают на Adobe Flash)

Почему компании отстают

Одним из объяснений этого отставания в определении рисков в сети является неправильный процесс управления уязвимостями, основанный на базе данных известных уязвимостей.

Сканеры, использующие эту базу данных, не обнаружат новых проблем, пока база данных не получит обновление, которое может происходить с задержкой в несколько часов или даже дней. Более того, сканеры не видят все устройства в сети…

С другой стороны, злоумышленники пользуются дешевыми облачными вычислительными мощностями, которые позволяют им выполнять сканирование в Интернете.

В настоящее время сканирование Интернета больше не ограничивается хорошо финансируемыми актерами. Облачные технологии позволили создать инфраструктуру, которая может «общаться» по одной паре порт-протокол с каждым устройством в общедоступной сети всего за 45 минут». ***(Ionut Ilascu. Hackers scan for vulnerable devices minutes after bug disclosure // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-scan-for-vulnerable-devices-minutes-after-bug-disclosure/). 19.05.2021).***

***

«Національна бібліотека Чехії заявила, що її системи у ніч на 18 травня зазнали хакерської атаки, у зв'язку з чим робота всіх систем тимчасово призупинена.

Про це у коментарі ČTK розповіла речниця закладу Ірена Манакова.

За її словами, фахівці зараз працюють над безпечним відновленням ключових систем, також готується заява до правоохоронних органів.

Опівдні Національна бібліотека розмістила у своїх соцмережах повідомлення про те, що повністю призупиняє роботу онлайн у зв'язку з наслідками кібератаки. Згодом повідомили, що деякі бази даних все ж доступні.

Раніше у Чехії від кібератак постраждали деякі лікарні та відомства.

У здійсненні атаки на стратегічну установу у 2019 році, та декілька лікарень навесні 2020 року запідозрили російських хакерів». ***(Національна бібліотека Чехії постраждала від хакерської атаки // Європейська правда (https://www.eurointegration.com.ua/news/2021/05/18/7123311/). 18.05.2021).***

***

«Медицинские организации по-прежнему представляют собой главную цель для хакеров - если не ведущую: средняя стоимость взлома для отрасли сейчас составляет 7,13 миллиона долларов (самый высокий показатель среди всех секторов) по сравнению с менее чем 4 миллионами долларов для организаций в целом.

Более того, больницам и другим медицинским организациям требуется 329 дней на выявление и устранение нарушения (т.е. Жизненный цикл инцидента), что на семь недель больше, чем средний жизненный цикл для компаний в целом. Опять же, здравоохранение возглавляет все сектора в этой категории.

Учитывая обстоятельства, руководители отрасли по информационной безопасности (CISO) и их команды твердо сосредоточены на внедрении новых инструментов и методов для лучшей защиты своих цифровых активов. Но - с учетом волны глобальных правил, которые сейчас действуют, и вероятность того, что они появятся, они не могут ограничивать свои ресурсы и цели исключительно кибербезопасностью как отдельными усилиями, поскольку конфиденциальность данных также стала критически важным приоритетом.

В частности, общий регламент Европейского Союза по защите данных (GDPR) вызвал волну, потребовав от предприятий включать защиту личных данных при разработке своих продуктов и услуг. Кроме того, они должны задокументировать, как и где хранятся данные, как они обрабатываются, и, что наиболее важно, предоставить потребителям контроль над тем, как организации могут использовать их данные.

В США по меньшей мере полдюжины штатов приняли аналогичные правила: например, чтобы соответствовать недавно принятому Закону о правах конфиденциальности в Калифорнии (CPRA), предприятия должны свести к минимуму использование, хранение и передачу личной информации. разумно необходимо для реализации заявленного ими намерения (т. е. принципа «минимизации данных» GDPR). Организациям также придется применять меры безопасности, обеспечивающие конфиденциальность, целостность и доступность личных данных. Если они этого не сделают и последующая атака раскрывает личную информацию, затронутые потребители смогут подать в суд на взломанные компании.

Если все это кажется сложным, то это потому, что это так. К счастью, кибербезопасность и соблюдение требований конфиденциальности не являются взаимоисключающими дисциплинами, поскольку принимаются меры для наилучшей защиты цифровых активов и устройств, которые служат прочной основой для эффективной стратегии конфиденциальности данных: безопасность заключается в предотвращении доступа к данным неавторизованными лицами, будь то интеллектуальная собственность или личная информация (PII) пациентов и сотрудников. Конфиденциальность - это правильное управление, сбор, совместное использование и, при необходимости, удаление данных о клиентах / пациентах.

Соблюдение конфиденциальности является естественным продолжением проверенных методов обеспечения безопасности - и то, и другое зависит от надлежащего выполнения защиты данных и управления. Чтобы проиллюстрировать это, давайте представим следующие основные компоненты для этих двух, начиная с того места, где должны начать работу директора по информационным технологиям - кибербезопасность:

Основные компоненты кибербезопасности

Шифрование. Директора по информационной безопасности в сфере здравоохранения должны использовать алгоритмы для шифрования или кодирования конфиденциальной информации, чтобы ее можно было прочитать только с помощью ключа дешифрования. Таким образом, они не позволят злоумышленникам прочитать информацию, если они перехватят ее во время атаки.

Контроль доступа. Все дело в том, чтобы точно ответить на вопрос: «Вы тот, кем себя называете - и принадлежите ли вы к этому месту?» вопрос. Если неавторизованные стороны получают доступ, скажем, к контроллеру домена, они могут поставить под угрозу критически важные учетные записи, пользовательские данные и служебную / конфиденциальную информацию.

Человеческий интеллект. Текущие инновации, такие как автоматизация и искусственный интеллект (ИИ), значительно расширяют возможности групп безопасности, но они не могут их заменить. Нам всегда потребуется человеческая интуиция аналитиков, охотников за угрозами и лиц, отвечающих на инциденты, чтобы успешно укрепить сети, системы, приложения и устройства.

Управляемое обнаружение и ответ (MDR). Директорам по информационной безопасности необходимо обеспечить полную видимость всей активности в сети, журналах и конечных точках, с круглосуточным обнаружением и реагированием в режиме 24/7/365. Но у них может не быть для этого ни персонала, ни бюджета. Именно тогда им следует подумать о привлечении партнера по MDR, чтобы передать многие (если не все) эти обязанности проверенным экспертам в области поиска, предотвращения и смягчения угроз.

Основные компоненты конфиденциальности данных

Открытие и классификация. Благодаря обнаружению, директора по информационным технологиям и их команды сканируют свою цифровую экосистему, чтобы определить, где существуют как структурированные, так и неструктурированные данные. С помощью классификации они классифицируют и приоритизируют все свои данные в соответствии с уровнями риска и соображениями конфиденциальности. Опять же, это демонстрирует, что конфиденциальность и безопасность не исключают друг друга. В течение многих лет службы безопасности жили мантрой: «Вы не можете защитить то, чего не видите». Концепция распространяется на обнаружение и классификацию конфиденциальности.

Минимизация. В соответствии с требованиями GDPR и других нормативных актов, организации должны ограничивать объем собираемых и хранимых персональных данных - они не должны хранить каждую биту, с которой они сталкиваются. Оптимальная минимизация приведет к уменьшению цифрового следа, что снизит риск.

Согласие. Такие пользователи, как пациенты, хотят знать, что больница планирует делать с их данными. Чтобы решить эту проблему, правила предписывают организациям получить согласие этих лиц перед любым предполагаемым использованием их информации.

Удаление. В рамках всеобъемлющей политики конфиденциальности команды должны иметь возможность удалять данные по запросу пользователя.

Эти шаги в конечном итоге приводят к качеству, к которому все медицинские организации должны стремиться сегодня: прозрачности.

В конце концов, людей беспокоит то, как их данные собираются, управляются и защищаются. Хранение их в неведении может принести краткосрочные выгоды, но, скорее всего, приведет к возможным нарушениям / штрафам и репутационному ущербу. Демонстрируя свою приверженность

высочайшим стандартам цифровой защиты и надзора / раскрытия конфиденциальности данных, руководители по информационной безопасности могут значительно отличить ценность своей организации от остальных. Это хорошо не только для безопасности и конфиденциальности, но и для бизнеса». ***(Why Healthcare Organizations Must Incorporate Data Privacy into Their Cybersecurity Strategies – and How to Do It // HealthcareScene.com (https://www.healthcareittoday.com/2021/05/27/why-healthcare-organizations-must-incorporate-data-privacy-into-their-cybersecurity-strategies-and-how-to-do-it/). 27.05.2021).***

***

«Министерство внутренних дел Бельгии оказалось целью «изощренного» кибершпионажа, сообщил во вторник RTBF пресс-секретарь общественного телеканала RTBF.

Директор по коммуникациям Федеральной государственной службы внутренних дел Оливье Мэренс, однако, настаивал на том, что серверы министерства хорошо защищены и что хакерам не удалось получить самые конфиденциальные данные.

Федеральная прокуратура начала расследование, чтобы установить происхождение операции, данные, которые были взломаны, и участие иностранного государства.

По мнению бельгийских экспертов, атака, раскрытая в марте, была начата в 2019 году.

Другая крупномасштабная атака в начале мая привела к сбою сети Belnet, которая соединяет высшие учебные заведения, университеты, исследовательские центры и органы государственного управления.

Но целью атаки на МВД было не заглушить сайт или потребовать выкуп.

По словам экспертов, которых цитирует RTBF, он был «более сложным и хорошо продуманным, что наводило нас на мысль, что это был шпионаж».

Маэренс сказал, что «были приняты срочные меры для предотвращения доступа злоумышленника», а безопасность сервера была усилена.

Обнаружение атаки держалось в секрете, чтобы не раскрыть уязвимость системы до тех пор, пока она не будет защищена.

Лидеры ЕС на встрече в Брюсселе в понедельник и вторник обсудили угрозу кибератак во время встреч, посвященных напряженности блока с Россией, которую обвиняют в проведении ряда таких операций.

«Уровень вмешательства России как в шпионскую деятельность, так и в интернет-манипуляции стал поистине тревожным», - заявил премьер-министр Италии Марио Драги на пресс-конференции.

«Мы должны усилить нашу защиту, особенно с точки зрения кибербезопасности. Мы должны сделать все, как на национальном уровне, так и на уровне ЕС», - сказал Драги». ***(Belgium Interior Ministry Targeted in Cyber Attack // Wired Business Media (https://www.securityweek.com/belgium-interior-ministry-targeted-cyber-attack). 25.05.2021).***

***

«Серия громких кибератак на цели на Западе высветила уязвимость компаний и учреждений, сделав проблему более приоритетной для общества, но без легкого решения.

Последний инцидент, продемонстрировавший способность киберпреступников нарушать повседневную жизнь, произошел в начале мая, когда компания Colonial Pipeline, американский оператор ключевого топливопровода, стала жертвой программы-вымогателя.

В результате атаки его компьютерные системы были зашифрованы, что привело к отключению всех операций и нехватке топлива для американских водителей.

В конце 2020 года власти США также обнаружили, что хакеры взломали программное обеспечение SolarWinds, которым управляет большая часть правительства США и компании по всей стране. Обвиняли Россию.

Другие атаки включают взлом Демократической партии перед выборами в США в 2016 году, а также крупные глобальные вспышки вредоносного ПО под названием WannaCry и NotPetya, которые парализовали компьютеры по всему миру в 2017 году.

Помимо крупных инцидентов, о которых пишут в новостях, компании и эксперты в области кибербезопасности в течение многих лет предупреждали о нарастающей волне онлайн-атак - некоторые из них организованы государством, некоторые - мотивированы преступлением.

«Трудно представить, что у нас не было достаточно серьезных киберинцидентов, чтобы каждый осознал, насколько это важно», - сказала Сюзанна Сполдинг из Вашингтонского аналитического центра Центра стратегических и международных исследований.

Несмотря на все, этому вопросу «не уделялось должного внимания», - сказала она.

- *Самодовольство* -

Лучшие средства защиты от киберпреступлений со стороны частных лиц и небольших компаний просты и почти бесплатны: удаление подозрительных электронных писем, регулярное обновление программного обеспечения, изменение паролей и хранение сохраненных резервных копий.

Более крупные организации могут позволить себе специализированные группы ИТ-безопасности, а наиболее оснащенные сотрудники используют внешние службы мониторинга, чтобы следить за своими сетями и круглосуточно проверять наличие вторжений, которые предсказывают серьезную атаку.

Но многие организации остаются довольными, сказал Сполдинг.

«В мире есть два типа компаний: те, которые были взломаны, и те, кто еще не обнаружил это», - сказала она AFP.

Другая проблема заключается в том, что во многих странах не хватает подготовленных ИТ-специалистов, что увеличивает заработную плату за наиболее востребованные навыки, делая их недоступными для многих организаций, особенно в государственном секторе.

Адам Мейерс из компании CrowdStrike, занимающейся кибербезопасностью, говорит, что ключом к безопасности часто является лучшая защита, чем самые слабые цели.

«Есть старая пословица, что вам не нужно бежать быстрее медведя, чтобы убежать. Вы должны бежать быстрее, чем человек рядом с вами», - сказал он.

- *Государственные возможности* -

Одной из сфер, приоритетных для западных правительств, является наращивание собственных кибервоенных мощностей, которые позволяют государствам расследовать и отражать атаки, а также проводить собственные шпионские операции и операции.

«В течение последнего десятилетия он находился в арсенале армий и спецслужб как часть конфликта, который не обязательно является открытым, но является латентным», - сказал Жюльен Носетти, исследователь из института Geode при университете Париж 8.

Национальный индекс кибернетической мощи, составленный Белферским центром при Гарвардском университете, ставит Соединенные Штаты в первую 30-ку стран мира по своим амбициям и кибер-возможностям, на втором месте Китай и на третьем - Великобритания.

Досягаемость и мощь Агентства национальной безопасности США были раскрыты в 2013 году после утечки информации беглого подрядчика Эдварда Сноудена.

«Европу и Соединенные Штаты иногда изображают как жертв и хороших парней в этой сфере... но это не так. Все люди не видят наших собственных операций», - сказал Ночетти.

И правила взаимодействия все еще определяются, с многосторонней попыткой создать своего рода структуру для государств, которые не могут добиться прогресса.

Некоторые эксперты опасаются, что в один прекрасный день поддерживаемая государством кибератака вызовет спираль репрессий и ответных репрессий, которые могут спровоцировать боевые действия в реальной жизни.

Страны, возможно, накопили достаточно цифрового оружия, чтобы служить сдерживающим фактором.

«Одна из причин, по которой Россия, США и Китай не выключают друг друга, заключается в том, что они боятся реакции», - сказал Адам Сигал, директор программы «Политика в области цифровых технологий и киберпространства» Совета по иностранным делам. Отношения, аналитический центр США». ***(Rising Cyberattacks in West Highlight Vulnerabilities // Wired Business Media (https://www.securityweek.com/rising-cyberattacks-west-highlight-vulnerabilities). 26.05.2021).***

***

«Microsoft предупредила, что Nobelium в настоящее время проводит фишинговую кампанию после того, как поддерживаемой Россией группе удалось взять под контроль учетную запись, используемую USAID на платформе электронного маркетинга Constant Contact.

По данным Microsoft, фишинговая кампания охватила около 3000 учетных записей, связанных с государственными учреждениями, аналитическими центрами, консультантами и неправительственными организациями. США получили большую часть вредоносных писем, но они достигли как минимум 24 стран.

«На этой неделе Nobelium начал атаки, получив доступ к учетной записи Constant Contact USAID, - сказал корпоративный вице-президент Microsoft по безопасности и доверию клиентов Том Берт.

«Оттуда злоумышленник мог распространять фишинговые электронные письма, которые выглядели аутентичными, но содержали ссылку, при нажатии на которую вставлялся вредоносный файл, используемый для распространения бэкдора, который мы называем NativeZone. Этот бэкдор может обеспечивать широкий спектр действий, от кражи данных до заражение других компьютеров в сети».

Берт добавил, что многие электронные письма были заблокированы, и нет оснований полагать, что атаки связаны с какой-либо уязвимостью в продуктах Microsoft.

Кампания была обнаружена в феврале, и Microsoft наблюдала, как Nobelium меняет свой подход к переносу вредоносного кода на компьютеры жертв, говорится в сообщении Microsoft Threat Intelligence Center (MTIC).

В одном случае, если сервер, контролируемый Nobelium, обнаружил устройство Apple iOS, он обнаружил уязвимость универсального межсайтового скриптинга WebKit. В среду Apple заявила, что ей известно об активной эксплуатации уязвимости.

«В кампании 25 мая было несколько итераций. В одном примере электронные письма, похоже, исходят от USAID, имея при этом подлинный адрес электронной почты отправителя, который соответствует стандартной службе постоянных контактов», - сказал MTIC.

«Этот адрес (который различается для каждого получателя) заканчивается на @ in.constantcontact.com... и был обнаружен адрес для ответа».

При нажатии на ссылку доставляется вредоносный ISO-образ, содержащий ложный документ, ярлык и вредоносную DLL с загрузчиком Cobalt Strike Beacon, который Microsoft назвала NativeZone. Если ярлык запущен, DLL будет запущена, и Nobelium отключится от гонок.

«Успешное развертывание этих полезных нагрузок позволяет Nobelium обеспечивать постоянный доступ к взломанным машинам», - заявили в MTIC.

«Тогда успешное выполнение этих вредоносных полезных нагрузок может позволить NOBELIUM выполнять задачи, такие как боковое перемещение, кража данных и доставка дополнительных вредоносных программ».

MTIC добавил, что Cobalt Strike Beacons использует порт 443 для вызова инфраструктуры управления и контроля, и предоставил индикаторы списка компрометации в своем сообщении.

«Ясно, что часть стратегии Nobelium - получить доступ к проверенным поставщикам технологий и заразить их клиентов. Совмещая обновления программного обеспечения и теперь массовых поставщиков электронной почты,

Nobelium увеличивает шансы сопутствующего ущерба в шпионских операциях и подрывает доверие к технологической экосистеме, "Сказал Берт.

«Это еще один пример того, как кибератаки стали предпочтительным инструментом для растущего числа национальных государств для достижения широкого спектра политических целей, с акцентом на этих атаках Nobelium на правозащитные и гуманитарные организации».

Берт призвал к установлению правил, касающихся того, как страны работают в сети, и к ответственности за нарушения.

«Microsoft продолжит работать с готовыми правительствами и частным сектором для продвижения дела цифрового мира», - сказал он.

Nobelium был наиболее известен благодаря хакерской атаке на цепочку поставок SolarWinds, в результате которой в тысячи организаций была заложена бэкдор, прежде чем были выбраны девять федеральных агентств США и около 100 компаний США для фактического взлома и кражи информации…». ***(Chris Duckett. Microsoft warns of current Nobelium phishing campaign impersonating USAID // ZDNet (https://www.zdnet.com/article/microsoft-warns-of-current-nobelium-phishing-campaign-impersonating-usaid/). 28.05.2021).***

***

«Фирменный знак Организации Объединенных Наций (ООН) злоупотребляется в кампании, направленной на слежку за уйгурами.

В четверг Check Point Research (CPR) и команда Kaspersky GReAT заявили, что кампания, которая, вероятно, будет работой китайскоязычного злоумышленника, ориентирована на уйгуров, тюркское этническое меньшинство, проживающее в Синьцзяне, Китай.

Потенциальным жертвам рассылаются фишинговые документы с логотипом Совета ООН по правам человека (UNHRC). Этот документ под названием UgyhurApplicationList.docx содержит ложные материалы, относящиеся к обсуждениям нарушений прав человека.

Однако, если жертва разрешает редактирование при открытии файла, макрокод VBA проверяет архитектуру ПК и загружает 32- или 64-разрядные данные.

Этот файл, получивший название «OfficeUpdate.exe», представляет собой шелл-код, который извлекает и загружает удаленную полезную нагрузку, но во время анализа IP-адрес был непригоден для использования. Однако домены, связанные с вредоносным вложением электронной почты, расширили расследование до вредоносного веб-сайта, используемого для доставки вредоносных программ под видом фальшивой правозащитной организации.

Домен «Фонд тюркской культуры и наследия» (TCAHF) утверждает, что работает на «Тукрскую культуру и права человека», но копия была украдена с opensocietyfoundations.org, законной организации по защите гражданских прав.

Этот веб-сайт, ориентированный на уйгуров, ищущих финансирование, пытается соблазнить посетителей загрузить «сканер безопасности» до подачи информации, необходимой для подачи заявки на грант. Однако программное обеспечение на самом деле является бэкдором.

Сайт предлагал версию для MacOS и Windows, но только ссылка на последнюю загружала вредоносное ПО.

Были обнаружены две версии бэкдора; WebAssistant, обслуживаемый в мае 2020 года, и TcahfUpdate, загруженный с октября. Бэкдоры обеспечивают постоянство системы-жертвы, проводят кибершпионаж и кражу данных и могут использоваться для выполнения дополнительных полезных нагрузок.

Жертвы были обнаружены в Китае и Пакистане, в регионах, в основном населенных уйгурами.

CPR и Kasperksy говорят, что, хотя группа, похоже, не разделяет какую-либо инфраструктуру с другими известными группами угроз, они, скорее всего, говорят по-китайски и все еще активны, с новыми доменами, зарегистрированными в этом году на тот же IP-адрес, связанный с прошлыми атаками.

«Оба домена перенаправляют на веб-сайт государственного органа Малайзии, который называется «Исламский фонд Теренггану», - говорят исследователи. «Это говорит о том, что злоумышленники преследуют дополнительные цели в таких странах, как Малайзия и Турция, хотя они, возможно, все еще разрабатывают эти ресурсы, поскольку мы еще не видели никаких вредоносных артефактов, связанных с этими доменами». ***(Charlie Osborne. Fake human rights organization, UN branding used to target Uyghurs in ongoing cyberattacks // ZDNet (https://www.zdnet.com/article/fake-human-rights-organization-un-branding-used-to-target-uyghurs-in-ongoing-cyberattacks/). 27.05.2021).***

***

«Активная фишинговая кампания пытается заставить людей поверить в то, что они подписались на сервис потоковой передачи фильмов, чтобы заставить их позвонить по номеру телефона для отмены, где кто-то проведет их через процедуру, которая заражает их компьютер вредоносным ПО BazaLoader.

BazaLoader создает бэкдор на машинах Windows, который можно использовать в качестве исходного вектора доступа для доставки дополнительных атак вредоносных программ, включая программы- вымогатели. Пресловутый Ryuk вымогатели являются обычно доставляются через BazaLoader, что означает успешный компромисс киберпреступников может иметь крайне негативные последствия.

Последняя кампания BazaLoader основана на взаимодействии человека и сложной цепочке атак, которая снижает вероятность обнаружения вредоносного ПО.

Согласно подробному описанию исследователей кибербезопасности в Proofpoint, первый этап кампании включает в себя распространение десятков тысяч фишинговых писем, якобы исходящих от BravoMovies - поддельной службы потокового видео, созданной киберпреступниками.

Веб-сайт выглядит убедительно, и те, кто за ним стоит, даже сделали фальшивые постеры с фильмами, используя изображения с открытым исходным кодом, доступные в Интернете, хотя способ, которым веб-сайт содержит различные

орфографические ошибки, может намекать, что что-то не так, если посетитель внимательно смотрит.

В электронном письме утверждается, что жертва подписалась на пробный период, и с нее будет взиматься плата в размере 39,99 долларов в месяц, но эта предполагаемая подписка может быть отменена, если она позвонит в службу поддержки.

Если пользователь звонит по номеру, на который он подключен, представителю «службы поддержки клиентов», который утверждает, что он проведет его через процесс отказа от подписки, но на самом деле он сообщает невольной жертве, как установить BazaLoader на свой компьютер.

Они делают это, направляя вызывающего абонента на страницу «Подписка», где часть процесса побуждает их щелкнуть ссылку, по которой загружается электронная таблица Microsoft Excel. Этот документ содержит макросы, которые, если они включены, будут тайно загружать BazaLoader на машину, заражая компьютер жертвы вредоносным ПО.

Хотя это требует от злоумышленников дополнительных усилий, направление пользователей к полезной нагрузке вдали от исходного фишингового письма затрудняет обнаружение вредоносного ПО в процессе загрузки и установки.

«Вредоносные вложения часто блокируются программным обеспечением для обнаружения угроз. Поручая людям звонить в центр обработки вызовов в рамках цепочки атак, злоумышленники могут обойти механизмы обнаружения угроз, которые в противном случае пометили бы их вложения как спам», - сказал Шеррод ДеГриппо, старший директор Об исследовании и обнаружении угроз в Proofpoint сообщили ZDNet.

«Однако это значительно снижает вероятность взаимодействия жертвы с контентом и требует больше времени и усилий со стороны злоумышленников».

Но для злоумышленников может случиться так, что меньший риск обнаружения атаки в конечном итоге стоит того.

«Социальная инженерия является ключом к этой цепочке атак, и злоумышленники зависят от своих приманок социальной инженерии, чтобы побудить получателей выполнить действие, чтобы завершить цепочку атаки и получить вредоносное ПО на машине цели», - сказал ДеГриппо.

Чтобы защитить пользователей и организацию в целом от фишинговых атак и социальной инженерии, группы информационной безопасности должны обучать пользователей обнаруживать вредоносные электронные письма и сообщать о них.

Также стоит отметить, что при получении электронного письма, в котором утверждается, что с вашей кредитной карты будет снята оплата, если вы не ответите, это поразительно, но создание ощущения срочности, как будто это распространенный метод, используемый в фишинговых кампаниях, чтобы обмануть пользователя и заставить его будьте осторожны и следуйте инструкциям». ***(Danny Palmer. This phishing attack is using a call centre to trick people into installing malware on their Windows PC // ZDNet (https://www.zdnet.com/article/this-phishing-attack-is-using-a-call-centre-to-trick-people-into-installing-malware-on-their-windows-pc/). 27.05.2021).***

***

«ФБР выпустило экстренное оповещение в четверг после того, как в начале этого месяца местное правительственное учреждение подверглось атаке с использованием уязвимостей Fortinet.

В сообщении говорилось, что «группа акторов APT почти наверняка использовала устройство Fortigate для доступа к веб-серверу, на котором размещен домен муниципального правительства США».

«Скорее всего, злоумышленники создали учетную запись с именем пользователя «elie», чтобы в дальнейшем активировать вредоносную активность в сети», - говорится в сообщении с белым флэш-предупреждением.

ФБР не сообщило, какое местное правительство подверглось атаке, но последний выпуск следует за многочисленными предупреждениями о кибератаках, использующих уязвимости, связанные с Fortinet.

«По крайней мере, в мае 2021 года ФБР и CISA ранее предупреждали в апреле 2021 года, что субъекты APT получили доступ к устройствам на портах 4443, 8443 и 10443 для Fortinet FortiOS CVE-2018-13379, а также к перечисленным устройствам для FortiOS CVE-2020-12812 и FortiOS CVE-2019-5591», - сказали в ФБР.

Взламывая системы через уязвимости Fortinet, киберпреступники или государства могут «осуществлять кражу данных, шифрование данных или другие вредоносные действия». В сообщении отмечается, что из их расследований кажется, что участники атаки сосредоточены на использовании этой конкретной уязвимости, а не на атаках на конкретные цели или отрасли.

Все перечисленные уязвимости относятся к Fortinet FortiOS, операционной системе, которая является основой Fortinet Security Fabric. Компания заявила, что она была разработана для обеспечения лучшей безопасности предприятия, облачных развертываний и централизованных сетей. Но, несмотря на предупреждения, похоже, что группы APT все еще могут использовать уязвимости.

В заявлении для ZDNet Fortinet сообщила, что «CVE-2018-13379 - это старая уязвимость, устраненная в мае 2019 года», по которой компания немедленно выпустила рекомендации PSIRT. Компания заявила, что также «неоднократно общалась напрямую с клиентами и через сообщения в корпоративных блогах в августе 2019 года, июле 2020 года и снова в апреле 2021 года, настоятельно рекомендуя обновление».

«CVE-2019-5591 также была устранена в 2019 году, это более старая уязвимость, а также CVE-2020-12812, которая была устранена в июле 2020 года. Если клиенты еще не сделали этого, мы настоятельно рекомендуем им немедленно внедрить обновление и меры по устранению», - сказал он. компания добавила.

Шон Никкель, старший аналитик по киберугрозам в Digital Shadows, отметил, что всем уязвимостям, перечисленным в уведомлении, не менее одного года, подчеркивая необходимость для государственных учреждений улучшить управление исправлениями.

«Хорошо получить напоминание, потому что нацелены не только злоумышленники Fortinet. Использование принципов наименьших привилегий, выполнение регулярных обновлений и исправлений, использование сегментации

сети, использование резервных копий и усиление процессов входа в систему - все это имеет большое значение для защиты имущества», - сказал он. Никкель сказал. «Можно с уверенностью сказать, что большинство преступных групп и APT рассчитывают на то, что предприятия не очень хороши в выполнении всех этих задач, и их постоянный успех только подчеркивает этот факт». ***(Jonathan Greig. FBI issues warning about Fortinet vulnerabilities after APT group hacks local gov't office // ZDNet (https://www.zdnet.com/article/fbi-issues-warning-about-fortinet-vulnerabilities-after-apt-group-hacks-local-govt-office/). 27.05.2021).***

***

«Преступники пытались использовать беспокойство жителей Гонконга по поводу COVID, согласно новым данным безопасности, опубликованным вчера секретарем Специального административного района по инновациям и технологиям Альфредом Ситом.

Секретарь раскрыл данные в ответ на письмо в Законодательный совет от адвоката и неофициального члена Исполнительного совета Мартина Ляо.

Ляо привел данные о том, что Управление больниц Гонконга (HA) подверглось 50 миллионам кибератак в прошлом году по сравнению с 20 миллионами в 2015 году, причем HA также отразило пять атак с использованием программ-вымогателей в прошлом году. Он попросил правительство предоставить более подробную информацию о текущих тенденциях в области кибербезопасности.

Сит ответил подробным описанием инцидентов информационной безопасности, обработанных Гонконгским координационным центром группы реагирования на компьютерные чрезвычайные ситуации (HKCERT) с 2018 по 2020 год, что свидетельствует об общем снижении атак, но росте фишинга.

Число инцидентов снизилось с 10 081 в 2018 году до 9 458 в 2019 году и 8 346 в 2020 году. Число случаев фишинга увеличилось на 66 процентов (с 2018 по 2019 год) и на 35 процентов до 3483 случаев (с 2019 по 2020 год). Вредоносное ПО сократилось на 85 процентов с 1219 случаев в 2019 году до 181 случая в 2020 году.

Секретарь Сит заявил: «Мы отмечаем, что многие хакеры воспользовались общественным беспокойством по поводу эпидемии, распространяя ложную информацию с помощью методов фишинга или притворяясь медицинскими организациями, ищущими пожертвования, чтобы заманить жертв на посещение вредоносных веб-сайтов, раскрытие конфиденциальной информации или даже хищение денег».

DDoS-атаки выражались двузначными числами в течение всех трех лет, но с 2019 по 2020 год увеличились на 43%. Ситуация объясняет это «увеличением «поверхностей атаки» в результате предоставления большего количества онлайн-услуг различными секторами в течение эпидемия.»

Секретарь также раскрыла данные о киберпреступлениях, которыми занимается полиция Гонконга. Эти цифры показали, что мошенничество с электронными покупками и мошенничество с любовью принесли меньше денег на мошенничество, но в 2020 году было обнаружено больше жертв, чем в 2019 году. Денежные потери составили 2,964 млрд гонконгских долларов (382 млн долларов

США) в 2020 году из-за 12916 случаев, что на 55 процентов больше. в делах от 2019 года, которые принесли 2,907 млрд гонконгских долларов (374 млн долларов США).

В письме Ляо был задан вопрос об атаках на отрасль здравоохранения, вызывающих озабоченность после недавних отключений приложений в больницах Гонконга, и апрельских данных Всемирной организации здравоохранения (ВОЗ), в которых зафиксировано пятикратное увеличение кибератак, а также об одном инциденте с утечкой 450 активных адресов электронной почты ВОЗ и пароли онлайн.

Программы-вымогатели также вызывают озабоченность в отрасли здравоохранения, и некоторые операторы этого программного обеспечения пообещали не нацеливаться на медицинские организации во время текущей пандемии. Однако в начале этого месяца как районный совет здравоохранения Новой Зеландии Вайкато, так и национализированная служба здравоохранения Ирландии были атакованы программами-вымогателями». ***(Laura Dobberstein. Hong Kong recorded phishing surge in 2020 as scum sought to cash in on viral worries // The Register (https://www.theregister.com/2021/05/28/hong_kong_cybercrime_stats/). 28.05.2021).***

***

«Распределенные атаки типа «отказ в обслуживании» (DDoS) продолжают развиваться по сложности, частоте и масштабу. Lumen Technologies отслеживает и устраняет эти угрозы, включая семейства ботнетов Gafgyt и Mirai, и компания выпустила квартальный отчет о DDoS-атаках за первый квартал 2021 года. Это исследование дает представление о DDoS-атаках с выводами, которые подтверждают и расширяют эти тенденции.

Чтобы создать отчет, команда безопасности Lumen изучила данные подразделения Black Lotus Labs по исследованию угроз и тенденции атак, полученные с помощью платформы Lumen DDoS Mitigation Service, которая интегрирует контрмеры непосредственно в обширную глобальную сеть компании, имеющую широкие возможности.

«Поскольку зависимость организаций от приложений для получения дохода усиливается, многие понимают, что они больше не могут рисковать, отказываясь от необходимой защиты от DDoS-атак. Информация в этом отчете является еще одним подтверждением этого», - говорит Майк Бенджамин, вице-президент Lumen по безопасности и Black Lotus Labs. «По мере того, как ботнеты DDoS в Интернете вещей продолжают развиваться, Lumen фокусируется на использовании нашей видимости для выявления и уничтожения вредоносной инфраструктуры».

Ключевые результаты: Размеры атак в отчете о DDoS отражают крупнейшие атаки, очищенные глобальной инфраструктурой очистки от DDoS-атак Lumen, а не самые крупные атаки, наблюдаемые через сеть Lumen.

Ботнеты Интернета вещей:

Хорошо известные ботнеты Интернета вещей, такие как Gafgyt и Mirai, остаются серьезными угрозами DDoS: 700 активных серверов управления и контроля (C2) вместе атакуют 28000 уникальных жертв.

В первом квартале Lumen отследил около 3000 DDoS-атак C2 по всему миру. Больше всего было размещено в Сербии (1260), за ней следуют США (380) и Китай (373).

Из наиболее активных глобальных C2, которые, по наблюдениям Lumen, отдавали команды атак, больше всего у США (163), за ними следуют Нидерланды (73) и Германия (70).

Lumen отслеживал более 160000 глобальных хостов DDoS-ботнетов. Почти 42 000 человек были в Соединенных Штатах - больше, чем в любой другой стране.

Тенденции DDoS-атак

Самая большая атака Lumen, измеренная по очищенной полосе пропускания, составила 268 Гбит / с; самая большая атака, измеренная по очищенной скорости пакетов, составила 26 млн пакетов в секунду.

Самый продолжительный период DDoS-атаки, который Lumen нейтрализовал для отдельного клиента, длился почти две недели.

Многовекторные меры защиты представляют 41% всех противодействий DDoS-атакам, при этом наиболее распространенным является использование потока запросов DNS в сочетании с потоком TCP SYN.

Тремя основными отраслями, на которые нацелено 500 крупнейших атак в 1 квартале 21 г., были: финансы, программное обеспечение и технологии, а также государственные органы.

Отражатели протокола отслеживания пользовательских диаграмм (UDP)

Одним из ключевых инструментов в руках киберпреступников, стремящихся увеличить пропускную способность своих атак, являются службы отражения на основе UDP, такие как Memcached, CLDAP и DNS.

Посредством этого процесса злоумышленник подделывает исходный IP-адрес, а затем использует промежуточный сервер в качестве отражателя для отправки массивных пакетов ответа на IP-адрес жертвы, а не обратно злоумышленнику.

Black Lotus Labs использует прозрачность своей обширной глобальной сети для выявления сервисов, которые потенциально могут быть использованы для запуска этих типов атак.

Согласно данным за 1 квартал 21 г., Black Lotus Labs считает, что сегодня активно используются службы Memcached, CLDAP и DNS...» ***(Research looks at DDoS attacks passing through scrubbing centres // IoT Now (https://www.iot-now.com/2021/05/25/110240-research-looks-at-ddos-attacks-passing-through-scrubbing-centres/). 25.05.2021).***

***

«Ландшафт киберугроз, где до недавнего времени преобладали либо финансируемые государствами APT-группы, либо жаждущие наживы киберпреступники, пополнился новой, начинающей набирать обороты угрозой. По данным Cisco Talos, на киберпреступной арене появились новые игроки, так называемые приватиры.

В широком понимании приватиры (или каперы) – это частные лица, которые с разрешения верховной власти воюющего государства использовали вооруженное

судно для захвата торговых кораблей неприятеля. Как пояснили специалисты Cisco Talos, с точки зрения киберугроз приватиры являются киберпреступниками, необязательно финансируемыми государством, но так или иначе находящимися под его защитой и при этом преследующими материальную выгоду.

Приватирами преимущественно являются кибервымогательские группировки, в частности DarkSide и Lockbit, и некоторые APT, такие как Lazarus или Fancy Bear. По словам специалистов, они не подчиняются и не финансируются правительствами напрямую и действуют в своих интересах, но при этом имеют протекцию с его стороны. Эта протекция зачастую означает отсутствие преследования группировок правоохранительными органами, даже при наличии официальных запросов от властей других стран. Оказывающее протекцию государство не получает прямой выгоды от этих групп, но оно защищено от их действий, зачастую нацеленных на его геополитических противников.

Приватиры представляют собой третью категорию киберпреступных группировок после непосредственно спонсируемых правительствами APT и хакеров, работающих в интересах правительства, но необязательно получающими от них финансирование. Исследователи отметили, что это новое поколение киберпреступников также представляет собой довольно сложную группу, в которой участвуют аффилированные лица и третьи стороны». ***(На киберпреступной арене стали появляться новые игроки – приватиры // SecurityLab.ru (https://www.securitylab.ru/news/520644.php). 28.05.2021).***

***

Вірусне та інше шкідливе програмне забезпечення

«Команда кибербезопасности Mandiant, фирмы FireEye, сообщила вчера, что фишинговая кампания, прокатившаяся в декабре двумя волнами по финансовым, коммуникационным, медицинским и прочим организациям во всём мире, базировалась на трёх абсолютно новых штаммах вредоносных программ, получивших названия Doubledrag, Doubledrop и Doubleback.

Создавшая это ПО преступная группа UNC2529, по их словам, «не испытывала недостатка ни в опыте, ни в ресурсах».

Всего в глобальной схеме фишинга было задействовано более 50 доменов. В ходе успешной атаки второй волны (11-18 декабря 2020 г.) UNC2529 взломала домен, принадлежащий американской компании по оказанию услуг отопления и охлаждения, изменила его записи DNS и использовал эту структуру для запуска фишинговых атак на не менее 22 других организаций.

Электронные письма-приманки содержали ссылки на URL-адреса, ведущие к файлам.PDF вместе с файлом JavaScript в Zip-архиве. Сами документы, взятые из общедоступных источников, были нарочно испорчены, чтобы побудить жертвы в попытке их открыть дважды щелкнуть на файл.js, где находился замаскированный загрузчик Doubledrag. В некоторые письма был вложен файл Excel с макросом, несущим ту же вредоносную нагрузку.

Запущенный Doubledrag пытался загрузить так называемый дроппер, Doubledrop, — обфусцированный сценарий PowerShell, служащий для загрузки на заражённую машину бэкдора, Doubleback.

Финальный элемент трёхкомпонентный вредоносной схемы, Doubleback, был создан сразу в двух вариантах: 32- и 64-разрядном. Получив контроль, он загружал свои плагины, а затем входил в контакт с командно-управляющим (C2) сервером.

Как отмечает Mandiant, интересным моментом является то, что в файловой системе присутствует один загрузчик. Остальные компоненты сериализованы в базе данных реестра, что затрудняет их обнаружение, в особенности антивирусными движками, ориентированными на поиск файлов.

Эксперты, продолжающие изучать новое вредоносное ПО, утверждают, что оно продолжает совершенствоваться. На это, в частности, указывает встроенная функция сканирования наличия в системе антивирусных продуктов, типа Kaspersky и BitDefender — они обнаруживаются, но никаких дальнейших действий не предпринимается.

Mandiant пока не располагает сведениями о намерениях инициаторов этой фишинговой кампании, отмечая, впрочем, что «широкий охват разных отраслей и географических регионов согласуется с расчётом таргетинга, наиболее часто встречающимся среди финансово мотивированных групп». ***(Тщательно подготовленная фишинговая схема преследует пока неясные цели // Компьютерное Обозрение (https://ko.com.ua/tshhatelno_podgotovlennaya_fishingovaya_shema_presleduet_poka_neyasnye_celi_137253). 05.05.2021).***

***

«Подразделение Check Point Research представило апрельский отчет Global Threat Index о наиболее активных кибер-угрозах. По данным исследователей, в глобальных масштабах троян AgentTesla впервые поднялся на второе место в рейтинге. Лидирующую позицию сохраняет троян Dridex.

В апреле Dridex (троян, нацеленный на Windows), распространялся через вредоносную кампанию с использованием бренда QuickBooks (бухгалтерский программный комплекс). Злоумышленники пытались привлечь внимание пользователей фейковыми уведомлениями об оплате счетов. К фишинговым письмам было прикреплено вредоносное вложение Microsoft Excel – оно могло заразить систему трояном Dridex.

Dridex часто используется на начальном этапе заражения программами-вымогателями. Хакеры используют метод двойного вымогательства: они не просто шифруют данные, требуя за них выкуп, а еще и угрожают опубликовать их, если не будет оплаты. В марте команда Check Point Research сообщила, что количество атак программ-вымогателей увеличилось на 57% в начале года. Это восходящая тенденция: она достигла 107% роста по сравнению с аналогичным периодом прошлого года. В 2020 г., по оценкам, ущерб от вымогателей во всем мире составил около 20 млрд. долл. – почти на 75% выше, чем в 2019 г.

AgentTesla впервые заняла второе место в рейтинге вредоносных программ. Это продвинутый RAT (троян удаленного доступа), который заражает компьютеры

с 2014 г., выполняя функции кейлоггера и похитителя паролей. Вредоносная программа способна отслеживать и собирать вводимые данные с клавиатуры жертвы, делать скриншоты и извлекать учетные данные, относящиеся к различным программам, установленным на компьютер жертвы (включая Google Chrome, Mozilla Firefox и Microsoft Outlook). В апреле наблюдался рост кампаний AgentTesla, которые распространяются через вредоносный спам. В таких фишинговых письмах предлагается загрузить файл (может быть документ любого типа), который может вызвать заражение системы AgentTesla.

«Согласно нашей статистике, каждые 10 секунд в мире одна организация становится жертвой атак программ-вымогателей, – комментирует Александр Савушкин, региональный директор по развитию бизнеса Check Point Software Technologies в Украине, Грузии и странах СНГ. – Пока эта угроза не снижается, и организации должны рассчитывать в первую очередь на себя. Необходимо обеспечить надежную защиту от программ-вымогателей, и не забывать о регулярных тренингах для сотрудников по кибергигиене: человеческий фактор до сих пор остается самым уязвимым».

Самое активное вредоносное ПО апреля в Украине:

В апреле Trickbot стал самым популярным вредоносным ПО, атаковав 19,5% организаций в Украине. За ним следуют XMRig и Turla, затронувшие 7,5% и 5% организаций соответственно.

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

XMRig – ПО с открытым исходным кодом, впервые обнаруженное в мае 2017 г. Используется для майнинга криптовалюты Monero.

Turla – бэкдор, нацеленный на платформу Windows. Вредоносная программа может предоставить злоумышленникам возможность удаленно управлять зараженным ПК.

Наиболее распространенные уязвимости в апреле в мире:

В этом месяце «Раскрытие информации в хранилище Git на веб-сервере» стала самой эксплуатируемой уязвимостью, затрагивающей 46% организаций во всем мире. На втором и третьем месте «Удаленное выполнение кода в заголовках HTTP» и «Удаленное выполнение кода MVPower DVR» с охватом 45,5% и 44% соответственно.

Раскрытие информации в хранилище Git на веб-сервере – уязвимость в Git-репозитории, которая способствует непреднамеренному раскрытию информации учетной записи.

Удаленное выполнение кода в заголовках HTTP (CVE-2020-10826, CVE-2020-10827, CVE-2020-10828, CVE-2020-13756) – заголовки HTTP позволяют клиенту и серверу передавать дополнительную информацию с помощью HTTP-запроса. Злоумышленник может использовать уязвимый заголовок HTTP для запуска произвольного кода на устройстве жертвы.

Удаленное выполнение кода MVPower DVR – в устройствах MVPower DVR существует уязвимость удаленного выполнения кода. Злоумышленник может

использовать ее для выполнения произвольного кода в уязвимом маршрутизаторе с помощью специально созданного запроса.

Актуальные мобильные угрозы месяца:

Самым популярным вредоносным ПО для мобильных устройств стал xHelper. За ним следуют Triada и Hiddad.

xHelper – вредоносное приложение для Android, активно с марта 2019 г., используется для загрузки других вредоносных приложений и отображения рекламы. Приложение способно скрываться от пользовательских и мобильных антивирусных программ и переустанавливаться, если пользователь удаляет его.

Triada – модульный бэкдор для Android, предоставляющий права суперпользователя для загруженного вредоносного ПО.

Hiddad – модульный бэкдор для Android, который предоставляет права суперпользователя для загруженного вредоносного ПО, а также помогает внедрить его в системные процессы. Он может получить доступ к ключевым деталям безопасности, встроенным в ОС, что позволяет ему получать конфиденциальные данные пользователя». ***(Троян Dridex лидирует в апрельском рейтинге наиболее активных кибер-угроз // Компьютерное Обозрение (https://ko.com.ua/troyan_dridex_lidiruet_v_aprelskom_rejtinge_naibolee_aktivnyh_kiber-ugroz_137395). 18.05.2021).***

***

«Исследователи из компании Kaspersky, занимающейся защитой от вредоносных программ, документируют ранее неизвестный руткит Windows, который используется в наборе инструментов APT-субъекта, нацеленного в настоящее время на дипломатические учреждения в Азии и Африке.

Руткит, получивший название Moriya, дает злоумышленнику возможность перехватывать сетевой трафик и скрывать команды, отправляемые на зараженные машины, что позволяет злоумышленникам оставаться скрытыми в скомпрометированных сетях в течение нескольких месяцев.

Руткит является частью инструментария, используемого TunnelSnake, неизвестным субъектом, который развертывает бэкдоры на общедоступных серверах, принадлежащих целевым объектам. Также было обнаружено множество других инструментов, которые показывают перекрытие прикрытия с руткитом.

Касперский обнаружил руткит в сетях региональных дипломатических организаций в Азии и Африке и сообщает, что самые старые из выявленных экземпляров датируются октябрем 2019 года. Злоумышленнику удалось сохранить устойчивость в течение нескольких месяцев после первоначального развертывания вредоносного ПО, и на сегодняшний день выявлено менее 10 жертв.

В рамках атаки на дополнительную жертву в Южной Азии были развернуты различные инструменты для бокового перемещения, в том числе один, ранее связанный с APT1. Исследователи безопасности Kaspersky считают, что злоумышленники имели доступ к сети с 2018 года.

Чтобы оставаться незамеченным, руткит Moriya проверяет сетевые пакеты в режиме ядра, отбрасывает интересующие пакеты до того, как они могут быть обнаружены, и не инициирует соединение с сервером, а вместо этого ожидает

входящего трафика. Постоянство достигается за счет создания службы с именем Network Services Manager.

«Этот инструмент представляет собой пассивный бэкдор, который позволяет злоумышленникам проверять весь входящий трафик на зараженную машину, отфильтровывать пакеты, помеченные как предназначенные для вредоносного ПО, и отвечать на них. Это создает скрытый канал, по которому злоумышленники могут отправлять команды оболочки и получать обратно свои выходные данные», - объясняет Касперский.

В Moriya есть компонент пользовательского режима, отвечающий за развертывание компонента режима ядра (драйвер VirtualBox (VBoxDrv.sys) используется для обхода принудительной подписи драйвера и загрузки неподписанного драйвера), а также для поиска и чтения команд, отправленных с C&C сервера через скрытый канал связи. Руткит также может установить сеанс обратной оболочки.

Компонент драйвера руткита использует платформу фильтрации Windows (WFP) для создания скрытого канала к C&C и использует механизм фильтрации для захвата отдельного трафика, связанного с Moriya.

По словам Касперского, злоумышленники, вероятно, используют уязвимые веб-серверы в целевых организациях для первоначального доступа, после чего они развертывают другие инструменты (например, веб-оболочку China Chopper) для обнаружения сети и дальнейшей доставки полезной нагрузки. Большинство инструментов настраиваются и адаптированы для предполагаемых жертв, но вредоносное ПО с открытым исходным кодом, используемое китайскими злоумышленниками, также использовалось в атаках.

По словам Касперского, Moriya является преемником IISSpy, руткита, который наблюдался в 2018 году при атаках, не связанных с кампанией TunnelSnake. Кроме того, исследователи обнаружили связь с разработчиками вредоносного ПО ProcessKiller, которое используется для отключения антивирусных продуктов.

Хотя они не связывают атаки с конкретным противником, исследователи «Лаборатории Касперского» говорят, что за кампанией, вероятно, стоит китайскоязычный злоумышленник. Нацеливание соответствует таковому у китайских групп, и используемые инструменты также подтверждают эту гипотезу.

«Кампания TunnelSnake демонстрирует деятельность искушенного субъекта, который вкладывает значительные ресурсы в разработку набора средств уклонения и проникновение в сети крупных организаций. Используя драйверы Windows, скрытые каналы связи и несвободные вредоносные программы, группа, стоящая за этим, поддерживает значительный уровень скрытности », - заключает Касперский». ***(Ionut Arghire. Diplomatic Entities Targeted with New 'Moriya' Windows Rootkit // Wired Business Media (https://www.securityweek.com/diplomatic-entities-targeted-new-moriya-windows-rootkit). 10.05.2021).***

***

«Документы, представленные в суде с участием Apple, показали, что вредоносная программа XcodeGhost, обнаруженная в 2015 году, затронула 128 миллионов пользователей iOS.

Информация была обнаружена в электронных письмах, полученных недавно в рамках антимонопольного судебного разбирательства между Epic Games и Apple. В прошлом году производитель игр подал иск против технологического гиганта в суд Калифорнии по поводу его действий в App Store, в частности, связанных с тем, что Apple удалила популярную игру Epic, Fortnite, из App Store за якобы нарушение условий контракта.

Опубликованные электронные письма (ссылка предоставлена Ars Technica) демонстрируют обмен мнениями между сотрудниками Apple, в том числе руководителями, по поводу инцидента с XcodeGhost и шагов, которые компания должна предпринять в ответ.

XcodeGhost - это вредоносная программа, предназначенная для внедрения вредоносного кода в приложения iOS и OS X через мошеннические версии Xcode, интегрированной платформы разработки Apple для создания программного обеспечения iOS и macOS. Злоумышленники доставляли мошеннический Xcode через сторонние веб-сайты, предназначенные для китайских разработчиков.

Когда вредоносное ПО было впервые обнаружено, компании, занимающиеся кибербезопасностью, и независимые исследователи обнаружили более 4000 приложений iOS, которые были взломаны XcodeGhost. Никаких вредоносных приложений для OS X не было обнаружено.

Вредоносные приложения для iOS позволяли злоумышленникам собирать информацию о взломанных устройствах и открывать произвольные URL-адреса. Однако вредоносное ПО, похоже, не нацелено на конфиденциальную пользовательскую информацию с устройств.

В то время Apple удалила вредоносные приложения из App Store и предоставила разработчикам информацию о том, как определить, является ли используемая ими версия Xcode законной.

Электронные письма, отправленные внутри Apple после инцидента, показывают, что Apple выявила более 2500 вредоносных приложений, которые были загружены 203 миллиона раз из App Store. Технологический гигант определил, что пострадали примерно 128 миллионов клиентов.

Хотя более половины затронутых пользователей находились в Китае, Apple выявила 18 миллионов клиентов в Соединенных Штатах, которые также пострадали. Компания обсуждала, следует ли напрямую уведомлять всех 128 миллионов затронутых пользователей, но, похоже, в конечном итоге решила не делать этого…

ОБНОВЛЕНИЕ: Apple заявила, что постоянно информирует своих пользователей о проблеме и предоставляет им информацию о шагах, которые они могут предпринять, но не сообщила, уведомила ли она их напрямую.

Компания также заявила, что в то время работала с разработчиками, помогая им публиковать чистые версии своих приложений и предлагать обновленные версии клиентам». ***(Eduard Kovacs. XcodeGhost Malware Discovered in 2015 Impacted 128 Million iOS Users // Wired Business Media***

(https://www.securityweek.com/xcodeghost-malware-discovered-2015-impacted-128-million-ios-users). 11.05.2021).

***

«Обнаружен новый вариант загрузчика вредоносных программ Buer, написанный на Rust. Исходная версия написана на C. Rust эффективен, прост в использовании и становится все более популярным языком программирования - его использует Microsoft и присоединилась к Rust Foundation в феврале 2021 года.

Исследователи из Proofpoint идентифицировали новый вариант в начале апреля 2021 года и назвали его RustyBuer. Как и Buer, он работает как загрузчик для распространения других вредоносных программ на скомпрометированные системы. Наиболее вероятной причиной разработки варианта Rust является уклонение от обнаружения вредоносных программ, основанных на особенностях вредоносного ПО, написанного на C.

В связанных кампаниях, обнаруженных Proofpoint, вредоносное ПО распространяется с помощью фишинговых писем DHL и используется для доставки вредоносных документов Word или Excel.

В одном примере во вложение Excel было встроено RustyBuer в виде макроса. В документе было показано несколько логотипов охранных фирм, предположительно в попытке повысить легитимность. Макрос использовал обход приложений (DLL оболочки Windows через LOLBAS), чтобы избежать обнаружения механизмами безопасности конечных точек.

Если документ просматривается, RustyBuer удаляется и сохраняется постоянство с помощью файла LNK, который запускается при запуске. Исследователи Proofpoint видели, что загрузчик доставлял Cobalt Strike Beacon в качестве полезной нагрузки второй ступени, но не все образцы содержали полезную нагрузку второй ступени. В последнем случае, говорят исследователи, «эти злоумышленники могут пытаться установить первоначальный доступ в среде жертв, чтобы затем продать свой доступ другим злоумышленникам на подпольных рынках».

RustyBuer пытается избежать анализа, проверяя наличие виртуальных машин. Он также имеет ограниченную географическую проверку, чтобы избежать работы в определенных странах - в основном, по-видимому, в странах, входящих в Содружество Независимых Государств (СНГ). Это может быть признаком того, что разработчики имеют некоторую связь с Россией, где власти, похоже, довольно спокойно относятся к хакерам, которые не атакуют цели в России.

Связь с серверами C2 практически идентична той, которая используется в последней версии языкового варианта C. Функции обрабатываются через запросы HTTP (S) POST. Первоначальный запрос POST будет отправлен с данными POST, разделенными символами «&» и «=». Параметры запроса зашифрованы и могут быть дешифрованы с помощью декодирования Base64, шестнадцатеричного декодирования и дешифрования RC4. Он содержит основную информацию о взломанном компьютере.

Ответный маяк может быть декодирован аналогичным образом. Как и в исходном варианте Buer, он содержит различные варианты загрузки и выполнения

полезной нагрузки. Сочетание доступа Buer / RustyBuer как услуги с вредоносным ПО как услуга означает, что преступники с небольшим техническим опытом теперь могут доставлять сложные вредоносные программы, в том числе программы-вымогатели, по своему выбору.

Комментируя выводы Proofpoint, технический директор и соучредитель Blue Hexagon Саумитра Дас сказал: «Вредоносные программы на основе Rust набирают популярность в последние несколько лет. Это становится все более распространенным, поскольку злоумышленники пытаются уклониться от улучшенных систем обнаружения». Он добавил: «Уже существуют реализации с открытым исходным кодом образцов вредоносных программ-вымогателей», приведя пример Rust-Ransomware на GitHub.

Proofpoint предполагает, что появление RustyBuer демонстрирует, что злоумышленники продолжают развивать свои вредоносные программы, пытаясь избежать обнаружения, и, следовательно, «цепочка атак может быть более эффективной в получении доступа и устойчивости». В нем добавлено: «RustyBuer и оригинальный загрузчик Buer были замечены как загрузчики первой ступени для дополнительных полезных нагрузок, включая Cobalt Strike и несколько штаммов вымогателей, а также, возможно, обеспечивающие доступ жертвы к другим злоумышленникам на подпольном рынке.

Ключевой вывод для защитников заключается в том, что старые вредоносные программы, скомпилированные на новом или другом языке, будут фактически необнаруживаемыми вредоносными программами нулевого дня для систем обнаружения на основе сигнатур до тех пор, пока поставщики не найдут и не проанализируют вредоносное ПО и не добавят новую сигнатуру в свой механизм обнаружения.

На прошлой неделе Proofpoint согласилась быть приобретена частной инвестиционной компанией Thoma Bravo в рамках сделки за наличные на сумму примерно 12,3 миллиарда долларов». ***(Kevin Townsend. New Variant of Buer Malware Loader Written in Rust to Evade Detection // Wired Business Media (https://www.securityweek.com/new-variant-buer-malware-loader-written-rust-evade-detection). 04.05.2021).***

***

«Новое исследование показывает, как Cobalt Strike используется в кампаниях по развертыванию вредоносных программ, начиная от банковского трояна Trickbot и заканчивая Bazar.

В среду Intel 471 опубликовала отчет о злоупотреблении Cobalt Strike, коммерческим инструментом тестирования на проникновение, выпущенным в 2012 году, который можно использовать для развертывания маяков в системах для имитации атак и тестирования сетевой защиты.

В январе аналитики безопасности заявили, что Cobalt Strike, наряду с фреймворком Metasploit, использовался для размещения более 25% всех вредоносных серверов управления и контроля (C2), развернутых в 2020 году.

Популярный комплект для тестирования на проникновение, исходный код которого для версии 4.0 якобы просочился в сеть в 2020 году, в течение многих лет

использовался злоумышленниками и стал незаменимым инструментом для групп продвинутых постоянных угроз (APT), включая Carbanak и Cozy Bear.

По данным Fox-IT, были зарегистрированы тысячи случаев злоупотребления Cobalt Strike, но большинство злоумышленников будут использовать устаревшие, пиратские или взломанные копии программного обеспечения.

«Cobalt Strike стал очень распространенной полезной нагрузкой второго уровня для многих вредоносных кампаний из многих семейств вредоносных программ», - отмечает Intel 471. «Доступ к этому мощному и очень гибкому инструменту был ограничен разработчиками продукта, но просочившиеся версии уже давно распространились по Интернету».

Исследователи говорят, что существующее злоупотребление Cobalt Strike было связано с кампаниями, варьирующимися от развертывания программ-вымогателей до наблюдения и кражи данных, но, поскольку инструмент позволяет пользователям создавать гибкие архитектуры C2, может быть сложно отследить владельцев C2.

Однако команда провела расследование использования Cobalt Strike в постэксплуатационных мероприятиях.

В качестве отправной точки был выбран Trickbot. Операторы банковских троянцев Trickbot сбросили Cobalt Strike в ходе атак, начиная с 2019 года, наряду с Meterpreter и PowerShell Empire, а также в атаках, отслеживаемых Walmart Global Tech и SentinelLabs.

Группа Hancitor (MAN1 / Moskalvzapoe / TA511) также начала использовать Cobalt Strike. Как отмечает Palo Alto Networks, недавнее заражение, связанное с развертыванием троянца Gozi и программы для похищения информации Evil Pony, показало, что эти инструменты были заменены на Cobalt Strike. Во время действий после эксплойтов Hancitor затем развернет троян удаленного доступа (RAT), программы для кражи информации или, в некоторых случаях, вредоносное ПО-спам-бота.

«Группа, устанавливающая серверы команды Cobalt Strike, связанные с Hancitor, предпочитает размещать свои маяки CS на хостах без домена», - сообщает Intel 471. «Маяки CS будут звонить домой к одному и тому же набору IP-адресов. Стадеры загружаются из инфраструктуры, настроенной через пуленепробиваемый хостинг Yalishanda. Важно отметить, что Hancitor запускает Cobalt Strike только на машинах, подключенных к домену Windows. Когда это условие не выполняется, Hancitor может отказаться от SendSafe (спам-бота), Onliner IMAP checker или Ficker information stealer».

Исследователи также изучают использование Cobalt Strike злоумышленниками, распространяющими банковского трояна Qbot / Qakbot, один из плагинов которого - plugin_cobalt_power3 - включает инструмент проверки пера.

«Конфигурация, извлеченная из связанного с Qbot маяка Cobalt Strike, не показывает никаких ссылок на какие-либо другие известные нам группы», - говорится в отчете. «При сравнении этой активности с образцами, о которых сообщают другие исследователи, мы наблюдали различные используемые общедоступные профили Malleable-C2, но общие черты в инфраструктуре хостинга».

Операторы вариантов вредоносного ПО SystemBC, как сообщает Proofpoint, используют прокси-серверы SOCKS5 для маскировки сетевого трафика и были включены в качестве полезной нагрузки как в наборы эксплойтов RIG, так и Fallout. Согласно Intel 471, операторы программ-вымогателей также внедрили SystemBC, которая отбрасывала Cobalt Strike во время кампаний в 2020 году и в начале 2021 года. Однако команда не приписывает эти недавние кампании конкретным известным злоумышленникам.

Также следует отметить, что в начале 2021 года кампании Bazar были зарегистрированы как отправка и распространение Cobalt Strike, а не типичные загрузчики Bazar, используемые злоумышленниками в прошлом.

«Cobalt Strike - мощный инструмент, который используют люди, которым вообще не следует использовать его: растущее число киберпреступников», - говорят исследователи. «Тем не менее, не все развертывания Cobalt Strike одинаковы. Некоторые развертывания демонстрируют плохую операционную безопасность за счет повторного использования инфраструктуры и без изменения своих гибких профилей C2. Кроме того, некоторые операторы сбрасывают Cobalt Strike на многих зараженных системах, в то время как другие будут только использовать инструмент очень избирательно». ***(Charlie Osborne. This is how the Cobalt Strike penetration testing tool is being abused by cybercriminals // ZDNet (https://www.zdnet.com/article/this-is-how-the-cobalt-strike-penetration-testing-tool-is-being-abused-by-cybercriminals/). 19.05.2021).***

***

«Недавно разработанный ботнет под названием «Simps» вышел из киберподполья для проведения распределенных атак типа «отказ в обслуживании» (DDoS) на игровые объекты и другие объекты с использованием узлов Интернета вещей (IoT). По словам исследователей, это часть набора инструментов, используемого киберпреступной группой Keksec.

По данным группы исследования угроз Uptycs, ботнет Gafgyt впервые увидел Simps в апреле на устройствах IoT. Gafgyt (он же Bashlite) - ботнет на базе Linux, впервые обнаруженный в 2014 году. Он нацелен на уязвимые устройства Интернета вещей, такие как маршрутизаторы Huawei, маршрутизаторы Realtek и устройства ASUS, которые затем использует для запуска крупномасштабных DDoS-атак и загрузки полезных данных следующего этапа на зараженные машины. Она недавно добавила новые эксплойты для первоначального компромисса для Huawei, Realtek и Dasan GPON устройств.

В текущей кампании Gafgyt заражает конечные точки Realtek (CVE-2014-8361) и Linksys, а затем загружает Simps. Сам Simps затем использует модули Mirai и Gafgyt для DDoS-атак, согласно анализу, опубликованному в среду.

Другой вариант атаки использует сценарии оболочки для загрузки Simps.

YouTube, Discord Simps Обсуждения

Сценарий оболочки и Gafgyt могут развертывать различные полезные нагрузки Simps следующего уровня для нескольких архитектур на базе Linux, отмечают исследователи, с помощью утилиты Wget. Wget - это законный

программный пакет для получения файлов с веб-серверов с использованием HTTP, HTTPS, FTP и FTPSa.

После выполнения двоичного файла Simps он удаляет файл журнала, в котором записывается факт заражения целевого устройства, и подключается к командному серверу (C2).

Журналы заражений имеют общие черты, что позволило исследователям искать ссылки на них в более широкой сети. Это привело к открытию, что автор Simps поддерживает канал YouTube, чтобы предлагать демонстрации функциональности ботнета, и сервер Discord для обсуждения вредоносного ПО.

«Ботнет может находиться на ранних стадиях разработки из-за наличия файла журнала после выполнения», - заявили исследователи, отметив, что оставлять такой легко обнаруживаемый артефакт - не лучшая практика для тех, кто пытается оставаться незамеченными.

В любом случае они идентифицировали видео YouTube, созданное пользователем с именем «itz UR0A», под названием «Simps Botnet□, Slamming !!!» - от 24 апреля.

Ссылка на YouTube также содержала ссылку на сервер Discord для «UR0A», которая, как показал анализ, также присутствовала в журнале заражений.

«На сервере Discord было несколько обсуждений DDoS-атак и бот-сетей с разными именами», - отмечают исследователи. «Один двоичный файл с именем gay.x86, который мы идентифицировали в чате, отображал сообщение, что «система заложена md5hashguy».

Атрибуция кексеку

Благодаря определенным сообщениям сервера Discord, Uptycs приписал активность группе Keksec (также известной как Kek Security), которая представляет собой обширную группу угроз, известную тем, что использует уязвимости для вторжения в несколько архитектур с помощью полиморфных инструментов (они могут включать полезные нагрузки Linux и Windows, а также пользовательский Python, вредоносное ПО).

Он постоянно пополняет свой арсенал; В январе было замечено развертывание вредоносного ПО для ботнета FreakOut Linux, которое выполняет сканирование портов, сбор информации, анализ пакетов данных и сетей, а также DDoS и криптомайнинг.

«Группа активно создает ботнеты IRC для целей DDoS-операций и кампаний криптоджекинга с использованием как Doge, так и Monero», - говорится в недавнем анализе группы Lacework.

В качестве доказательства атрибуции Simps Uptycs обнаружил, что одно из сообщений Discord содержало образец вредоносной программы Gafgyt, который содержал сообщение «Infected By Simps Botnet;)».

«Эта вредоносная программа сбросила файл с именем keksec.infected.you.log, в котором содержалось сообщение «вы были заражены urmommy, спасибо, что присоединились к keksec».

Кроме того, Gafgyt является одним из самых популярных инструментов Keksec, согласно прошлому анализу, и группа известна тем, что смешивает свой код с другими двоичными файлами для создания вредоносного ПО Franken.

Например, Keksec также управляет HybridMQ-keksec, ботнетом, созданным путем объединения и модификации исходного кода Mirai и Gafgyt, отмечает Uptycs.

В случае Simps двоичные файлы, в частности, содержат модули для запуска DDoS-атак на игровые платформы, такие как Valve Source Engine и OVH. Это также было замечено в варианте Gafgyt, используемом Keksec, который нацелился на маршрутизаторы Huawei и Asus и убил его конкурирующие ботнеты IoT.

Как предприятия могут защитить себя от ботнетов

Uptycs рекомендовал корпоративным пользователям и администраторам несколько мер по выявлению и защите от атак ботнетов:

Регулярно отслеживайте подозрительные процессы, события и сетевой трафик, возникающие при выполнении любых ненадежных двоичных файлов / скриптов.

Всегда будьте осторожны при выполнении сценариев оболочки из неизвестных или ненадежных источников.

Обновляйте системы и микропрограммное обеспечение с помощью последних выпусков и исправлений». ***(Tara Seals. Keksec Cybergang Debuts Simps Botnet for Gaming DDoS // Threatpost (https://threatpost.com/keksec-simps-botnet-gaming-ddos/166306/). 19.05.2021).***

***

«Печально известная банда киберпреступников FIN7, финансово мотивированная группа, распространяет бэкдор под названием Lizar под видом инструмента проверки на проникновение Windows для этичных хакеров.

По данным группы исследования киберугроз BI.ZONE, FIN7 выдает себя за законную организацию, предлагающую инструменты анализа безопасности. По словам исследователей, они делают все возможное для правдоподобия: «Эти группы нанимают сотрудников, которые даже не подозревают, что они работают с настоящим вредоносным ПО или что их работодатель является настоящей преступной группировкой».

С 2015 года FIN7 нацелена на системы точек продаж в ресторанах, казино и отелях с непринужденной атмосферой. Группа обычно использует фишинговые атаки с использованием вредоносных программ против жертв в надежде, что они смогут проникнуть в системы, чтобы украсть данные банковских карт и продать их. Исследователи отметили, что с 2020 года он также добавил в свой набор атак с использованием программ-вымогателей и кражи данных, тщательно отбирая цели в соответствии с доходом с помощью службы ZoomInfo.

Выбор вредоносных программ постоянно меняется, в том числе время от времени используются ранее неизвестные образцы, что удивляет исследователей. Но его основным инструментарием был троян удаленного доступа Carbanak (RAT), который, как показал предыдущий анализ, очень сложен и изощрен по сравнению с аналогами: это, по сути, Cadillac в море тележек для гольфа. Карбанак обычно используется для разведки и установления точки опоры в сетях.

Однако в последнее время исследователи BI.ZONE заметили, что группа использует новый тип бэкдора под названием Lizar. Последняя версия используется

с февраля и предлагает мощный набор функций поиска данных и бокового перемещения, согласно анализу, опубликованному в четверг.

«Lizar - это разнообразный и сложный инструментарий», - заявляют в компании. «В настоящее время он все еще находится в стадии активной разработки и тестирования, но уже широко используется для контроля зараженных компьютеров, в основном по всей территории Соединенных Штатов».

К настоящему времени жертвами стали нападения на игорное заведение, несколько учебных заведений и фармацевтические компании в США, а также на ИТ-компанию со штаб-квартирой в Германии и финансовое учреждение в Панаме.

Внутри Lizar Toolkit от FIN7

По словам исследователей, инструментарий Lizar структурно похож на Carbanak. Он состоит из загрузчика и различных плагинов, которые используются для разных задач. Вместе они работают в зараженной системе и могут быть объединены в бот-клиент Lizar, который, в свою очередь, обменивается данными с удаленным сервером.

«Модульная архитектура бота делает инструмент масштабируемым и позволяет независимо разрабатывать все компоненты», - говорится в анализе. «Мы обнаружили три вида ботов: DLL, EXE и сценарии PowerShell, которые выполняют DLL в адресном пространстве процесса PowerShell».

Плагины отправляются с сервера на загрузчик и выполняются, когда в клиентском приложении Lizar выполняется определенное действие, согласно BI.ZONE.

Шесть этапов жизненного цикла плагинов следующие:

Пользователь выбирает команду в интерфейсе клиентского приложения Lizar;

Сервер Lizar получает информацию о выбранной команде;

Сервер находит подходящий плагин в каталоге плагинов, затем отправляет его загрузчику;

Загрузчик запускает плагин и сохраняет результат выполнения плагина в специально выделенной области памяти в куче;

Сервер получает результаты выполнения плагина и отправляет их клиенту; а также

Клиентское приложение отображает результаты плагина.

Плагины по-разному разработаны для загрузки других инструментов, таких как Mimikatz или Carbanak, получения информации с машины жертвы, создания снимков экрана, сбора учетных данных, получения истории браузера и многого другого.

Конкретные команды бота следующие:

Командная строка - получить CMD на зараженной системе;

Executer - запустить дополнительный модуль;

Grabber - запустить один из плагинов, собирающих пароли в браузерах, протоколе удаленного рабочего стола и ОС Windows;

Информация - получить информацию о системе;

Перейти - перенести загрузчик в другой процесс;

Убить - остановить плагин;

Список процессов - получить список процессов;

Mimikatz - запустить Mimikatz;

Сетевой анализ - запустите один из плагинов для получения информации Active Directory и сети;

Новый сеанс - создать еще один сеанс загрузчика (запустить копию загрузчика на зараженной системе);

Крыса - беги Карбанак; а также

Снимок экрана - сделать снимок экрана.

Между тем, по словам исследователей, серверное приложение Lizar написано с использованием платформы.NET и работает на удаленном хосте Linux. Он поддерживает шифрованную связь с бот-клиентом.

«Перед отправкой на сервер данные шифруются с помощью сеансового ключа длиной от 5 до 15 байт, а затем ключа, указанного в конфигурации (31 байт)», - пояснили исследователи. «Если ключ, указанный в конфигурации (31 байт), не соответствует ключу на сервере, данные с сервера не отправляются».

Киберпреступники выдают себя за исследователей безопасности

Впечатляюще ироничная тактика выдавать себя за службу безопасности, одновременно усиливая небезопасность, не нова даже для FIN7. В прошлом BI.ZONE заметила, что она продвигает Carbanak под видом пакета, являющегося инструментом от приверженцев кибербезопасности Check Point Software или Forcepoint.

Ранее в этом году северокорейская группа продвинутых постоянных угроз (APT) под названием Zinc, которая связана с более печально известным APT Lazarus, организовала две отдельные атаки, нацеленные на исследователей безопасности.

В январе группа использовала тщательно продуманные меры социальной инженерии через Twitter и LinkedIn, а также другие медиа-платформы, такие как Discord и Telegram, чтобы установить доверительные отношения с исследователями, представившись законными исследователями, заинтересованными в наступательной безопасности.

В частности, злоумышленники инициировали контакт, спросив исследователей, хотят ли они совместно исследовать уязвимости. Они продемонстрировали свою надежность, разместив видеоролики с эксплойтами, над которыми они работали, в том числе имитируя успех рабочего эксплойта для существующей исправленной уязвимости Защитника Windows, которая использовалась в рамках масштабной атаки SolarWinds.

В конце концов, после долгой переписки злоумышленники предоставили целевым исследователям проект Visual Studio, зараженный вредоносным кодом, который мог установить бэкдор в их систему. Жертвы также могли заразиться, перейдя по вредоносной ссылке в Twitter.

По данным Google TAG, исследователи безопасности, зараженные этими атаками, использовали полностью исправленные и обновленные версии браузера Windows 10 и Chrome, что свидетельствовало о том, что хакеры, вероятно, использовали уязвимости нулевого дня в своей кампании.

Цинк вернулся к этому в апреле, использовав ту же тактику в социальных сетях, но добавив профили в Twitter и LinkedIn для поддельной компании под названием «SecuriElite», которая якобы была атакующей охранной фирмой, расположенной в Турции. Компания заявила, что предлагает тесты на проникновение, оценку безопасности программного обеспечения и эксплойты, и намеревалась активно нанимать персонал по кибербезопасности через LinkedIn». ***(Tara Seals. FIN7 Backdoor Masquerades as Ethical Hacking Tool // Threatpost (https://threatpost.com/fin7-backdoor-ethical-hacking-tool/166194/). 14.05.2021).***

***

«Официальный репозиторий программных пакетов Python, PyPI, наводняется пакетами спама…

Эти пакеты названы в честь различных фильмов в стиле, который обычно ассоциируется с торрентами и «варезными» сайтами, на которых размещен пиратский контент.

Каждый из этих пакетов публикуется уникальной псевдонимной учетной записью сопровождающего, что затрудняет одновременное удаление пакетов и учетных записей спама для PyPI.

PyPI наводнен спам-пакетами

PyPI наводнен спам-пакетами, названными в честь популярных фильмов в стиле, который обычно ассоциируется с торрент-сайтами или сайтами «варез», которые предоставляют пиратские загрузки: watch- (название-фильма) -2021-full-online-movie-free-hd-...

Открытие стало известно, когда Адам Бош, старший инженер-программист в Sonatype, проводил аудит набора данных и заметил забавно звучащий компонент PyPI, названный в честь популярного телесериала.

«Я просматривал набор данных и заметил ' wandavision ', что немного странно для названия пакета».

«Присмотревшись, я нашел этот пакет и посмотрел на PyPI, потому что не поверил ему», - сказал Беш в интервью BleepingComputer.

Хотя некоторым из этих пакетов несколько недель, BleepingComputer заметил, что спамеры продолжают добавлять новые пакеты в PyPI совсем недавно, всего час назад.

Подсчет результатов поиска «10 000+» может быть неточным, поскольку мы наблюдали, что фактическое количество спам-пакетов, отображаемых в репозитории PyPI, было намного меньше.

Веб-страница этих поддельных пакетов содержит ключевые слова для спама и ссылки на сайты потоковой передачи фильмов, хотя их законность и законность сомнительна...

…каждый из этих пакетов был опубликован отдельным автором (сопровождающим) аккаунтом с использованием псевдонима, что, вероятно, затруднило администраторам PyPI удаление этих пакетов.

Как сообщает ZDNet, в феврале этого года PyPI был наводнен поддельными кейгенами «Discord», «Google» и «Roblox» в результате масштабной спам-атаки.

В то время Ева Йодловска, исполнительный директор Python Software Foundation, сообщила ZDNet, что администраторы PyPI работают над предотвращением спам-атаки, однако по природе pypi.org любой может публиковать в репозитории, и такие случаи были общий.

Пакеты содержат код из легитимных компонентов PyPI

Помимо ключевых слов для спама и ссылок на сайты квази-потокового видео, эти пакеты содержат файлы с функциональным кодом и информацией об авторе, взятые из законных пакетов PyPI.

…спам-пакет «смотреть-армия-мертвых-2021-полный онлайн-фильм-бесплатно-hd-качество» содержал информацию об авторе и некоторый код из законного пакета PyPI, jedi- язык-сервер».

…злоумышленники объединили код из легитимных пакетов с поддельными или вредоносными пакетами, чтобы замаскировать свои шаги и сделать обнаружение этих пакетов немного более сложным.

«Это не редкость в других экосистемах, таких как npm, где у вас есть миллионы пакетов. Такие пакеты, к счастью, довольно легко обнаружить и избежать».

«Всегда полезно изучить пакет перед его использованием. Если что-то кажется неправильным, для этого есть причина», - улыбнулся Бош.

В последние месяцы участились атаки на экосистемы с открытым исходным кодом, такие как npm, RubyGems и PyPI.

Злоумышленники были уличены в наводнении репозиториев программного обеспечения вредоносными программами, подражателями путаницы вредоносных зависимостей или просто пакетами линчевателей для распространения своего сообщения.

Таким образом, обеспечение безопасности этих репозиториев превратилось в гонку между участниками угроз и разработчиками репозиториев…». ***(Ax Sharma. Spammers flood PyPI with pirated movie links and bogus packages // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/spammers-flood-pypi-with-pirated-movie-links-and-bogus-packages/). 20.05.2021).***

***

«Исследователи обнаружили четыре новых семейства вредоносных программ, предназначенных для устройств Pulse Secure VPN.

Решения Pulse Secure для виртуальной частной сети (VPN) и Secure Connect (PSC) используются корпорациями по всему миру для обеспечения безопасного доступа к бизнес-системам. Однако 20 апреля группа кибер-криминалистов FireEye Mandiant раскрыла атаки на оборонные, правительственные и финансовые организации с использованием уязвимостей в программном обеспечении.

Основная уязвимость под руку, является CVE-2021-22893, выдается CVSS тяжесть 10 баллов, описанные в качестве аутентификации перепускной воздействуя Импульсного соединения Secure позволяет неаутентифицированным атакующие выполнить удаленное выполнение произвольного кода (PC).

К другим недостаткам безопасности, связанным с атаками, относятся CVE-2019-11510, CVE-2020-8260 и CVE-2020-8243, которые можно использовать для обеспечения устойчивости уязвимого устройства и дальнейшего взлома устройств.

Mandiant подозревает, что китайские злоумышленники используют уязвимости, и теперь вторжения были обнаружены в оборонных, правительственных, технологических, транспортных и финансовых организациях в Соединенных Штатах и Европе.

По словам исследователей, UNC2630 и UNC2717 являются основными группами повышенной постоянной угрозы (APT), участвующими в этих атаках, и обе они «поддерживают ключевые приоритеты правительства Китая».

«Многие скомпрометированные организации работают в вертикалях и отраслях, соответствующих стратегическим целям Пекина, изложенным в недавнем 14-м пятилетнем плане Китая», - сообщает Mandiant. «Несмотря на то, что есть свидетельства кражи данных во многих организациях, мы напрямую не наблюдали инсценировку или кражу каких-либо данных китайскими шпионами, которые могли бы рассматриваться как нарушение соглашения между Обамой и Си».

В первоначальном отчете Mandiant было обнаружено 12 отдельных семейств вредоносных программ и инструментов, включая веб-оболочки Atrium и Slightpulse, которые использовали уязвимости Pulse Secure в качестве оружия.

Сейчас это число достигло 16 с открытием четырех новых семейств вредоносных программ, связанных с UNC2630:

Bloodmine: эта утилита анализирует файлы журнала PSC и извлекает информацию, относящуюся к логинам, идентификаторам сообщений и веб-запросам.

Банк крови: эта вредоносная программа предназначена для кражи учетных данных и анализирует файлы, содержащие хэши паролей или учетные данные в виде открытого текста.

Cleanpulse: Cleanpulse - это инструмент исправления памяти для предотвращения определенных событий журнала. Mandiant обнаружил это вредоносное ПО «в непосредственной близости» от веб-оболочки Atrium.

Rapidpulse: это веб-оболочка, которая существует как модификация законного файла Pulse Secure и не только способна читать произвольные файлы, но также может выступать в качестве загрузчика зашифрованных файлов.

Mandiant отмечает, что в некоторых случаях вторжения китайские злоумышленники удаляли ряд бэкдоров, но оставляли постоянные патчеры потенциально в качестве средства восстановления доступа в будущем, демонстрируя необычную «заботу об оперативной безопасности и чувствительности к публичности».

«Китайская кибершпионаж продемонстрировала более высокую терпимость к риску и в меньшей степени сдерживается дипломатическим давлением, чем это было охарактеризовано ранее», - добавил Mandiant.

Ivanti, материнская компания Pulse Secure, выпустила исправления и инструмент обеспечения целостности, позволяющий пользователям проверять свои сборки на предмет риска. Рекомендуется применить исправления как можно скорее.

Агентство по кибербезопасности и безопасности инфраструктуры США (CISA) впервые опубликовало предупреждение об использовании продуктов Pulse Connect Secure 21 апреля и с тех пор обновило свои рекомендации.

В других предупреждениях на этой неделе ФБР предупреждало о продолжающихся атаках с использованием уязвимостей Fortinet / FortiOS (CVE-2018-13379, CVE-2020-12812, FortiOS CVE-2019-5591). В мае группе APT удалось использовать эти ошибки для доступа к веб-серверу, на котором размещен домен муниципального правительства США». ***(Charlie Osborne. Researchers find four new malware tools created to exploit Pulse Secure VPN appliances // ZDNet (https://www.zdnet.com/article/researchers-find-four-new-malware-tools-created-to-exploit-pulse-secure-vpn-appliances/). 28.05.2021).***

***

«Китайские группы угроз продолжают развертывать новые вредоносные программы в скомпрометированных сетях десятков организаций США и ЕС после эксплуатации уязвимых устройств Pulse Secure VPN.

Как сообщили в прошлом месяце аналитики угроз FireEye, спонсируемые государством злоумышленники использовали недавно исправленный нулевой день в шлюзах Pulse Connect Secure.

После компрометации целевых устройств они развернули вредоносное ПО для обеспечения длительного доступа к сетям, сбора учетных данных и кражи конфиденциальных данных.

«Теперь мы оцениваем, что шпионская деятельность UNC2630 и UNC2717 поддерживает ключевые приоритеты китайского правительства», - говорится в сообщении FireEye, опубликованном в четверг.

«Многие скомпрометированные организации работают в вертикалях и отраслях, соответствующих стратегическим целям Пекина, изложенным в недавнем 14-м пятилетнем плане Китая».

Новое вредоносное ПО, развернутое в сетях организаций США и ЕС

В предыдущем отчете FireEye упомянула 12 семейств вредоносных программ, которые были обнаружены и специально разработаны для заражения устройств Pulse Secure VPN.

По мнению аналитиков FireEye, вредоносное ПО, которое китайские кибершпионы использовали до выпуска первого отчета, включает:

UNC2630 нацелена на компании DIB США с помощью SLOWPULSE, RADIALPULSE, THINBLOOD, ATRIUM, PACEMAKER, SLIGHTPULSE и PULSECHECK с августа 2020 года по март 2021 года.

UNC2717 нацелена на глобальные правительственные учреждения в период с октября 2020 года по март 2021 года с использованием HARDPULSE, QUIETPULSE и PULSEJUMP.

С тех пор FireEye обнаружила, что китайские злоумышленники UNC2630 установили еще четыре штамма вредоносных программ, в результате чего общее количество вредоносных программ составило 16 семейств, специально предназначенных для взлома устройств Pulse Secure VPN.

FireEye все еще собирает доказательства и реагирует на новые инциденты, связанные с взломом устройства Pulse Secure VPN, в организациях США и Европы в нескольких вертикалях, включая оборону, правительство, высокие технологии, транспорт и финансовый сектор.

«Цели китайских операций кибершпионажа часто выбираются исходя из их соответствия национальным стратегическим целям, и существует сильная корреляция между основными отраслями, перечисленными в официальных официальных документах, и целями китайской кибершпионажа», - заявили аналитики угроз.

Признаки того, что злоумышленники убирают следы

В ходе расследования этих атак FireEye также обнаружила доказательства того, что злоумышленники отслеживали исследования компании.

Как выяснили аналитики, до первого отчета FireEye по UNC2630 и UNC2717 злоумышленники начали удалять свои вредоносные программы из некоторых скомпрометированных систем.

«В период с 17 по 20 апреля 2021 года специалисты по реагированию на инциденты Mandiant наблюдали, как UNC2630 получает доступ к десяткам взломанных устройств и удаляет веб-оболочки, такие как ATRIUM и SLIGHTPULSE», - заявили исследователи.

«Для китайских шпионов необычно удалять большое количество бэкдоров в нескольких средах жертв во время публичного раскрытия информации или примерно в это время. Это действие демонстрирует интересную озабоченность по поводу операционной безопасности и чувствительность к публичности».

«И UNC2630, и UNC2717 демонстрируют продвинутую торговлю и делают впечатляющие меры, чтобы избежать обнаружения. Актеры изменяют временные метки файлов и регулярно редактируют или удаляют судебные доказательства, такие как журналы, дампы ядра веб-сервера и файлы, подготовленные для эксфильтрации».

CISA также обновила предупреждение об использовании уязвимостей Pulse Connect Secure, включив в него новые методы, тактики и процедуры (TTP) и индикаторы взлома (IOC), обнаруженные FireEye.

Федеральное агентство США также обновило меры по смягчению последствий и призывает организации, которые обнаруживают доказательства эксплуатации в своих сетях, проверить руководство, опубликованное Ivanti, материнской компанией Pulse Secure». ***(Sergiu Gatlan. Chinese cyberspies are targeting US, EU orgs with new malware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/chinese-cyberspies-are-targeting-us-eu-orgs-with-new-malware/). 28.05.2021).***

***

Програми-вимагачі

«Программы-вымогатели - одна из самых серьезных проблем безопасности в Интернете и одна из самых серьезных форм

киберпреступлений, с которыми сегодня сталкиваются организации. Программы-вымогатели - это разновидность вредоносного программного обеспечения - вредоносного ПО, которое шифрует файлы и документы на чем угодно - от одного ПК до всей сети, включая серверы. Жертвам часто остается мало выбора; они могут либо восстановить доступ к своей зашифрованной сети, заплатив выкуп преступникам, стоящим за программой-вымогателем, либо восстановить данные из резервных копий, либо надеяться, что ключ дешифрования имеется в свободном доступе. Или начать заново с нуля.

Некоторые заражения программами-вымогателями начинаются с того, что кто-то внутри организации щелкает то, что выглядит как невинное вложение, которое при открытии загружает вредоносные данные и шифрует сеть.

В других, гораздо более крупных кампаниях по вымогательству используются программные эксплойты и недостатки, взломанные пароли и другие уязвимости для получения доступа к организациям, использующим слабые места, такие как серверы с выходом в Интернет или входы на удаленный рабочий стол для получения доступа. Злоумышленники будут тайно искать в сети, пока не получат контроль как можно больше, прежде чем зашифровать все, что они могут.

Если важные файлы и документы, сети или серверы внезапно зашифровываются и становятся недоступными, это может стать головной болью для компаний любого размера. Хуже того, после того, как вы подвергнетесь атаке с помощью программы-вымогателя для шифрования файлов, преступники нагло объявят, что держат ваши корпоративные данные в заложниках, пока вы не заплатите выкуп, чтобы вернуть их.

Это может показаться слишком простым, но это работает - до такой степени, что директор британского разведывательного агентства GCHQ Джереми Флеминг предупредил, что угроза программ-вымогателей «растет с угрожающей скоростью».

Какова история программ-вымогателей?

Хотя в последние годы количество программ-вымогателей резко возросло, это явление не новое: первый экземпляр того, что мы теперь называем программами-вымогателями, появился в 1989 году.

Этот вирус, известный как AIDS или PC Cyborg Trojan, рассылался жертвам - в основном в сфере здравоохранения - на дискетах. Программа-вымогатель подсчитала количество загрузок ПК: как только она достигла отметки 90, она зашифровала машину и файлы на ней и потребовала от пользователя «продлить лицензию» с помощью «PC Cyborg Corporation», отправив 189 или 378 долларов в почтовое отделение. коробка в Панаме.

Как развивались программы-вымогатели?

Эта ранняя программа-вымогатель представляла собой относительно простую конструкцию, в которой использовалась базовая криптография, которая в основном просто изменяла имена файлов, что позволяло легко преодолеть ее.

Но это положило начало новому направлению компьютерных преступлений, которое медленно, но верно расширялось - и действительно взлетело в эпоху Интернета. Прежде чем они начали использовать передовую криптографию для

нацеливания на корпоративные сети, хакеры нацеливались на обычных пользователей Интернета с помощью базовых программ-вымогателей.

Одним из наиболее успешных вариантов была «полицейская программа-вымогатель», которая пыталась вымогать у жертв, утверждая, что компьютер был зашифрован правоохранительными органами. Он заблокировал экран с запиской о выкупе, предупреждающей пользователя о том, что он совершил незаконную онлайн-активность, из-за чего его могли отправить в тюрьму.

Однако, если жертва заплатит штраф, «полиция» позволит разрешить нарушение и восстановить доступ к компьютеру, передав ключ дешифрования. Конечно, это не было связано с правоохранительными органами - это преступники, эксплуатирующие невинных людей.

Хотя эти формы программ-вымогателей в некоторой степени успешны, они часто просто накладывают свое «предупреждающее» сообщение на дисплей пользователя - и перезагрузка машины может избавить от проблемы и восстановить доступ к файлам, которые никогда не были действительно зашифрованы.

Преступники извлекли уроки из этого, и теперь большинство схем вымогателей используют передовую криптографию, чтобы по-настоящему заблокировать зараженный компьютер и файлы на нем.

Какие основные типы программ-вымогателей?

Программы-вымогатели постоянно развиваются, постоянно появляются новые варианты и создают новые угрозы для бизнеса. Однако некоторые типы программ-вымогателей оказались более успешными, чем другие.

Наиболее плодовитая семья вымогателей во время 2021 года до сих пор является Sodinokibi, которая преследует организацию по всему миру с развивающимся в апреле 2019 года.

Эта программа-вымогатель, также известная как REvil, была ответственна за шифрование сетей большого количества известных организаций, включая Travelex и юридическую фирму из Нью-Йорка со знаменитыми клиентами.

Банда, стоящая за Sodinokibi, долгое время закладывала основу для атаки, незаметно перемещаясь по скомпрометированной сети, чтобы гарантировать, что все возможное может быть зашифровано до того, как будет запущена атака программы-вымогателя.

Известно, что те, кто стоит за Sodinokibi, требовали выплат в миллионы долларов в обмен на расшифровку данных. А учитывая, что хакеры часто получают полный контроль над сетью, те организации, которые отказываются платить выкуп после того, как стали жертвой Содинокиби, также обнаруживают, что банда угрожает раскрыть украденную информацию, если выкуп не будет выплачен.

Sodinokibi - не единственная кампания по вымогательству, которая угрожает утечкой данных от жертв в качестве дополнительного рычага для вымогательства платежа; вымогателей банды, как Конти, Doppelpaymer и Эгрегор среди тех, кто угрожает опубликовать украденную информацию, если жертва не платить.

Все время появляются новые семейства программ-вымогателей, в то время как другие внезапно исчезают или выходят из моды, а на подпольных форумах постоянно появляются новые вариации. Любая из распространенных форм

программ-вымогателей прямо сейчас может стать вчерашней новостью всего через несколько месяцев.

Например, Locky когда-то был самой печально известной формой вымогателей, создававшей хаос в организациях по всему миру в течение 2016 года, распространяясь через фишинговые электронные письма. Locky оставался успешным, потому что те, кто стоял за ним, регулярно обновляли код, чтобы избежать обнаружения. Они даже обновили его, добавив в него новые функции, в том числе возможность требовать выкуп на 30 языках, чтобы преступникам было проще преследовать жертв по всему миру. В какой-то момент Locky стал настолько успешным, что стал одной из самых распространенных форм вредоносного ПО. Однако менее чем через год он, казалось, исчез, и с тех пор о нем никто не слышал.

В следующем году именно Cerber стал наиболее распространенной формой вымогателей, на долю которых в апреле 2017 года приходилось 90% атак программ-вымогателей на Windows. Одной из причин, по которой Cerber стал настолько популярным, был способ его распространения как «программа-вымогатель как услуга», позволяющая пользователям без технических знаний проводить атаки в обмен на часть прибыли, возвращаемой первоначальным авторам.

В то время как Cerber, казалось, исчез к концу 2017 года, он стал пионером модели «как услуга», которая сегодня популярна во многих формах программ-вымогателей.

Еще одной успешной формой программ-вымогателей в 2017 и 2018 годах была SamSam, которая стала одним из первых семейств, получивших печальную известность не только тем, что взимала выкуп в десятки тысяч долларов за ключ дешифрования, но и использовала незащищенные системы с выходом в Интернет в качестве средства. заражения и распространения по сетям.

В ноябре 2018 года Министерство юстиции США обвинило двух хакеров, работающих в Иране, в создании программы-вымогателя SamSam, которая, как сообщается, в течение года выплатила выкуп на сумму более 6 миллионов долларов. Вскоре после этого SamSam перестала быть активной формой вымогателей.

В течение 2018 и 2019 годов еще одним семейством программ-вымогателей, которое оказалось проблематичным как для предприятий, так и для домашних пользователей, было GandCrab, которое Европол охарактеризовал как «одну из самых агрессивных форм программ-вымогателей» в то время.

GandCrab работал «как услуга» и получал регулярные обновления, что означает, что даже когда исследователи безопасности взломали его и смогли выпустить ключ дешифрования, вскоре после этого появилась новая версия программы-вымогателя с новым методом шифрования.

Создатели GandCrab, очень успешные в первой половине 2019 года, внезапно объявили о закрытии операции, заявив, что они получали 2,5 миллиона долларов в неделю, сдавая ее в аренду другим киберпреступникам. GandCrab исчез через несколько недель, хотя похоже, что злоумышленники могли просто переключить свое внимание на другую кампанию; Исследователи предположили сильное

сходство в коде GandGrab по сравнению с Sodinokibi, который по-прежнему пользуется успехом в 2020 году.

Между тем, одним из самых успешных семейств программ-вымогателей в 2020 году была программа- вымогатель Maze, которая сочетала регулярные обновления кода вредоносного ПО с угрозами утечки украденной информации в случае невыплаты шестизначного выкупа. Группа «вышла на пенсию» в конце 2020 года, но есть подозрения, что некоторые из тех, кто стоял за успехом Maze, перешли к другим криминальным операциям с программами-вымогателями.

Что представляла собой атака программы-вымогателя Colonial Pipeline?

В мае 2021 года Колониальный трубопровод, на который приходится 45% поставок топлива для Восточного побережья США, временно прекратил работу из-за атаки программы-вымогателя.

Бензин, дизельное топливо, реактивное топливо, мазут для отопления домов и топливо для армии США - все это зависит от топлива по Колониальному трубопроводу.

Опасаясь перебоев в поставках из-за инцидента, Федеральное управление безопасности автотранспортных средств (FMCSA) Министерства транспорта США выпустило чрезвычайное заявление, поэтому автомобильная транспортировка топлива может помочь удовлетворить потребности тех, кто не обслуживается трубопроводом, перекрытым программами-вымогателями.

Произошел такой сбой, вызванный атакой программ-вымогателей, которая нанесла вред ИТ-операциям за трубопроводом, что президент Джо Байден был проинформирован об этом.

В некоторых сообщениях говорится, что за атакой, шифрующей ИТ-сеть Colonial Pipeline, стояла программа-вымогатель как услуга Darkside. Darkside был относительно малоизвестным оператором в области программ-вымогателей до инцидента с Colonial Pipeline, но атака продемонстрировала, что даже если программа-вымогатель не является громким «брендом» на подпольных форумах, она все равно может вызвать серьезные сбои.

Что такое программа-вымогатель WannaCry?

WannaCry, также известный как WannaCrypt и Wcry, до сих пор считается самой крупной атакой программ-вымогателей, вызвав хаос во всем мире в результате атаки, которая началась в пятницу, 12 мая 2017 года.

Программа-вымогатель WannaCrypt требует 300 долларов в биткойнах за разблокировку зашифрованных файлов - цена, которая удваивается через три дня. Пользователям также угрожают с помощью записки о выкупе на экране навсегда удалить все их файлы, если выкуп не будет выплачен в течение недели.

В течение одного уик-энда жертвами программ-вымогателей стали более 300 000 жертв в более чем 150 странах, при этом пострадали предприятия, правительства и отдельные лица по всему миру.

В организациях здравоохранения по всей Великобритании системы были отключены из-за атаки программ-вымогателей, что вынудило пациентов отменить записи на прием, в результате чего в больницах стали говорить людям избегать посещения отделений неотложной помощи и неотложной помощи, если в этом нет крайней необходимости.

По мнению исследователей в области безопасности, из всех стран, пострадавших от атаки, Россия пострадала больше всего: вредоносное ПО WannaCry привело к обрушению российских банков, операторов телефонной связи и даже ИТ-систем, поддерживающих транспортную инфраструктуру. Китай также сильно пострадал от атаки: всего 29 000 организаций стали жертвами этой особенно опасной формы вымогателей.

Среди других громких целей был производитель автомобилей Renault, который был вынужден остановить производственные линии в нескольких местах, поскольку программа-вымогатель нанесла ущерб системам.

Червь-вымогатель настолько силен, что использует известную программную уязвимость EternalBlue. Уязвимость Windows - одна из многих уязвимостей нулевого дня, о которых, по всей видимости, было известно АНБ - до того, как хакерский коллектив Shadow Brokers сообщил о ней. Ранее в этом году Microsoft выпустила исправление для этой уязвимости, но только для самых последних операционных систем.

В ответ на атаку Microsoft предприняла беспрецедентный шаг, выпустив исправления для неподдерживаемых операционных систем для защиты от вредоносного ПО.

С тех пор службы безопасности США и Великобритании указали на Северную Корею как на виновника атаки с использованием программы-вымогателя WannaCry, а Белый дом официально объявил Пхеньян источником вспышки.

Однако Северная Корея назвала обвинения в том, что она стоит за WannaCry, «абсурдными».

Независимо от того, кто в конечном итоге стоял за WannaCry, если целью схемы было заработать большие суммы денег, она потерпела неудачу - было выплачено всего около 100000 долларов.

Прошло почти три месяца, прежде чем злоумышленники WannaCry, наконец, вывели средства из биткойн-кошельков WannaCry - из-за колебаний стоимости биткойнов они ушли на общую сумму 140 000 долларов.

Но, несмотря на наличие критических исправлений для защиты систем от WannaCry и других атак, использующих уязвимость SMB, большое количество организаций, по-видимому, предпочли не применять обновления.

Считается, что это причина, по которой LG перенесла инфекцию WannaCry в августе - через три месяца после первоначальной вспышки. С тех пор компания заявила, что применила соответствующие исправления.

Публичный дамп эксплойта EternalBlue, стоящий за WannaCry, привел к тому, что различные хакерские группы попытались использовать его для распространения своего вредоносного ПО. Исследователи даже задокументированы, как кампания среди европейских отелей от APT28 - российской хакерской группой, связанной с вмешательством в президентских выборах в США - теперь с помощью просочилась NSA уязвимости.

Что такое программа-вымогатель NotPetya?

Спустя чуть больше месяца после вспышки вируса-вымогателя WannaCry мир подвергся еще одной глобальной атаке вымогателей.

Эта кибератака сначала поразила цели в Украине, включая ее центральный банк, главный международный аэропорт и даже чернобыльский ядерный объект, а затем быстро распространилась по всему миру, заразив организации по всей Европе, России, США и Австралии.

После некоторой первоначальной путаницы относительно того, что это за вредоносное ПО - некоторые сказали, что это Petya, некоторые - что-то другое, отсюда и название NotPetya, - исследователи Bitdefender пришли к выводу, что причиной эпидемии стала модифицированная версия программы-вымогателя Petya, сочетающая элементы GoldenEye - особенно злобного родственника Petya - и вымогателя WannaCry в чрезвычайно мощное вредоносное ПО.

Эта вторая форма вымогателя также использует тот же эксплойт EternalBlue для Windows, который предоставил WannaCry червеобразные функции для распространения по сети (а не просто через вложения электронной почты, как это часто бывает) и поразил 300 000 компьютеров по всему миру.

Однако NotPetya - гораздо более жестокая атака. Атака не только шифрует файлы жертв, но и целые жесткие диски, перезаписывая основную запись перезагрузки, не позволяя компьютеру загружать операционную систему или что-либо делать.

Злоумышленники просят выкуп в биткойнах в размере 300 долларов, который будет отправлен на конкретный адрес электронной почты, который был отключен хостом почтовой службы. Однако то, как эта очень сложная программа-вымогатель, очевидно, была оснащена очень простыми, неавтоматизированными функциями для получения выкупа, заставило некоторых предположить, что деньги не были целью.

Это заставило многих поверить, что записка о вымогателе была всего лишь прикрытием настоящей цели вируса - вызвать хаос путем безвозвратного удаления данных с зараженных машин.

Какой бы ни была цель атаки, она существенно повлияла на финансы зараженных организаций. Британская компания по производству потребительских товаров Reckitt Benckiser заявила, что потеряла 100 миллионов фунтов стерлингов в доходах в результате того, что стала жертвой Пети.

Но это относительно скромные потери по сравнению с другими жертвами атаки: оператор судов и судов снабжения Maersk и компания по доставке товаров FedEx оценили убытки в 300 миллионов долларов из-за удара Пети.

В феврале 2018 года правительства Великобритании, США, Австралии и других стран официально заявили, что вымогатель NotPetya - дело рук российских военных. Россия отрицает свою причастность.

Во сколько вам обойдется атака программы-вымогателя?

Очевидно, что самые непосредственные издержки, связанные с заражением программой-вымогателем - если она оплачена, - это требование выкупа, которое может зависеть от типа программы-вымогателя или размера вашей организации.

Атаки программ-вымогателей могут различаться по размеру, но хакерские банды все чаще требуют миллионы долларов для восстановления доступа к сети. И причина, по которой хакерские банды могут требовать такие деньги, состоит в том, что многие организации будут платить.

Это особенно актуально, если сеть, заблокированная программой-вымогателем, означает, что организация не может вести бизнес - они могут терять большие суммы дохода каждый день, возможно, даже каждый час, сеть недоступна. По оценкам, атака программы-вымогателя NotPetya обошлась транспортной компании Maersk в размере до 300 миллионов долларов убытков.

Если организация решит не платить выкуп, она не только обнаружит, что теряет доход в течение периода времени, который может длиться недели, возможно, месяцы, но и, вероятно, обнаружит, что платит крупную сумму за то, чтобы охранная компания пришла и восстановила доступ к сети. В некоторых случаях это может даже стоить больше, чем требование выкупа, но, по крайней мере, в этом случае платеж идет законному бизнесу, а не финансирует преступников.

Каким бы способом организация ни боролась с атакой программы-вымогателя, она также будет иметь финансовые последствия в будущем; потому что, чтобы защититься от повторной жертвы, организации необходимо будет вложить средства в свою инфраструктуру безопасности, даже если это означает разорвать сеть и начать все сначала.

Вдобавок ко всему этому, существует также риск того, что клиенты потеряют доверие к вашему бизнесу из-за плохой кибербезопасности и уведут свой бизнес в другое место.

Почему организациям следует беспокоиться о программах-вымогателях?

Проще говоря: программы-вымогатели могут разрушить ваш бизнес. Если вредоносное ПО заблокирует свои файлы даже на день, это повлияет на ваш доход. Но с учетом того, что программы-вымогатели отключают большинство жертв как минимум на неделю, а иногда и на месяцы, потери могут быть значительными. Системы так долго отключаются не только потому, что программы-вымогатели блокируют систему, но и из-за всех усилий, необходимых для очистки и восстановления сетей.

И дело не только в непосредственном финансовом ударе программ-вымогателей; потребители опасаются передавать свои данные организациям, которые они считают небезопасными.

Киберпреступники узнали, что не только предприятия становятся прибыльными целями для атак программ-вымогателей, поскольку такие важные инфраструктуры, как больницы и даже промышленные предприятия, разрушаются программами-вымогателями - нарушение этих сетей может иметь большие последствия для людей в физическом мире.

В конечном итоге злоумышленники ищут простой способ заработать деньги, а больница, обнаружившая, что ее сеть зашифрована с помощью программ-вымогателей, не может позволить себе поставить под угрозу лечение пациентов, отключив сеть на несколько недель, чтобы вручную восстановить ее. Вот почему, к сожалению, многие жертвы программ-вымогателей в сфере здравоохранения заплатят выкуп, особенно когда они уже были ошеломлены последствиями пандемии COVID-19.

Сектор образования также стал очень частой целью кампаний вымогателей. Школы и университеты стали полагаться на дистанционное обучение из-за

пандемии коронавируса, и это заметили киберпреступники. Сети потенциально используются тысячами людей, многие из которых используют свои личные устройства, и все, что может потребоваться злоумышленнику для получения доступа к сети, - это одно успешное фишинговое письмо или взлом пароля одной учетной записи.

Национальный центр кибербезопасности Великобритании (NCSC) призвал школы и университеты обратить внимание на растущую угрозу программ-вымогателей после того, как инцидент с вымогательством привел к потере студентами курсовых работ, финансовых отчетов школ, а также данных, касающихся тестирования COVID-19.

Почему малые предприятия становятся мишенью для программ-вымогателей?

Малые и средние предприятия являются популярной целью, поскольку они, как правило, имеют более низкую кибербезопасность, чем крупные организации. Несмотря на это, многие малые и средние предприятия ошибочно полагают, что они слишком малы, чтобы стать мишенью, но даже «меньший» выкуп в несколько сотен долларов по-прежнему очень выгоден для киберпреступников.

Почему программы-вымогатели так успешны?

Вы можете сказать, что есть одна ключевая причина, по которой вымогатели процветают: потому что они работают. Все, что требуется от программы-вымогателя, чтобы проникнуть в вашу сеть, - это чтобы один пользователь ошибся и запустил вредоносное вложение электронной почты или повторно использовал ненадежный пароль.

Если бы организации не уступали требованиям выкупа, преступники перестали бы использовать программы-вымогатели. Но бизнесу действительно нужен доступ к данным, чтобы функционировать, поэтому многие готовы заплатить выкуп и покончить с этим.

Между тем для преступников это очень простой способ заработать. Зачем тратить время и силы на разработку сложного кода или создание поддельных кредитных карт из украденных банковских реквизитов, если программа-вымогатель может привести к мгновенным выплатам сотен или даже тысяч долларов сразу от большого количества зараженных жертв?

Некоторые утверждают, что киберстрахование делает программы-вымогатели еще более серьезной проблемой. Киберстрахование - это полис, предназначенный для защиты организаций от последствий кибератак.

Однако некоторые полисы киберстрахования будут покрывать саму выплату выкупа, в результате чего некоторые эксперты по кибербезопасности предупреждают, что выплаты по киберстрахованию, покрывающие стоимость выплаты выкупа, усугубляют проблему, потому что киберпреступники знают, что если они попадут в правильную цель, они получат деньги.

Какое отношение биткойн и другие криптовалюты имеют к распространению программ-вымогателей?

Рост криптовалют, таких как биткойн, облегчил киберпреступникам возможность тайного получения платежей, вымогаемых с помощью этого типа вредоносного ПО, без риска для властей установить виновных.

Безопасный, не отслеживаемый метод совершения платежей - жертв просят произвести платеж на биткойн-адрес - делает его идеальной валютой для преступников, которые хотят, чтобы их финансовая деятельность оставалась скрытой.

Киберпреступные банды постоянно становятся более профессиональными - многие даже предлагают обслуживание клиентов и помощь жертвам, которые не знают, как получить или отправить биткойны, потому что какой смысл требовать выкуп, если пользователи не знают, как платить? Некоторые организации даже скопили часть криптовалюты на случай, если они заразятся или их файлы зашифрованы, и им придется срочно платить биткойнами.

Как предотвратить атаку программ-вымогателей?

При большом количестве атак программ-вымогателей, начиная с того, что хакеры используют небезопасные порты с выходом в Интернет и протоколы удаленного рабочего стола, одна из ключевых вещей, которые организация может сделать, чтобы не стать жертвой, - это обеспечить, если это не существенно, чтобы порты не были доступны Интернет, если они не нужны.

Когда необходимы удаленные порты, организации должны убедиться, что учетные данные для входа имеют сложный пароль для защиты от злоумышленников, желающих развернуть программу-вымогатель, от возможности взломать простые пароли с использованием атак грубой силы в качестве способа защиты. Применение двухфакторной аутентификации к этим учетным записям также может выступать в качестве барьера для атак, поскольку при попытке несанкционированного доступа будет выдано предупреждение.

Организации также должны убедиться, что в сети установлены последние обновления безопасности, поскольку многие формы программ-вымогателей и других вредоносных программ распространяются с использованием широко известных уязвимостей.

EternalBlue, уязвимость, использовавшаяся в WannaCry и NotPetya, по-прежнему является одним из наиболее распространенных эксплойтов, используемых для распространения атак, несмотря на то, что исправление безопасности для защиты от нее доступно уже более трех лет.

Когда дело доходит до предотвращения атак по электронной почте, вы должны обучить сотрудников тому, как обнаруживать входящие атаки вредоносного ПО. Даже обнаружение небольших индикаторов, таких как плохое форматирование или то, что электронное письмо якобы от Microsoft Security отправлено с непонятного адреса, в котором даже нет слова Microsoft, может спасти вашу сеть от заражения. Те же политики безопасности, которые защищают вас от атак вредоносных программ, в некоторой степени помогут предотвратить создание вымогателями хаоса для вашего бизнеса.

Также есть что сказать о том, чтобы сотрудники могли учиться на ошибках, находясь в безопасной среде. Например, одна фирма разработала интерактивный видео-опыт, который позволяет ее сотрудникам принимать решения по серии событий, а затем выяснять последствия тех, что в конце концов. Это позволяет им учиться на своих ошибках, не страдая ни от каких реальных последствий.

На техническом уровне запрет сотрудникам включать макросы - это большой шаг к тому, чтобы они не могли случайно запустить файл вымогателя. Microsoft Office 2016, а теперь и Microsoft Office 2013, обладают функциями, позволяющими отключать макросы. По крайней мере, работодатели должны инвестировать в антивирусное программное обеспечение и поддерживать его в актуальном состоянии, чтобы оно могло предупреждать пользователей о потенциально вредоносных файлах. Резервное копирование важных файлов и проверка того, что эти файлы не могут быть скомпрометированы во время атаки с использованием другого ключа.

Сколько времени нужно, чтобы оправиться от атаки программы-вымогателя?

Проще говоря, программы-вымогатели могут нанести вред всей организации - зашифрованная сеть более или менее бесполезна, и мало что можно сделать, пока системы не будут восстановлены.

Если ваша организация разумна и имеет резервные копии, системы могут вернуться в оперативный режим за время, необходимое для восстановления работоспособности сети, хотя в зависимости от размера компании это может варьироваться от нескольких часов до дней.

Одна компания подробно описала ZDNet, как потребовались недели, чтобы восстановить их сеть до полного рабочего состояния, даже при восстановлении сети из резервных копий после отказа платить выкуп.

Однако, хотя восстановить функциональность можно в краткосрочной перспективе, организациям может быть сложно восстановить и запустить все системы, что продемонстрировала атака Petya.

Через месяц после вспышки Reckitt Benckiser подтвердила, что некоторые из ее операций все еще прерываются и не будут полностью запущены до двух месяцев после первоначальной вспышки болезни Пети.

Помимо непосредственного воздействия программ-вымогателей на сеть, они могут привести к постоянному финансовому ущербу. Каждый раз, когда оффлайн плохо для бизнеса, так как это в конечном итоге означает, что организация не может предоставлять услуги, которые она намеревается, и не может зарабатывать деньги, но чем дольше система находится в автономном режиме, тем больше это может быть.

Это если ваши клиенты хотят вести с вами бизнес: в некоторых секторах тот факт, что вы стали жертвой кибератаки, потенциально может оттолкнуть клиентов.

Как удалить программу-вымогатель?

В «No More Ransom инициатива» - запущен в июле 2016 года Европола и национальной полиции Нидерландов в сотрудничестве с рядом кибербезопасности компаний, включая Лаборатории Касперского и McAfee - предлагает бесплатные инструменты для дешифрования для вымогателей вариантов, чтобы помочь жертвам восстановить свои зашифрованные данные, не поддаваясь волю кибер-вымогателей.

Портал предлагает инструменты дешифрования для четырех семейств программ-вымогателей - Shade, Rannoh, Rakhn и CoinVault - и схема регулярно

добавляет дополнительные инструменты дешифрования для еще большего числа версий программ-вымогателей.

Портал, который также содержит информацию и советы о том, как не стать жертвой программ-вымогателей в первую очередь, обновляется как можно чаще, чтобы обеспечить доступность инструментов для борьбы с новейшими формами программ-вымогателей.

No More Ransom вырос из набора из четырех инструментов до огромного количества инструментов дешифрования, охватывающих сотни семейств программ-вымогателей. К настоящему времени эти инструменты расшифровали десятки тысяч устройств, лишив преступников миллионов выкупов.

Платформа теперь доступна на десятках языков, и ее поддерживают более 100 партнеров в государственном и частном секторах.

Отдельные компании, занимающиеся безопасностью, также регулярно выпускают инструменты дешифрования, чтобы противостоять продолжающейся эволюции программ-вымогателей - многие из них будут публиковать обновления об этих инструментах в блогах своих компаний, как только они взломают код.

Еще один способ обойти заражение программами-вымогателями - обеспечить регулярное резервное копирование данных в вашей организации в автономном режиме. Перенос файлов резервных копий на новую машину может занять некоторое время, но если компьютер заражен и у вас есть резервные копии, можно просто изолировать этот модуль, а затем продолжить свой бизнес. Просто убедитесь, что мошенники, использующие криптоблокировку, также не могут зашифровать ваши резервные копии.

Стоит ли платить выкуп с помощью программы-вымогателя?

Некоторые говорят, что жертвы должны просто заплатить выкуп, ссылаясь на то, что это самый быстрый и простой способ получить их зашифрованные данные - и многие организации платят, даже если правоохранительные органы предупреждают об этом.

Но будьте осторожны: если станет известно, что ваша организация является легкой мишенью для киберпреступников, потому что она заплатила выкуп, вы можете оказаться под прицелом других киберпреступников, которые стремятся воспользоваться вашей слабой системой безопасности. И помните, что вы имеете дело с преступниками, и сама их природа означает, что они могут не сдержать свое слово: нет никакой гарантии, что вы когда-нибудь получите ключ дешифрования, даже если он у них есть. Расшифровка даже не всегда возможна: есть истории о жертвах, которые платили выкуп, но при этом не разблокировали зашифрованные файлы.

Например, программа-вымогатель, нацеленная на Linux, обнаруженная ранее в этом году, требовала оплаты биткойнами, но не хранила ключи шифрования локально или через командно-управляющий сервер, что в лучшем случае делало уплату выкупа бесполезной.

Можно ли получить на свой смартфон программы-вымогатели?

Абсолютно. Атаки программ-вымогателей на устройства Android значительно возросли, поскольку киберпреступники понимают, что многие люди не знают, что смартфоны могут быть атакованы, а содержимое (часто более личное,

чем то, что мы храним на ПК) зашифровано с целью выкупа с помощью вредоносного кода. Таким образом, появились различные формы программ-вымогателей для Android, которые беспокоят мобильных пользователей.

Фактически, любое устройство, подключенное к Интернету, является потенциальной целью для программ-вымогателей, которые, как уже было замечено, блокируют смарт-телевизоры.

Программы-вымогатели и Интернет вещей

Устройства Интернета вещей уже имеют плохую репутацию с точки зрения безопасности. По мере того, как их все больше и больше выходит на рынок, они будут предоставлять миллиарды новых векторов атак для киберпреступников, потенциально позволяя хакерам удерживать ваш подключенный дом или подключенный автомобиль в заложниках. Зашифрованный файл - это одно, но как насчет того, чтобы найти записку о выкупе, которая отображается на вашем умном холодильнике или тостере?

Есть даже вероятность того, что хакеры могут заразить медицинские устройства, подвергнув жизни риску.

В марте 2018 года исследователи из IOActive сделали еще один шаг вперед, продемонстрировав, как коммерчески доступный робот может подвергнуться атаке программы-вымогателя. Исследователи не только заставляли робота устно требовать оплаты, чтобы вернуть его в нормальное состояние, но и издавать угрозы и ругаться.

Британский NCSC также предупредил, что рост умных городов также может стать заманчивой целью для кибератак - и нетрудно представить, что сдерживание общегородских сервисов от атак программ-вымогателей может быть очень прибыльным для преступников.

По мере того, как программы-вымогатели продолжают развиваться, вашим сотрудникам крайне важно понимать угрозу, которую они представляют, а организациям - делать все возможное, чтобы избежать заражения, поскольку программы-вымогатели могут нанести вред, а расшифровка не всегда возможна». ***(Danny Palmer. What is ransomware? Everything you need to know about one of the biggest menaces on the web // ZDNet (https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/). 10.05.2021).***

***

«Colonial Pipeline Co заплатила почти 5 миллионов долларов восточноевропейским хакерам в пятницу, что противоречит сообщениям ранее на этой неделе о том, что компания не собиралась платить вымогательство, чтобы помочь восстановить крупнейший топливопровод в стране, по словам двух людей, знакомых с сделкой.

По словам этих людей, компания заплатила огромный выкуп в криптовалюте, которую трудно отследить, в течение нескольких часов после атаки, подчеркнув огромное давление, с которым столкнулся оператор из Джорджии, чтобы снова направить бензин и авиакеросин в крупные города Восточного побережья. Третий человек, знакомый с ситуацией, сказал, что официальным лицам правительства США известно, что Colonial произвела оплату.

Получив платеж, хакеры предоставили оператору средство дешифрования, чтобы восстановить его отключенную компьютерную сеть. Инструмент работал настолько медленно, что компания продолжала использовать собственные резервные копии для восстановления системы, сказал один из людей, знакомых с усилиями компании.

Представитель Colonial от комментариев отказался. Colonial заявила, что начала возобновлять поставки топлива около 17:00 по восточному времени в среду.

Когда агентство Bloomberg News спросило президента Джо Байдена, проинформировали ли он о выплате выкупа компании, президент сделал паузу, а затем сказал: «У меня нет комментариев по этому поводу».

Подробнее: после кибератаки перезапускается крупнейший в США бензопровод

Хакеры, которые, по утверждениям ФБР, связаны с группой под названием DarkSide, специализируются на цифровом вымогательстве и предположительно находятся в России или Восточной Европе.

В среду средства массовой информации, включая Washington Post и Reuters, также основанные на анонимных источниках, сообщили, что компания не собиралась немедленно платить выкуп…

«Им пришлось заплатить», - сказал Ондрей Крехель, генеральный директор и основатель компании LIFARS, занимающейся цифровой криминалистикой, и бывший киберэксперт в Loews Corp., владеющей Boardwalk Pipeline. «Это кибер-рак. Ты хочешь умереть или хочешь жить? Это не та ситуация, когда можно ждать». ***(William Turton, Michael Riley, Jennifer Jacobs. Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom // Bloomberg (https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom). 13.05.2021).***

***

«Служба здравоохранения Ирландии временно отключила свою ИТ-систему после того, что она описала как «серьезную атаку с использованием программ-вымогателей».

Руководство службы здравоохранения (HSE) заявило, что приняло меры предосторожности и закрыло свои системы, чтобы защитить их и оценить ситуацию.

Министр здравоохранения Ирландии Стивен Доннелли заявил, что инцидент «серьезно повлиял на [] медицинские и социальные услуги».

По его словам, службы экстренной помощи продолжали работать.

Больница Ротонда в Дублине отменила амбулаторные визиты из-за «критического состояния», за исключением случаев, когда женщины находятся на сроке беременности 36 недель или позже. Все гинекологические клиники закрыты.

В роддоме сказали, что всем, у кого есть срочные проблемы, следует обратиться.

Национальный родильный дом на Холлс-стрит в Дублине также заявил, что в пятницу будет «серьезный сбой» в его услугах «из-за серьезной проблемы с информационными технологиями».

«Серьезное влияние на медицинское обслуживание»

Он извинился перед пациентами и общественностью и сказал, что предоставит дополнительную информацию, когда она станет доступной.

В своем твите г-н Доннелли сказал, что его отдел работает над обеспечением защиты систем и информации.

Он добавил, что вакцинация и тестирование на Covid-19 будут проходить в обычном режиме.

«Значительный и серьезный»

Исполнительный директор HSE Пол Рид сообщил корреспонденту RTÉ Morning Ireland, что он работает над сдерживанием изощренной атаки программ-вымогателей, управляемых человеком, на свои ИТ-системы.

Он сказал, что кибератака оказала влияние на все национальные и местные системы, задействованные во всех основных сервисах.

Г-н Рид охарактеризовал атаку как «значительную и серьезную» и сказал, что HSE предприняло все меры предосторожности, чтобы отключить многие свои основные системы для их защиты.

«Мы работаем со всеми нашими основными поставщиками ИТ-безопасности, и кибер-группа национальной безопасности вовлечена и получает предупреждение, так что это будет основная поддержка государства, включая гарда (ирландская полиция), силы обороны и группы поддержки третьих лиц», - добавил он.

«Очевидно, мы приносим свои извинения за влияние, которое оно оказало, но мы находимся на очень ранних этапах полного понимания угрозы, воздействия и попытки сдержать их».

Г-н Рид сказал, что атака направлена на доступ к данным, хранящимся на центральных серверах.

Он сказал, что это серьезный инцидент, но на данном этапе не требовалось выкупа…

Мастер госпиталя Ротонда профессор Фергал Мэлоун сказал, что ночью они обнаружили, что стали жертвами атаки вымогателя, которая затронула все его электронные системы и записи.

Профессор Мэлоун сказал, что, по его мнению, это могло затронуть и другие больницы.

«Мы используем общую систему регистрации пациентов в НИУ ВШЭ, и, похоже, это должно было быть отправной точкой или источником.

«Это означает, что нам пришлось отключить все наши компьютерные системы».

Профессор Мэлоун сказал, что все пациенты в безопасности, и в больнице есть планы на случай непредвиденных обстоятельств, поэтому она может нормально функционировать с использованием бумажной системы.

Он добавил, что это замедлит обработку пациентов, поэтому больница пытается ограничить количество посещений приемов в пятницу.

Он сказал, что работало спасательное оборудование и пострадали компьютеры с медицинскими записями.

«У нас есть системы, позволяющие вернуться к старомодному ведению документации», - сказал он.

«На выходных придут роженицы, и мы сможем позаботиться о них».

Профессор Мэлоун сказал, что над решением этой проблемы работает команда.

Больница Ротонда написала в Твиттере, что пациенты, посещающие педиатрическую клинику по расписанию, должны «приходить как обычно».

В HSE написали в Твиттере, что Национальная служба скорой помощи «работает в обычном режиме, не влияя на обработку вызовов скорой помощи и их отправку на национальном уровне».

«Зона неопределенности»

Профессор Симус О'Рейли, онколог университетской больницы Корка, сказал, что все его компьютеры были отключены из-за кибератаки.

Он сказал RTÉ, что HSE действовала быстро, но это огорчает пациентов, которые ждут результатов и «живут в этой зоне неопределенности».

«Из-за этого в наших клиниках и палатах сегодня много бедствий», - добавил он.

Профессор О'Рейли сказал, что лечение рака зависело от технологий, и больница очень хочет продолжить лечение.

Он сказал, что ИТ-системы уже оказались под давлением из-за воздействия Covid-19.

Крысия Линч, председатель Ассоциации по улучшению услуг по охране материнства в Ирландии, сказала, что пришло время спросить HSE, есть ли у них надежное хранение записей пациентов и есть ли у них надлежащая киберзащита от этого типа программ-вымогателей.

«Если они переходят на электронные записи во всех родильных домах, им необходимо иметь свои гарантии, поскольку таким образом очень сложно нарушить работу родильных домов». ***(Irish health service hit by cyber attack // BBC (https://www.bbc.com/news/world-europe-57111615). 14.05.2021).***

***

«Один из крупнейших трубопроводов страны, Colonial Pipeline, по которому транспортируется 45 процентов запасов топлива на восточном побережье, был вынужден закрыть 7 мая после того, как подвергся атаке программ-вымогателей. Программы-вымогатели - это тип вредоносного ПО, в котором преступные группы шифруют данные, эффективно «удерживая их в заложниках», пока жертва не заплатит выкуп.

Colonial Pipeline возобновила работу 15 мая. Однако кибератака вызвала общественную панику и возмущение, поскольку в некоторых частях страны наблюдается нехватка топлива, а цены на топливо поднимаются до самого высокого уровня почти за семь лет. Инцидент также привел к возобновлению усилий правительства по укреплению безопасности трубопроводов и энергосистемы США. 11 мая Комитет по энергетике и торговле Палаты представителей США вновь ввел в действие двухпартийное законодательство, направленное на усиление способности Министерства энергетики («DOE») реагировать на угрозы кибербезопасности энергетической инфраструктуре США. Среди нескольких введенных мер были:

(1) Закон о готовности к кибербезопасности трубопроводов и объектов СПГ, что потребует от Министерства энергетики реализации программы по координации федеральных агентств, штатов и энергетического сектора для обеспечения безопасности, отказоустойчивости и живучести трубопроводов природного газа, трубопроводов для опасных жидкостей и объектов сжиженного природного газа («СПГ»);

(2) Закон о лидерстве в чрезвычайных ситуациях в сфере энергетики, который требует от министра энергетики возложить на помощника секретаря функции по чрезвычайным ситуациям в области энергетики и энергетической безопасности, включая обязанности в отношении инфраструктуры и кибербезопасности;

(3) Закон о Cyber Sense и Закон о повышении безопасности сетей посредством государственно-частного партнерства, который предписывает Министру энергетики создать добровольную программу Cyber Sense для проверки кибербезопасности продуктов и технологий, предназначенных для использования в системе оптовой электроснабжения; а также

(4) Закон о повышении безопасности сети посредством государственно-частного партнерства, который предписывает Министерству энергетики реализовывать программы по устранению связанных с кибербезопасностью уязвимостей и физических угроз для электрической сети.

Также в ответ на колониальный инцидент председатель Федеральной комиссии по регулированию энергетики («FERC») Ричард Глик и комиссар Элисон Клементс опубликовали заявление.10 мая призвал к введению обязательных стандартов кибербезопасности трубопроводов, аналогичных обязательным стандартам для электроэнергетического сектора, которые вводятся в координации с Североамериканской корпорацией надежности электроснабжения («NERC»). В заявлении FERC подчеркивается отсутствие «сопоставимых обязательных стандартов для трубопроводов природного газа, нефти и опасных жидкостей протяженностью почти 3 миллиона миль» в США, и что «подразумевают, что поощрение трубопроводов к добровольному внедрению передовых методов является неадекватным ответом на постоянно растущее число и изощренность злонамеренных кибер-акторов». Управление транспортной безопасности («TSA»), которое является частью Министерства транспорта, в настоящее время предоставляет добровольные руководящие принципы кибербезопасности для топливопроводов. Бывший председатель и комиссар Чаттерджи и председатель Глик раскритиковалиTSA в прошлом из-за отсутствия надзора за безопасностью трубопроводов, ответственность за которую в 2017 году была делегирована всего шести штатным сотрудникам. В то время FERC призвала Конгресс передать надзор за безопасностью трубопроводов Министерству энергетики…» ***(Kayla J. Grant, Randall S. Rich. Government Races to Secure Critical Infrastructure in Wake of Colonial Pipeline Ransomware Attack // Pierce Atwood LLP (https://energyinfrastructurelaw.com/government-races-to-secure-critical-infrastructure-in-wake-of-colonial-pipeline-ransomware-attack/#page=1).*** 17.05.2021).

***

«Ирландское национальное агентство по управлению здравоохранением (Health Service Executive, HSE) объявило сегодня, что занимается «серьезной атакой программ-вымогателей» на свои ИТ-системы, и в качестве меры предосторожности отключило определенные компьютерные системы, чтобы оценить уязвимость. масштаб атаки и отреагируйте соответствующим образом.

Влияние остановки будет значительным. HSE, крупнейший работодатель Ирландии с почти 70 000 штатными сотрудниками, управляет 86 больницами и большим количеством общественных медицинских учреждений, многие из которых были вынуждены отменить записи. Тем не менее, последствия закрытия, скорее всего, коснутся других государственных органов, при этом агентство социальных услуг Tusla подтвердило, что оно также пострадало от закрытия, как и система направления тестирования на Covid-19.

В СМИ сообщается, что в ВШЭ пока не поступало никаких требований, но, по ее мнению, атака была совершена с целью вымогательства денег. В интервью RTE генеральный директор НИУ ВШЭ Пол Рид отметил, что атака «изощренная» и «человеческая». Масштабы атаки не станут ясны в течение некоторого времени, но Рид подтвердил, что HSE работает над обеспечением защиты как ИТ-систем, так и содержащейся в них информации.

Вероятно, есть надежда, что атака представляет собой программу-вымогатель, поскольку если атака представляет собой атаку вредоносного ПО, предназначенную для максимального сбоя, такая как атака вредоносного ПО NotPetya, которая затронула судоходного гиганта Maersk в 2017 году, влияние на HSE может быть очень значительным.

Медицинские записи

Помимо возможного сбоя в работе ирландской службы здравоохранения и социального обеспечения, еще одна проблема будет заключаться в том, были ли скомпрометированы какие-либо медицинские записи пациентов. Ранние отчеты предполагают, что затронуто не медицинское оборудование, а системы, содержащие медицинские записи пациентов.

Медицинские записи - одни из самых ценных личных данных для хакеров, которые, как говорят, собирают на черном рынке в 10 раз больше, чем данные кредитной карты.

Тенденции

Атака программы-вымогателя на HSE имеет параллели с атакой программы-вымогателя WannaCry, поразившей NHS Великобритании в 2017 году. Эта атака затронула около одной трети трастов Национальной службы здравоохранения Великобритании, около 8% клиник общей практики и привела к отмене около 19 000 обращений в больницу.. Национальную службу здравоохранения критиковали за использование устаревшего программного обеспечения без исправлений и расходов на сумму около 92 миллионов фунтов стерлингов. К счастью, никакие личные данные пациентов не были скомпрометированы.

Атака HSE также демонстрирует тревожную тенденцию атак на критически важные службы в целом после громкой атаки программ-вымогателей на Colonial Pipeline в Соединенных Штатах на прошлой неделе, которая привела к остановке

трубопровода, поставляющего топливо на восточное побережье США. Это привело к росту цен на нефть, панике и объявлению чрезвычайного положения во Флориде. Несмотря на то, что Colonial, как сообщается, заплатила выкуп в размере 5 миллионов долларов, предполагается, что восстановление ее систем заняло значительное время.

Атака HSE также является демонстрацией растущей тенденции «программы-вымогателя как услуги»: считается, что DarkSide, восточноевропейская группа, разработала используемые инструменты-вымогатели, а атака была проведена аффилированным лицом.

Сектор здравоохранения остается мишенью для киберпреступников, и после атаки Национальной службы здравоохранения неоднократно делались предупреждения. В мае прошлого года Национальный центр кибербезопасности направил сектору экстренное уведомление после дальнейшего увеличения числа атак, по всей видимости, связанных со сбором информации о Covid-19. Еще неизвестно, насколько надежной была кибербезопасность ВШЭ в данном случае и были ли извлечены уроки. В любом случае это будет проблемой для всех пользователей системы, страховщиков и всех организаций. Бдительность в области ИТ-безопасности как никогда важна». ***(Sean O'Halloran and Andrew Jones. RANSOMWARE ATTACK ON IRISH HEALTH SERVICE EXECUTIVE AND IMPLICATIONS // Beale & Company Solicitors LLP (https://beale-law.com/article/ransomware-attack-on-irish-health-service-executive-and-implications/). 17.07.2021).***

***

«**В полицейском управлении столицы страны произошла массовая утечка внутренней информации после отказа удовлетворить требования шантажа русскоязычного синдиката вымогателей.** Эксперты говорят, что это самая ужасная из известных атак с использованием программ-вымогателей, когда-либо поражавшая полицейское управление США.

Банда, известная как группа Бабука, в четверг опубликовала в даркнете тысячи конфиденциальных документов столичного департамента полиции. В обзоре, проведенном Associated Press, были обнаружены сотни дисциплинарных досье полицейских и разведывательные отчеты, которые включают информацию из других агентств, включая ФБР и Секретную службу.

Атаки программ-вымогателей достигли уровня эпидемии, поскольку иностранные преступные группировки парализуют компьютерные сети в государственных и местных органах власти, департаментах полиции, больницах и частных компаниях. Они требуют крупных платежей за расшифровку украденных данных или для предотвращения их утечки в Интернете.

В результате кибератаки на прошлой неделе был остановлен Colonial Pipeline, крупнейший в стране топливопровод, что привело к накоплению запасов газа и панической покупке в некоторых частях юго-востока.

Бретт Кэллоу, аналитик угроз и эксперт по программам-вымогателям из компании Emsisoft, сказал, что утечка информации из полиции считается «возможно, самым значительным инцидентом с использованием программ-

вымогателей на сегодняшний день» из-за рисков, которые она представляет для офицеров и гражданских лиц.

Некоторые из документов включают информацию о безопасности от других правоохранительных органов, связанную с инаугурацией президента Джо Байдена, включая ссылку на «источник, встроенный» в группу ополченцев.

В одном документе подробно описываются шаги, предпринятые ФБР при расследовании двух самодельных бомб, оставленных в штаб-квартирах Национального комитета Демократической партии и Национального комитета Республиканской партии перед восстанием в Капитолии США 6 января. в вышках сотовой связи и планирует «проанализировать покупки» обуви Nike, которую носит заинтересованный человек, говорится в документе.

В отделении полиции не сразу ответили на запрос о комментарии, но ранее заявляли, что личные данные некоторых офицеров были украдены.

Некоторая из этой информации ранее просочилась, раскрывая личную информацию некоторых офицеров, взятую из проверок биографических данных, включая детали их прошлого употребления наркотиков, финансов и - по крайней мере в одном случае - сексуального насилия в прошлом.

В недавно опубликованных файлах содержится подробная информация о дисциплинарных разбирательствах в отношении сотен офицеров, начиная с 2004 года. Файлы часто содержат конфиденциальные и смущающие личные данные.

«Это вызовет шок среди правоохранительных органов по всей стране», - сказал Тед Уильямс, бывший офицер департамента, а теперь поверенный. Он представляет отставного офицера, чьи биографические данные были включены в более раннюю утечку.

Утечка таких конфиденциальных данных подчеркивает, насколько иностранные банды вымогателей верят, что могут действовать безнаказанно. Отчет аналитического центра Third Way за 2018 год показал, что менее 1% злонамеренных киберинцидентов приводят к принудительным мерам, принятым против злоумышленников.

Говоря о взломе трубопровода в четверг, Байден сказал, что его администрация «собирается принять меры, чтобы помешать» иностранным бандам вымогателей «действовать». Он также не исключил ответных кибератак.

Председатель Союза полицейских округа Колумбия Грегг Пембертон сказал, что профсоюз подал жалобу на город за нарушение коллективного договора. Профсоюз также хочет, чтобы генеральный инспектор города провел расследование.

«Как мы когда-либо наймем кого-нибудь для работы здесь, не мне, - сказал Пембертон.

На этой неделе группа Бабука указала, что она хотела бы 4 миллиона долларов, чтобы не публиковать файлы, а предложила только 100 000 долларов.

В ведомстве не сообщили, сделало ли оно предложение. Любые переговоры будут отражать сложность проблемы с программами-вымогателями, поскольку полиция будет вынуждена рассмотреть вопрос о выплатах преступным группировкам. ФБР, которое помогает в этом случае, препятствует выплатам программ-вымогателей.

Группа раскрыла нападение в прошлом месяце, пригрозив затем раскрыть личности конфиденциальных информаторов. Опубликованные в четверг данные показали, что они являются масштабными, и не сразу стало ясно, включены ли в них имена информаторов». ***(DC Police Victim of Massive Data Leak by Ransomware Gang // Wired Business Media (https://www.securityweek.com/dc-police-victim-massive-data-leak-ransomware-gang). 14.05.2021).***

***

«Французский страховой гигант AXA подтвердил, что некоторые из его операций в Азии подверглись атаке программ-вымогателей.

По всей видимости, за атакой стоит банда киберпреступников, использующая вымогатель под названием Avaddon.

У операторов Avaddon есть веб-сайт на базе Tor, на котором они называют имена жертв, которые не сотрудничают, и утечки украденных у них данных. В случае с AXA киберпреступники заявили, что нацелены на системы AXA в Гонконге, Таиланде, Филиппинах и Малайзии, и они утверждают, что украли 3 ТБ данных.

Банда утверждает, что украла файлы, хранящие информацию о клиентах, в том числе те, которые содержат такую информацию, как медицинские отчеты, претензии, платежи, информацию о банковских счетах, контракты и идентификационные карты. В подтверждение своих заявлений они опубликовали около 20 скриншотов.

Киберпреступники также начали DDoS-атаки на веб-сайты, принадлежащие AXA для Таиланда, Малайзии, Гонконга и Филиппин. Они начали запускать DDoS-атаки для дальнейшего вымогательства своих жертв в начале этого года.

В заявлении для СМИ AXA заявила, что «целенаправленная атака с использованием программ-вымогателей» затронула ее подразделение Asia Assistance, в частности, ИТ-операции в Таиланде, Малайзии, Гонконге и на Филиппинах. Компания подтвердила, что хакеры могли украсть некоторую информацию из ее систем, но - на основании проведенного до сих пор расследования - она полагает, что были доступны только данные, обработанные Inter Partners Assistance в Таиланде.

Компания уведомила деловых партнеров и регулирующие органы и пообещала связаться с пострадавшими лицами, если они подтвердят, что конфиденциальные данные были скомпрометированы.

Атака, нацеленная на AXA, стала известна через неделю после - очевидно, первой в отрасли - страховой гигант объявил, что прекратит оформление страховых полисов для вымогательства платежей операторам программ-вымогателей.

Приостановление действует только во Франции и не влияет на действующие правила. Это также не влияет на покрытие для реагирования и восстановления после атак программ-вымогателей.

AXA - не единственная страховая компания, пострадавшая от программ-вымогателей за последние месяцы. CNA из Чикаго, штат Иллинойс, объявила на прошлой неделе, что она полностью восстановила системы после обнаружения атаки вымогателя в марте». ***(Eduard Kovacs. AXA Confirms Ransomware Attack***

Impacted Operations in Asia // Wired Business Media (https://www.securityweek.com/axa-confirms-ransomware-attack-impacted-operations-asia). 17.05.2021).

***

«DarkSide - так называлась банда и программа-вымогатель, которой она управляла - 13 мая 2021 года объявила, что немедленно прекратит работу программы DarkSide Ransomware -as-a-Service (RaaS). Три дня спустя исследователи опубликовали анализ недавно обнаруженного варианта DarkSide, содержащего новую функцию. Он был обнаружен до закрытия программы, что вызвало два вопроса: представляет ли новый вариант угрозу; и что нам делать с отключением DarkSide?

Ответы на эти вопросы щедро разбросаны по поводу возможного, вероятного и возможного.

Операция DarkSide RaaS

DarkSide управляла сложной программой RaaS. Мэтт Лок, технический директор компании Varonis в Великобритании, объясняет, что иногда их филиалы перехватывали программу-вымогатель и контролировали всю атаку; иногда партнер предоставлял доступ, и DarkSide осуществлял атаку; иногда было бы наоборот; а для действительно «пикантных» целей DarkSide может все делать сама. Доходы от любого успешного вымогательства будут разделены между DarkSide и соответствующим аффилированным лицом.

По этой причине, даже если распознать атаку DarkSide легко, часто бывает трудно точно узнать, кто ее проводит. FireEye считает, что выявила как минимум пять партнерских групп.

По данным аналитической компании Elliptic, в ходе своей деятельности DarkSide и ее аффилированные лица заработали около 90 миллионов долларов (рассчитанных на момент анализа) в биткойнах.

Каждое использование вредоносного ПО будет адаптировано для каждой отдельной атаки, вплоть до использования разных C2. Это не были новые версии, просто разные варианты. Хотя антивирусные продукты могут легко распознать базовое вредоносное ПО, новые варианты часто означают, что первоначальное обнаружение на основе сигнатур было легко побеждено.

13 мая 2021 года DarkSide объявил о прекращении партнерской программы. Он потерял доступ к своему блогу, платежному серверу и серверам CDN, а средства с платежного сервера были выведены на неизвестный счет. В записке подразумевается, что ответственность за это несет неуказанный правоохранительный орган, и добавляется (перевод с русского любезно предоставлен intel471): «Ввиду вышеизложенного и из-за давления со стороны США партнерская программа закрыта. Оставайся в безопасности и удачи».

Принято считать, что, закрывая Colonial Pipeline, DarkSide перешагнула планку и вызвала серьезный гнев трехбуквенных агентств США.

Новый вариант Fortinet

17 мая 2021 года лаборатория Fortinet FortiGuard Labs опубликовала отчет о недавно обнаруженной функции в варианте DarkSide, нацеленной на разделы

диска. Открытие было сделано до закрытия DarkSide, но это функция, которую раньше не видели. Новый вариант имеет возможность обнаруживать и взламывать жесткие диски, разделенные на разделы, и, как предполагается, обеспечивает более надежное шифрование файлов, чтобы сделать попытки вымогательства более эффективными. Он также, конечно же, обнаружит любые файлы резервных копий, скрытые администраторами в скрытых разделах.

Исследователи подчеркивают профессионализм программистов вредоносных программ. По их словам, он был «эффективно запрограммирован с очень небольшим количеством потраченного впустую места, а раздувание компилятора было сведено к минимуму, что необычно для большинства вредоносных программ». Двумя наиболее интересными областями этого варианта DarkSide являются использование Active Directory и его действие против разделов.

Сначала он ищет контроллеры домена, а затем пытается использовать их для анонимного подключения к Active Directory через LDAP с пустым паролем и пустым именем пользователя. В случае успеха он пытается зашифровать файлы в любых сетевых папках, которые может найти (после проверки, что они доступны для записи), но избегает любых общих папок с именами C $ и ADMIN $. Это общие административные ресурсы по умолчанию, которые должны быть доступны только администраторам и операторам резервного копирования.

«Кажется вероятным, - говорят исследователи, - что DarkSide избегает этих общих ресурсов на случай, если он не будет работать в контексте администратора, и попытки доступа к ним потенциально могут вызвать предупреждение».

Он также сканирует жесткий диск, чтобы увидеть, является ли это мультизагрузочной системой, чтобы найти дополнительные тома / разделы, чтобы попытаться зашифровать их файлы. Если у найденного раздела есть GUID, который соответствует результатам вызова DeviceloControl API, он пропускает раздел и переходит к следующему. Необходимо, чтобы зараженные машины оставались хотя бы в полуисправимом состоянии. Для разделов, прошедших тесты, DarkSide пытается смонтировать их с помощью API SetVolumeMountPointW. После монтирования он пытается зашифровать все содержащиеся файлы.

«Насколько нам удалось определить, - говорят исследователи, - эти действия являются новинкой для программ-вымогателей. В результате глобальное сообщество кибербезопасности может не быть должным образом защищено от этой стратегии атак ».

Завершение работы и будущее DarkSide

Остается вопрос: является ли эта новая функция чем-то большим, чем академическим открытием после закрытия DarkSide; и действительно ли мы видели последний из DarkSide?

Ответ на первый: «возможно». Известно, что банды вредоносных программ делятся между собой методами или копируют их. Теперь, когда другие банды увидели, что DarkSide использует эту функцию, они, вероятно, включат подобное в свои собственные программы-вымогатели, даже если сам DarkSide не вернется.

Остается вопрос о природе отключения DarkSide. Возможно, это не будет постоянным. Единственный способ остановить банду - запереть основных членов. Мэтт Лок считает, что это может дать первый ключ к разгадке остановки. «Это не

значит, что мы не знаем, кто они такие», - сказал он SecurityWeek. «Они довольно открыто говорили о своей личности».

Это означает, что они фактически ограничены Россией. Если они выйдут наружу, им грозит арест и экстрадиция (или выдача) в США. «Может быть, - продолжил он, - они решили лечь на дно, пока не уляжется жара».

Но он также добавляет, что это может быть моральное решение. DarkSide совершенно ясно дал понять, что не будет атаковать ничего, что могло бы привести к гибели людей. Колониальный трубопровод находится на пороге этого, но, вероятно, нарушает собственный моральный кодекс DarkSide. Это также расстроило бы российское правительство, которое пока не занимается прямыми атаками на инфраструктуру США. Лок предполагает, что атака Colonial Pipeline могла быть ошибкой либо самой DarkSide, либо одной из ее дочерних компаний.

В этом нет ничего, что указывало бы на окончательный конец DarkSide. И члены банды, и код вымогателя все еще существуют. «В долгосрочной перспективе, - сказал SecurityWeek Вал Саенгпайбул, старший исследователь угроз в FortiGuard Labs, - я не верю, что отключение повлияет на деятельность программ-вымогателей по одной досадной причине: это слишком прибыльно». Однако в краткосрочной перспективе это может отпугнуть злоумышленников низкого уровня, использующих программу-вымогатель в качестве услуги, потому что они боятся быть пойманными. «Но для профессионалов, которые были в игре долгое время, я бы подумал, что они проводят хорошие практики OpSec, чтобы их не поймали. Кроме того, обычный международный характер злоумышленников добавляет еще один уровень сложности, когда дело доходит до юрисдикции правоохранительных органов».

Похоже, что DarkSide вернется. Это может быть другое имя с измененным программным обеспечением, или это может быть другая группа, использующая программное обеспечение DarkSide, но эта модель оказалась слишком эффективной и слишком прибыльной, чтобы от нее навсегда отказаться». ***(Kevin Townsend. DarkSide: Newly Found Variant and Implications for the Ransomware Gang's Future // Wired Business Media (https://www.securityweek.com/darkside-newly-found-variant-and-implications-ransomware-gangs-future). 19.05.2021).***

***

«Агентство по кибербезопасности и безопасности инфраструктуры США (CISA) опубликовало анализ программы-вымогателя FiveHands примерно через неделю после того, как исследователи безопасности Mandiant компании FireEye сообщили, что видели вредоносное ПО в недавних атаках.

Написанная на C++ программа-вымогатель FiveHands, по всей видимости, является преемником DeathRansom, исходя из сходства кода между ними. Однако оба семейства также показывают связь с программой-вымогателем HelloKitty.

Вредоносное ПО используется финансово мотивированным злоумышленником, известным как UNC2447, который активно атакует различные организации в Европе и Северной Америке и продемонстрировал передовые возможности.

На этой неделе CISA сообщила, что получила в общей сложности 18 вредоносных файлов, связанных с атакой FiveHands, включая восемь инструментов для тестирования на проникновение и эксплуатации с открытым исходным кодом, саму программу-вымогатель и девять файлов, связанных с трояном удаленного доступа SombRAT (RAT).

В рамках атаки, в ходе которой удалось успешно скомпрометировать организацию, злоумышленник использовал эти законные и вредоносные инструменты для кражи данных, шифрования файлов и требования выкупа от организации-жертвы.

Недостаток безопасности в продукте виртуальной частной сети (VPN) использовался как начальный вектор атаки, а общедоступные инструменты затем использовались для обнаружения сети, а программа-вымогатель запускалась на более позднем этапе атаки.

FiveHands, как отмечает CISA, использует схему шифрования с открытым ключом, называемую NTRUEncrypt, и выполняет перечисление, а затем стирает теневые копии томов для предотвращения восстановления данных. В рамках атаки также был развернут SombRAT, чтобы облегчить загрузку и выполнение дополнительных вредоносных полезных нагрузок.

В своем отчете об анализе вредоносных программ (MAR) и сопутствующем аналитическом отчете (AR) CISA предоставляет не только подробную техническую информацию о самом вредоносном ПО, но и рекомендации о том, как организации могут смягчить подобные атаки…». ***(Ionut Arghire. CISA Analyzes FiveHands Ransomware // Wired Business Media (https://www.securityweek.com/cisa-analyzes-fivehands-ransomware). 07.05.2021).***

***

«По данным британской службы безопасности Sophos, у кибератак в среднем есть 11 дней после взлома целевой сети, прежде чем они будут обнаружены, и часто, когда они обнаруживаются, это происходит из-за того, что они развернули программу-вымогатель.

Как отмечают исследователи Sophos в новом отчете, злоумышленнику более чем достаточно времени, чтобы получить подробный обзор того, как выглядит целевая сеть, в чем заключаются ее слабые места, а злоумышленникам-вымогателям - чтобы разрушить ее.

Данные Sophos, основанные на его ответах на инциденты с клиентами, предполагают, что «время ожидания» для злоумышленников гораздо короче, чем данные группы реагирования на инциденты FireEye, Mandiant. Mandiant недавно сообщил, что среднее время обнаружения составляет 24 дня, что является улучшением по сравнению с предыдущими годами.

Sophos объясняет, что относительно короткое время ожидания в своих данных о реагировании на инциденты связано с тем, что в колоссальных 81% инцидентов она помогала клиентам с использованием программ-вымогателей - шумной атаки, которая немедленно вызывает сигнал тревоги для технических отделов. Таким образом, хотя более короткое время ожидания может указывать на улучшение так называемого состояния безопасности, это также может быть связано

с тем, что программа-вымогатель с шифрованием файлов является разрушительной атакой по сравнению с кражей данных.

"Чтобы представить это в контексте, 11 дней потенциально предоставляют злоумышленникам около 264 часов для злонамеренных действий, таких как боковое движение, разведка, сброс учетных данных, кража данных и многое другое. Учитывая, что некоторые из этих действий могут занять минуты или несколько часов Чтобы реализовать, 11 дней дают злоумышленникам достаточно времени, чтобы нанести ущерб», - отмечает Sophos в своем отчете Active Adversary Playbook 2021.

Подавляющее большинство инцидентов, на которые реагировал Sophos, были атаками программ-вымогателей, что позволяет предположить масштаб проблемы. К другим атакам относятся кража данных, криптомайнеры, банковские трояны, очистители данных и использование инструментов тестирования на проникновение, таких как Cobalt Strike.

Еще одним примечательным моментом является широкое использование злоумышленниками протокола удаленного рабочего стола (RDP): около 30% атак начинается с RDP, а 69% последующих действий выполняется с помощью RDP. С другой стороны, фишинг был отправной точкой только для 12% атак, в то время как 10% атак были связаны с использованием незащищенных систем.

Атаки на конечные точки RDP уже давно используются для инициирования атак программ-вымогателей и гораздо более распространены, чем эксплойты против VPN. Несколько охранных компаний назвали RDP основным вектором вторжений для инцидентов с вымогательством в 2020 году. Компания по безопасности ESET сообщила, что в 2020 году количество RDP-атак увеличилось почти на 800%.

«RDP участвовал в 90% атак. Однако стоит отметить способ, которым злоумышленники использовали RDP. В инцидентах, связанных с RDP, он использовался для внешнего доступа только в 4% случаев. Около четверти (28%) атак показали, что злоумышленники использовали RDP как для внешнего доступа, так и для внутреннего перемещения, в то время как в 41% случаев RDP использовался только для внутреннего бокового перемещения внутри сети», - отмечают исследователи угроз Sophos.

Sophos также составил список наиболее широко наблюдаемых групп вымогателей. DarkSide, новый, но профессиональный провайдер программ-вымогателей, который начал свою деятельность в середине 2020 года, составлял только 3% расследований Sophos до 2020 года. Он оказался в центре внимания из-за атаки на Colonial Pipeline, которая, как сообщается, заплатила группе 5 миллионов долларов.

DarkSide предлагает свои программы-вымогатели в качестве услуги другим преступным группировкам, которые распространяют программы-вымогатели, подобно тому, как это делает банда вымогателей REvil. REvil был в центре внимания в прошлом году из-за атак на правительства и цели здравоохранения, а также из-за его высоких требований выкупа, которые в среднем составляли около 260 000 долларов.

Согласно Sophos, REvil (он же Sodinokibi) был самой активной угрозой вымогателей в 2020 году наряду с Ryuk, который, по некоторым оценкам, заработал 150 миллионов долларов с помощью программ-вымогателей.

Другие важные игроки-вымогатели, включая Dharma, Maze (несуществующий), Ragnarok и Netwalker (несуществующий).

Президент США Джо Байден на прошлой неделе заявил, что обсуждал с Москвой атаку с использованием вымогателей Colonial, и предложил России принять «решительные меры» против этих злоумышленников. США считают, что DarkSide базируется в России, но не связан с российским правительством.

«Мы напрямую общались с Москвой о том, что ответственные страны должны принять решительные меры против этих сетей-вымогателей», - сказал Байден 13 мая». ***(Liam Tung. This is how long hackers will hide in your network before deploying ransomware or being spotted // ZDNet (https://www.zdnet.com/article/this-is-how-long-hackers-will-spend-in-your-network-before-deploying-ransomware-or-being-spotted/). 18.05.2021).***

***

«Каждую неделю новая организация сталкивается с атакой программ-вымогателей, но в новом отчете исследовательской группы по безопасности eSentire и исследователя Dark Web Майка Мэйса говорится, что инциденты, которые мы видим в новостях, - это лишь небольшая часть истинного числа жертв.

В отчете о программах-вымогателях eSentire говорится, что только в 2021 году шесть групп вымогателей взломали 292 организации в период с 1 января по 30 апреля.

В отчете оценивается, что группам удалось выручить не менее 45 миллионов долларов от этих атак, и подробно описываются многочисленные инциденты, о которых никогда не сообщалось.

Команда eSentire и Мэйс сосредоточились исключительно на группах вымогателей Ryuk / Conti, Sodin / REvil, CLOP и DoppelPaymer, а также на двух новых, но заметных бандах в DarkSide и Avaddon.

Согласно отчету, каждая банда фокусируется на определенных отраслях и регионах мира. Банда Рюка / Конти атаковала 352 организации с 2018 года и 63 организации в этом году, сосредоточившись в основном на производственных, строительных и транспортных компаниях.

Десятки их жертв никогда не оглашались, но наиболее заметные организации, подвергшиеся нападению, включают школьный округ округа Бровард и французскую кубковую компанию CEE Schisler, обе из которых не заплатили непомерные выкупы, говорится в сообщении.

Помимо производства, в 2020 году группа произвела фурор для атак на ИТ-системы небольших правительств в США, таких как округ Джексон, Джорджия, Ривьера-Бич, Флорида, и округ ЛаПорт, штат Индиана. Все три местных правительства выплатили выкуп в размере от 130 000 до почти 600 000 долларов. Группа также провела большую часть 2020 года, нападая на местные больницы.

Как и банда Ryuk / Conti, люди, стоящие за вымогателем Sodin / REvil, также сосредоточены на медицинских организациях, а также направляют свои усилия на нападение на производителей ноутбуков. Из их 161 жертвы 52 пострадали в 2021 году, и они попали в международные новости из-за нападений на Acer и Quanta, двух крупнейших мировых производителей технологий.

Quanta, производящая ноутбуки Apple, получила требование выкупа в размере 50 миллионов долларов. Компания отказалась, и банда Sodin / REvil в ответ утекла в подробный дизайн продукта Apple. Согласно отчету, в котором отмечается, что с тех пор Apple не сообщала о вторжении, банда пригрозила утечкой дополнительных документов, но к маю удалила фотографии и любые другие упоминания об атаке.

DoppelPaymer / BitPaymer сделал себе имя, ориентируясь на государственные учреждения и школы. В декабре ФБР опубликовало уведомление специально о программе-вымогателе, отметив, что она используется для атаки на критически важные объекты инфраструктуры, такие как больницы и службы экстренной помощи.

В отчете также говорится, что большинство из 59 жертв группы в этом году не были публично идентифицированы, за исключением генеральной прокуратуры Иллинойса, которая подверглась нападению 29 апреля.

Банда Clop сосредоточила свои усилия на использовании широко известной уязвимости в системе передачи файлов Accellion. Команда eSentire и Мэйс объясняют, что группа широко использовала уязвимость, нанеся удар по Калифорнийскому университету, американскому банку Flagstar, глобальной юридической фирме Jones Day, канадскому производителю самолетов Bombardier, Стэнфордскому университету, голландскому нефтяному гиганту Royal Shell, Университету Колорадо, Университет Майами, заправочная компания RaceTrac и многие другие.

В отчете отмечается, что банда Clop стала печально известной тем, что якобы прочесывала файлы организации и связалась с клиентами или партнерами, чтобы потребовать от жертвы давления с целью выкупа.

Банда DarkSide в последнее время фигурирует в новостях об их нападении на Colonial Pipeline, которое вызвало политическую бурю в Соединенных Штатах и наезд на заправочные станции в некоторых городах на Восточном побережье.

Согласно отчету, эта группа является одной из новейших ведущих групп вымогателей, возникшей в конце 2020 года. Но они потратили мало времени, собрав 59 жертв с ноября и 37 жертв в этом году.

В отчете отмечается, что группа DarkSide - одна из немногих, кто действует как программа-вымогатель как услуга, перекладывая ответственность на подрядчиков, которые атакуют цели и разделяют выкуп. eSentire заявили, что их исследование показало, что люди, стоящие за DarkSide, не знали о колониальной атаке до того, как она произошла, и узнали об этом только из новостей. На прошлой неделе они произвели фурор, когда якобы прекратили все свои операции из-за усиленного контроля со стороны правоохранительных органов.

Программа-вымогатель была замешана в нескольких атаках на производителей энергии, таких как одна из крупнейших электроэнергетических

компаний Бразилии Companhia Paranaense de Energia, которую они атаковали в феврале.

Последняя изученная группа - это банда Аваддона, о которой на этой неделе рассказали в новостях из-за их атаки на крупную европейскую страховую компанию AXA. Атака примечательна тем, что AXA предоставляет киберстрахование десяткам компаний и пообещала прекратить возмещать своим клиентам во Франции уплаченные выкупы.

Помимо AXA, группа также атаковала 46 организаций в этом году и действует как программа-вымогатель как услуга, такая как DarkSide. В отчете объясняется, что банда примечательна включением часов обратного отсчета на своем сайте Dark Web и дополнительной угрозой DDoS-атаки в случае невыплаты выкупа.

В список их жертв входят медицинские организации, такие как Capital Medical Center в Олимпии, Вашингтоне и Bridgeway Senior Healthcare в Нью-Джерси.

Команда eSentire и Мэйс добавили, что огромное количество незарегистрированных атак указывает на то, что эти банды «сеют хаос против гораздо большего числа организаций, чем думает общественность».

«Еще одно отрезвляющее осознание того, что ни одна отрасль не застрахована от этого бедствия программ-вымогателей», - говорится в отчете. «Эти изнурительные атаки происходят во всех регионах и во всех секторах, и абсолютно необходимо, чтобы все компании и организации частного сектора внедрили средства защиты, чтобы уменьшить ущерб, причиненный атакой программы-вымогателя». ***(Jonathan Greig. More than 290 enterprises hit by 6 ransomware groups in 2021 // ZDNet (https://www.zdnet.com/article/more-than-290-enterprises-hit-by-6-ransomware-groups-in-2021/). 19.05.2021).***

***

«Некоторые профессионалы в области кибербезопасности хотят запретить жертвам программ-вымогателей платить хакерам за разблокировку их компьютерных систем. Они утверждают, что это единственный способ остановить волну изнурительных и все более наглых кибератак с целью получения прибыли.

Но такие запреты могут принести больше вреда, чем пользы, вынудив компании выйти из бизнеса, если они не смогут вернуться в онлайн, предупреждают другие эксперты. Они также могут поставить под угрозу жизни и средства к существованию, если больницы, школы и другие важные службы будут закрыты на несколько дней подряд.

«Это очень спорно», - сказал мне Джеймс Шэнк, главный архитектор общественных служб в фирме по кибербезопасности Team Cymru. «Некоторые люди категорически считают, что без бана проблему не решить. … С другой стороны, у вас есть жертвы, на которых действительно влияют программы-вымогатели, и их жизнеспособность как угроза для бизнеса».

Дебаты приобрели вновь обретенную актуальность на фоне множества разрушительных атак.

Атака программы-вымогателя на Colonial Pipeline привела к нехватке топлива в Соединенных Штатах и возникновению длинных очередей на заправочных станциях. В этом случае компания уступила и заплатила выкуп в размере 4,4 миллиона долларов - шаг, который генеральный директор Джозеф Блаунт назвал «правильным для страны» в интервью Wall Street Journal.

Между тем, представители системы здравоохранения Ирландии отказываются платить после атаки программы-вымогателя, которая заблокировала доступ к электронному сканированию и рентгеновским снимкам по всей стране.

Киберпреступники также становятся все более смелыми в своих требованиях. Как сообщает агентство Bloomberg News, хакеры, заблокировавшие сети CNA Financial Corp., одной из крупнейших страховых компаний страны, потребовали и получили гигантский выкуп в размере 40 миллионов долларов за разблокировку этих сетей в марте.

Правоохранительные органы США обычно призывали компании не платить выкуп, но никогда не пытались запретить такие выплаты.

Действия Конгресса после взлома колоний были сосредоточены на улучшении безопасности нефтегазовой инфраструктуры, а не на запрете платежей с использованием программ-вымогателей.

Президент Байден отказался комментировать на прошлой неделе решение Colonial о выплате выкупа хакерской группе, которая, по словам официальных лиц США, базируется в России, но не связана с правительством России.

Это вызвало насмешки со стороны некоторых республиканцев, которые использовали это, чтобы выставить президента слабым в киберпреступности…

Шэнк назвал запрет на платежи одним из самых спорных в сфере кибербезопасности.

Он был членом целевой группы по программам-вымогателям, состоящей из более чем 60 экспертов по кибербезопасности и бывших высокопоставленных правительственных чиновников, которая подготовила свой отчет в апреле - и особенно зашла в тупик в вопросе запрета выкупа.

Майкл Дэниел, координатор по кибербезопасности Белого дома при администрации Обамы, был одним из ведущих сторонников таких запретов на целевую группу и привел свои доводы в адрес Би-би-си : «Атаки программ-вымогателей в первую очередь мотивированы прибылью... и без прибыли злоумышленники уйдут от этого. тактика », - сказал он.

Банды программ-вымогателей также, вероятно, используют выкуп за гораздо более опасные преступления, «такие как торговля людьми, эксплуатация детей и терроризм», - предупредил Дэниел, который сейчас является президентом Cyber Threat Alliance.

Однако он предупредил, что запреты следует вводить медленно и осторожно, чтобы ограничить ущерб жертвам.

Джен Эллис, руководитель фирмы Rapid7, занимающейся кибербезопасностью, и еще один член целевой группы выступили против запретов.

«Запрет платежей почти наверняка приведет к довольно ужасной игре в «курицу», в которой преступники переключат все свое внимание на организации, которые с меньшей вероятностью смогут справиться с простоями - например,

больницы, водоочистные сооружения, поставщики энергии и школы», - сказала она. «Хакеры могут рассчитывать на вред обществу, причиненный этим временем простоя, чтобы оказать необходимое давление, чтобы гарантировать, что им заплатят. При этом они мало что теряют - и потенциально могут получить большую зарплату».

Группа действительно перечислила ряд изменений, которые правительства должны внести перед запретом платежей с использованием программ-вымогателей, если они захотят это сделать, в том числе создание государственных фондов, чтобы помочь жертвам оправиться от атак, не опустошая их собственные банковские счета, и поэтапное введение запретов, чтобы они касались большинства критически важные службы в последнюю очередь.

Со своей стороны, Шэнк сказал, что он «видит обе стороны проблемы» и считает, что правоохранительным органам лучше сосредоточиться на том, чтобы усложнить работу банд вымогателей и потратить платежи, которые они обычно получают в криптовалюте, чем полностью запретить выкуп…» ***(Joseph Marks. The Cybersecurity 202: Cybersecurity pros are split on banning ransomware payments // The Washington Post (https://www.washingtonpost.com/politics/2021/05/21/cybersecurity-202-cybersecurity-pros-are-split-banning-ransomware-payments/). 21.05.2021).***

***

«Страховая компания Донкастера пострадала от программы-вымогателя от команды Darkside, чей «пресс-релиз», в котором говорилось о прекращении деятельности на прошлой неделе, был воспринят некоторыми экспертами за чистую монету.

The Doncaster Free Press сообщает, что неделю назад компания Darkside взломала страховую компанию One Call Insurance, базирующуюся в северном английском городе.

Ссылаясь на известную записку о выкупе «добро пожаловать в темную сторону» банды вымогателей, местная газета сообщила: «На экране появилось сообщение от хакеров, в котором говорится, что если они не получат 15 миллионов фунтов стерлингов, имеющиеся у них данные будут обнародованы. включая все данные клиентов, такие как пароли и банковские реквизиты».

One Call сообщил The Register : «13 мая у нас начались некоторые нарушения в работе наших ИТ-систем, и мы немедленно наняли специальную группу экспертов-криминалистов в области ИТ, чтобы они помогли восстановить наши системы и расследовать случившееся. совершенно новая и безопасная среда, что означает, что все существующие клиенты получают нормальную поддержку».

Это произошло всего через несколько дней после первоначального компрометации Colonial Pipeline 7 мая и за день до того, как банда вымогателей заявила о закрытии магазина.

Пресс-секретарь One Call добавила: «Специалисты подтвердили, что нарушение было результатом атаки вымогателя, совершенной преступной организацией, которая находится под следствием властей».

Сообщается, что расследованию помогает судебно-медицинская ИТ-компания. Несмотря на то, что это произошло неделю назад, страховщик сообщил The Register, что еще не знает, «были ли затронуты какие-либо данные в результате инцидента».

ICO знает об атаке, как и регуляторы страховой отрасли, сообщил One Call, добавив: «Мы приносим свои извинения за временный сбой и любое вызванное разочарование».

Разве преступники не закрылись?

Darkside - это преступная группировка вымогателей, нацеленная на американскую компанию Colonial Pipeline, оператора нефтепровода на восточном побережье Америки, который поставлял чуть менее половины ежедневных потребностей региона в переработке нефти.

После этой атаки и яростного ответа со стороны США Darkside использовала свой размещенный в Tor репозиторий украденных данных, чтобы объявить о прекращении своей деятельности, как сообщил всему миру блог, связанный с информационной фирмой Recorded Future.

Это было преждевременно: как многие предполагали, Darkside, похоже, использовала яростные обещания США возмездия, чтобы отключить свою публично известную инфраструктуру (и унесла с собой криптовалюту на несколько десятков миллионов долларов), продолжая при этом свою преступную деятельность, поскольку Случай One Call предполагает.

По данным информационной компании Crowdstrike, еще в марте вымогатель Darkside был нацелен на гипервизоры VMware ESXi. Исследователи считали, что операторы Darkside в этом случае были хорошо зарекомендовавшей себя преступной бригадой, известной как Carbon Spider, также известной как Carbanak.

Эта банда действует с середины 2010-х годов, наиболее заметно притащив заявленные 300 миллионов долларов в период до 2015 года с помощью одноименного банковского вредоносного ПО». ***(Gareth Corfield. Doncaster insurance firm One Call hit by not-dead-at-all Darkside ransomware gang // The Register (https://www.theregister.com/2021/05/21/darkside_ransomware_doncaster/). 21.05.2021).***

***

«С тех пор, как неделю назад работа программы-вымогателя DarkSide была закрыта, несколько аффилированных лиц жаловались на то, что им не платят за прошлые услуги, и предъявили претензию на биткойны в условном депонировании на форуме хакеров.

Русскоязычные киберпреступные сообщества обычно имеют систему условного депонирования, чтобы избежать мошенничества между продавцами и покупателями. Для операций с программами-вымогателями депозит является четким указанием на то, что они имеют в виду большой бизнес.

Чтобы завоевать доверие потенциальных партнеров и расширить свою деятельность, DarkSide разместила 22 биткойна на популярном хакерском форуме XSS. Кошелек управляется администратором сайта, который в данном случае выступает гарантом для банды и арбитром в случае возникновения спора.

В прошлом году программа-вымогатель REvil разместила биткойны на сумму 1 миллион долларов на другом хакерском форуме, чтобы привлечь к операции новых участников. Этот шаг показал, что они доверяли администратору форума деньги и что можно было заработать много денег.

На прошлой неделе DarkSide закрыла магазин и сообщила филиалам, что решение было принято после потери доступа к их публичным серверам, и это было « из-за давления со стороны США » после атаки на Colonial Pipeline.

Невыплаченные долги

Прекращение деятельности программы-вымогателя как услуги (RaaS) DarkSide было внезапным и явно оставило некоторые незавершенные дела. Пять партнеров пожаловались на то, что операторы задолжали им деньги за уплаченный выкуп или за услуги взлома:

Первый партнер, запросивший претензию, заявил, что они были «пентестером» атаки и получили 80% выкупа. Однако после того, как жертва заплатила, операторы DarkSide заявили, что у них больше нет доступа к средствам, и партнер может использовать депозит в XSS для получения платежа.

Второй партнер заявляет, что у них были биткойны, оставленные для них на партнерском портале, но им пришлось поспешить к своим родственникам, прежде чем они могли потребовать их.

Третий филиал заявляет, что они тоже были «пентестерами» и получили выкуп прямо перед закрытием работы DarkSide. Этот партнер заявляет, что отправил подтверждение администратору XSS.

Четвертый филиал заявляет, что они работали над корпоративными нарушениями, но так и не получили свой последний платеж в размере 150 000 долларов.

Пятый и последний партнер заявляет, что им было перечислено 72000 долларов на партнерском портале, но они не смогли получить их до закрытия операции по состоянию здоровья.

В случае первого иска, поданного 14 марта, администратор форума, выступающий в качестве арбитра, утвердил компенсацию из депозита DarkSide. Они также просили других выступить, если у них есть причина.

Через четыре дня появилась вторая претензия, а затем еще три - 19 и 20 марта. Ни на одну из них ответа от администратора форума не последовало…

Даже если DarkSide закроется, жертвы вымогают. Аффилированные лица получили соответствующие ключи дешифрования, чтобы продолжить переговоры с компаниями-жертвами отдельно». ***(Ionut Ilascu. DarkSide affiliates claim gang's bitcoin deposit on hacker forum // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/darkside-affiliates-claim-gangs-bitcoin-deposit-on-hacker-forum/). 21.05.2021).***

***

«QNAP рекомендует клиентам обновить приложение аварийного восстановления HBS 3, чтобы блокировать атаки программ-вымогателей Qlocker, нацеленных на их подключенные к Интернету устройства сетевого хранения (NAS).

«Программа-вымогатель, известная как Qlocker, использует CVE-2021-28799 для атаки на QNAP NAS с определенными версиями HBS 3 (Hybrid Backup Sync)», - говорится в сообщении по безопасности, выпущенном тайваньским производителем устройств NAS.

«Чтобы предотвратить заражение Qlocker, мы рекомендуем обновить HBS 3 до последней версии».

Массивные вымогатели кампания Qlocker начала пробивать брешь устройства QNAP NAS в течение недели 19 апреля, заменив файлы жертв с защищенным паролем 7-Zip архивами.

Хотя в то время вектор атаки не был известен, QNAP теперь подтвердила, что злоумышленники злоупотребляли уязвимостью с жестко закодированными учетными данными CVE-2021-28799.

Эта уязвимость безопасности действует как бэкдор-аккаунт, позволяя злоумышленникам получить доступ к устройствам с устаревшими версиями HBS 3 (Hybrid Backup Sync).

QNAP добавил, что CVE-2021-28799 уже исправлена в следующих версиях HBS 3 (HBS 2 и HBS 1.3 не затронуты):

QTS 4.5.2: HBS 3 v16.0.0415 и новее

QTS 4.3.6: HBS 3 v3.0.210412 и новее

QTS 4.3.3 и 4.3.4: HBS 3 v3.0.210411 и новее

QuTS hero h4.5.1: HBS 3 v16.0.0419 и новее

QuTScloud c4.5.1 ~ c4.5.4: HBS 3 v16.0.0419 и новее

Несмотря на то, что это не первый раз, когда QNAP упоминает об эксплойтах Qlocker, нацеленных на бэкдор-аккаунт HBS 3, компания впервые связывает этот недостаток с основным вектором атаки кампании.

Предупреждение, которое приходит слишком поздно

К сожалению, для клиентов QNAP, нацеленных на кампанию вымогателей Qlocker, это предупреждение поступило слишком поздно, поскольку злоумышленники, стоящие за этими атаками, уже остановили натиск.

Однако это произошло только после вымогательства у сотен пользователей QNAP и ограбления у них 350 000 долларов в течение одного месяца после того, как они заставили их заплатить выкуп в размере 0,01 биткойна (что на тот момент составляло примерно 500 долларов США), чтобы получить пароль для своих файлов.

Отчеты о жертвах в нашей теме поддержки Qlocker и тесты BleepingComputer подтвердили, что все сайты Qlocker Tor больше не доступны, а жертвы, у которых были хранилища файлов NAS в архивах, защищенных паролем, больше не имели возможности платить выкуп.

Пока не ясно, что вызвало внезапное закрытие Qlocker, но можно сказать наверняка, что он следует постоянной тенденции, которая началась после того, как DarkSide поразил системы Colonial Pipeline.

Неудачная атака программы-вымогателя DarkSide привела к усилению давления со стороны правоохранительных органов США на аналогичные киберпреступные операции. Как прямой результат, банды вымогателей начали

либо полностью отключаться, либо ограничивать свои цели выходом из поля зрения правоохранительных органов.

Хотя программа-вымогатель Qlocker могла выключиться, это не единственная программа-вымогатель, нацеленная в настоящее время на устройства QNAP NAS.

В течение последних нескольких недель клиентов QNAP также призвали защитить свои устройства от новых кампаний вымогателей Agelocker и eCh0raix.

Клиентам, которые хотят дополнительно защитить свои NAS-устройства от атак, рекомендуется применять следующие передовые методы». ***(Sergiu Gatlan. QNAP confirms Qlocker ransomware used HBS backdoor account // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/qnap-confirms-qlocker-ransomware-used-hbs-backdoor-account/). 21.05.2021).***

***

«Программа-вымогатель MountLocker теперь использует корпоративные API-интерфейсы Windows Active Directory для проникновения через сети.

MountLocker начал работать в июле 2020 года как программа-вымогатель как услуга (RaaS), где разработчики отвечают за программирование программного обеспечения для вымогателей и платежного сайта, а аффилированные лица нанимаются для взлома предприятий и шифрования их устройств.

В рамках этой договоренности основная команда MountLocker получает меньшую долю в размере 20-30% от суммы выкупа, а аффилированное лицо получает остальную часть.

В марте 2021 года появилась новая группа вымогателей под названием Astro Locker, которая начала использовать настроенную версию вымогателя MountLocker с примечаниями о выкупе, указывающими на их собственные сайты платежей и утечки данных.

«Это не ребрендинг, вероятно, мы можем определить его как альянс», - сказал Astro Locker BleepingComputer, когда мы спросили об их связи с MountLocker.

Наконец, в мае 2021 года появилась третья группа под названием XingLocker, которая также использует настроенный исполняемый файл вымогателя MountLocker.

MountLocker проникает на другие устройства

На этой неделе команда MalwareHunterTeam поделилась образцом того, что считается новым исполняемым файлом MountLocker, который содержит новую функцию червя, которая позволяет ему распространяться и шифровать на другие устройства в сети.

После установки образца BleepingComputer подтвердил, что это был адаптированный образец для команды XingLocker.

Краткий анализ, проведенный BleepingComputer, показал, что вы можете включить функцию червя, запустив образец вредоносной программы с аргументом командной строки / NETWORK. Поскольку для этой функции требуется домен Windows, наши тесты быстро завершились неудачно…

После обмена образцом с генеральным директором Advanced Intel Виталием Кремезом было обнаружено, что MountLocker теперь использует API интерфейсов служб Windows Active Directory как часть своей функции червя.

Программа-вымогатель сначала использует функцию NetGetDCName () для получения имени контроллера домена. Затем он выполняет запросы LDAP к ADS контроллера домена с помощью функции ADsOpenObject () с учетными данными, переданными в командной строке.

После подключения к службам Active Directory он будет перебирать базу данных для объектов «objectclass = computer», как показано на изображении выше.

Для каждого найденного объекта MountLocker попытается скопировать исполняемый файл программы-вымогателя в папку «\ C $ \ ProgramData» удаленного устройства.

Затем программа-вымогатель удаленно создаст службу Windows, которая загружает исполняемый файл, чтобы продолжить шифрование устройства.

Используя этот API, программа-вымогатель может найти все устройства, которые являются частью взломанного домена Windows, и зашифровать их, используя украденные учетные данные домена.

«Многие корпоративные среды полагаются на сложные леса активных каталогов и компьютер в то время. Теперь MountLocker - первая известная программа-вымогатель, которая использует уникальные корпоративные архитектурные идеи для выявления дополнительных целей для операций шифрования вне обычной сети и сканирования общих ресурсов», - сказал Кремез BleepingComputer в разговоре о вредоносном ПО.

«Это качественный сдвиг в профессиональной разработке программ-вымогателей для эксплуатации корпоративных сетей».

Поскольку сетевые администраторы Windows обычно используют этот API, Кремез считает, что злоумышленник, добавивший этот код, вероятно, имеет некоторый опыт администрирования домена Windows».

Хотя этот API был замечен в других вредоносных программах, таких как TrickBot, это может быть первая «корпоративная программа-вымогатель для профессионалов», использующая эти API для выполнения встроенной разведки и распространения на другие устройства». ***(Lawrence Abrams. MountLocker ransomware uses Windows API to worm through networks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/mountlocker-ransomware-uses-windows-api-to-worm-through-networks/). 19.05.2021).***

***

«Новая операция вымогателей, известная как Lorenz, нацелена на организации по всему миру с помощью специализированных атак, требующих выкупа в сотни тысяч долларов.

Банда программ-вымогателей Lorenz начала свою деятельность в прошлом месяце и с тех пор накопила растущий список жертв, чьи украденные данные были опубликованы на сайте утечки данных программ-вымогателей.

Майкл Гиллеспи из ID Ransomware сообщил BleepingComputer, что шифровальщик-вымогатель Lorenz аналогичен предыдущей операции, известной как ThunderCrypt.

Неясно, принадлежит ли Lorenz той же группе или приобрел исходный код программы-вымогателя для создания своего собственного варианта.

Запущен сайт утечки данных для вымогательства жертв

Как и другие атаки программ-вымогателей, управляемые человеком, Lorenz проникнет в сеть и распространится на другие устройства, пока они не получат доступ к учетным данным администратора домена Windows.

Распространяясь по системе, они будут собирать незашифрованные файлы с серверов жертв, которые они загружают на удаленные серверы, находящиеся под их контролем.

Эти украденные данные затем публикуются на специальном сайте утечки данных, чтобы заставить жертв заплатить выкуп или продать данные другим злоумышленникам.

На этом сайте утечки данных Lorenz в настоящее время перечислены двенадцать жертв, при этом данные обнародованы по десяти из них.

Когда банда Lorenz публикует данные, они действуют несколько иначе, чем другие банды вымогателей.

Чтобы заставить жертв заплатить выкуп, Lorenz сначала делает данные доступными для продажи другим злоумышленникам или возможным конкурентам. Со временем они начинают выпускать защищенные паролем архивы RAR, содержащие данные жертвы.

В конечном итоге, если выкуп не выплачивается и данные не приобретаются, Lorenz выпускает пароль для архивов утечки данных, так что они становятся общедоступными для всех, кто загружает файлы.

Еще одна интересная особенность, которую нельзя увидеть на других сайтах утечки данных, - это то, что Lorenz продает доступ к внутренней сети жертвы вместе с данными.

Для некоторых злоумышленников доступ к сетям может быть более ценным, чем сами данные.

Шифровальщик Лоренца

По образцам вымогателя Lorenz, обнаруженным BleepingComputer, злоумышленники настраивают исполняемый файл вредоносной программы для конкретной организации, на которую они нацелены.

В одном из примеров, предоставленных BleepingComputer, программа-вымогатель выдаст следующие команды для запуска файла с именем ScreenCon.exe из того, что выглядит как контроллер домена локальной сети.

При шифровании файлов программа-вымогатель использует шифрование AES и встроенный ключ RSA для шифрования ключа шифрования. Для каждого зашифрованного файла к имени файла будет добавлено расширение.Lorenz.sz40 …

В отличие от других программ-вымогателей, ориентированных на предприятия, рассматриваемый нами образец Lorenz не убивал процессы и не завершал работу служб Windows перед шифрованием.

В каждой папке на компьютере будет записка с требованием выкупа HELP_SECURITY_EVENT.html, содержащая информацию о том, что случилось с файлами жертвы. Он также будет включать ссылку на сайт утечки данных Lorenz и ссылку на уникальный сайт оплаты Tor, где жертва может увидеть свое требование выкупа.

У каждой жертвы есть специальный сайт оплаты Tor, который включает в себя требование выкупа в биткойнах и форму чата, в которой жертвы могут вести переговоры с злоумышленниками.

Судя по запискам о выкупе, которые видел BleepingComputer, Lorenz требует выкупа от 500000 до 700000 долларов. В более ранних версиях вымогателя требовался выкуп в размере миллиона долларов, но неясно, были ли они связаны с той же операцией.

В настоящее время программа-вымогатель анализируется на наличие слабых мест, и BleepingComputer не рекомендует жертвам платить выкуп до тех пор, пока не будет определено, может ли бесплатный дешифратор бесплатно восстанавливать файлы». ***(Lawrence Abrams. Meet Lorenz — A new ransomware gang targeting the enterprise // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/meet-lorenz-a-new-ransomware-gang-targeting-the-enterprise/). 13.05.2021).***

***

«Команда разработчиков Exploit, крупного форума по борьбе с киберпреступностью, используемого бандами вымогателей для найма партнеров и рекламы своих услуг Ransomware-as-a-Service (RaaS), объявила, что реклама программ-вымогателей теперь запрещена и будет удалена.

Этот шаг последовал за объявлением, сделанным вчера русскоязычным хакерским форумом XSS, о том, что темы программ-вымогателей навсегда запрещены.

Exploit утверждает, что это решение было принято потому, что группы программ-вымогателей, атакующие цели без разбора, привлекают «большое внимание».

Помимо запрета, администраторы форума также удалят все темы, связанные с операциями с программами-вымогателями и всеми партнерскими программами.

Полный текст заявления, предоставленный и переведенный Елисеем Богуславским и Виталием Кремезом из Advanced Intel, доступен ниже.

Good day,

We are glad to see pentesters, malware specialists, coders, but we are not happy with lockers - they attract a lot of attention. This type of activity is not good to us in view of the fact that networks are locked indiscriminately we do not consider it appropriate for RaaS partner programs to be present on our forum.

It was decided to remove all affiliate programs and prohibit them as a type of activity on our forum.

All topics related to lockers will be deleted.

Банды программ-вымогателей уже выразили свое неодобрение после того, как XSS опубликовал свое решение запретить им доступ на форумах. Например, банда вымогателей REvil объявила, что операция перейдет на Exploit.

REvil добавил, что банда перейдет на частную платформу в течение недели. Однако они должны быть намного быстрее, поскольку Exploit также запретил темы, связанные с программами-вымогателями, чтобы избежать нежелательного внимания со стороны правоохранительных органов США.

Поскольку все больше киберпреступников и хакерских сообществ вытесняют операции с программами-вымогателями со своих платформ, еще неизвестно, как и если банды RaaS будут продолжать продвигать свою деятельность и привлекать новых партнеров.

DarkSide прекращает работу RaaS

Exploit и XSS реагируют на усиление давления на банды RaaS, которые ранее использовали два форума, включая REvil, LockBit, DarkSide, Netwalker и Nefilim.

Это прямой результат того, что они оказались под прицелом правоохранительных органов после атаки программы-вымогателя DarkSide на Colonial Pipeline, которая нарушила работу топливопровода США.

Об атаке также рассказывалось в Белом доме на брифингах по национальной безопасности на этой неделе, и на этой неделе было объявлено чрезвычайное положение в регионе, затронувшее 17 штатов и округ Колумбия.

После инцидента банда вымогателей DarkSide опубликовала «пресс-релиз», в котором говорилось, что они аполитичны и начнут проверять все цели перед атаками.

Colonial Pipeline с тех пор восстановила все операции конвейера после того, как, как сообщается, заплатила DarkSide почти 5 миллионов долларов криптовалюты за ключ дешифрования.

UNKN, злоумышленник, известный как публичный представитель конкурирующей банды вымогателей REvil, также объявил сегодня о прекращении работы DarkSide RaaS после потери доступа к общедоступному сайту утечки данных, платежным серверам и серверам CDN "по требованию закона. агентств "и перевод их криптовалюты на неизвестный кошелек.

DarkSide подтвердила утверждения UNKN в сообщении, отправленном их филиалам RaaS, в котором говорилось, что они решили закрыть свою деятельность «из-за давления со стороны США» и потеряли доступ к своим публичным серверам.

После закрытия DarkSide REvil объявил о новых ограничениях на цели, которые могут быть зашифрованы аффилированными лицами.

В UNKN сообщили, что филиалы REvil теперь должны получать разрешение, прежде чем нацеливаться на организацию, и что:

1. Запрещается работа в социальной сфере (здравоохранение, учебные заведения);

2. Запрещается работать в гос-секторе (государстве) любой страны». ***(Sergiu Gatlan. Ransomware ads now also banned on Exploit cybercrime forum // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ransomware-ads-now-also-banned-on-exploit-cybercrime-forum/). 14.05.2021).***

***

«Поскольку разрушительные атаки программ-вымогателей продолжают иметь далеко идущие последствия, компании по-прежнему стараются скрыть атаки, а не быть прозрачными. Ниже мы выделяем реакцию компании на атаку, которую следует использовать в качестве модели для раскрытия информации в будущем.

5 мая поставщик технологий экологически чистой энергии Volue подвергся атаке программы-вымогателя Ryuk, которая затронула некоторые из их клиентских клиентских платформ.

С тех пор Volue открыто заявляет о кибератаке, предоставляя веб-трансляции, ежедневные обновления, а также адреса электронной почты и номера телефонов для своих генеральных и финансовых директоров, которые могут задать вопросы об атаке.

Кроме того, компания заявляет, что они поделились всеми признаками компрометации с KraftCert, норвежской группой реагирования на компьютерные чрезвычайные ситуации, чтобы предупредить другие компании и правоохранительные органы.

Прозрачность Volue резко контрастирует с раскрытием информации, обычно наблюдаемым при атаках программ-вымогателей, и должна использоваться в качестве модели для раскрытия информации в будущем.

Эта прозрачность не осталась незамеченной профессионалами в области кибербезопасности, которые высоко оценивают реакцию Volue на атаку.

Многие сравнивают прозрачность Volue с Norsk Hydro, другой норвежской компанией, которая также заслужила уважение тем, как она справилась с атакой программы-вымогателя LockerGoga в 2019 году.

Хотя BleepingComputer обычно покрывает атаки вымогателей Volue, они были настолько прозрачными и подробными, что нам нечего добавить.

Прозрачность выглядит лучше, а не хуже

Прозрачность защищает ваших клиентов и сотрудников, вселяет доверие в вашу компанию и помогает правоохранительным органам, однако немногие компании предпочитают быть прозрачными.

Вместо этого почти каждая жертва программы-вымогателя сначала пытается скрыть атаку из опасения, что она может нанести репутационный или юридический ущерб.

В конечном итоге истинная природа атаки раскрывается после того, как будет обнаружен образец или заметка вредоносного ПО, или после того, как банды вымогателей публикуют данные, украденные во время атаки.

Сотрудники взломанных компаний рассказали BleepingComputer, что их работодатели отрицали атаку или что данные были украдены, пока банды вымогателей не опубликовали файлы.

Из-за непрозрачности с самого начала клиенты, сотрудники и деловые партнеры жертвы подвергаются большему риску, поскольку им не предоставляется подробное предупреждение о том, что было украдено.

Прозрачность также позволяет взломанным компаниям помогать правоохранительным органам в их расследованиях и предотвращать дальнейшие атаки.

Наконец, прозрачность вселяет в ваших сотрудников, клиентов и инвесторов уверенность в том, что компания правильно реагирует на атаку и что беспокоиться не о чем.

Компании призвали сообщать об атаках программ-вымогателей

ФБР призвало жертв сообщать об атаках программ-вымогателей, чтобы они могли получать свежие IOC (индикаторы компрометации) об операции вымогателя.

Когда организация подвергается атаке, для правоохранительных органов критически важно быстро получать известные IP-адреса, файлы и домены, используемые злоумышленниками, для немедленного анализа и использования в рамках своих расследований.

Чем дольше бизнес ждет, чтобы предоставить правоохранительным органам IOC, тем менее полезными они становятся, поскольку злоумышленники скрывают свои следы или удаленные сайты закрываются.

Зачем позволять бандам вымогателей контролировать повествование, если вы можете контролировать его сами, оставаясь прозрачными?» ***(Lawrence Abrams. Ransomware victim shows why transparency in attacks matters // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ransomware-victim-shows-why-transparency-in-attacks-matters/). 17.05.2021).***

***

«Банда Cuba Ransomware объединилась с операторами рассылки вредоносного ПО Hancitor, чтобы упростить доступ к взломанным корпоративным сетям.

Загрузчик Hancitor (Chancitor) работает с 2016 года, когда Zscaler обнаружил, что он распространяет троян Vawtrak, ворующий информацию. С тех пор на протяжении многих лет было замечено множество кампаний, в которых Hancitor устанавливает программы для кражи паролей, такие как Pony, Ficker, а с недавних пор - Cobalt Strike.

Hancitor обычно распространяется через вредоносные спам-кампании, выдавая себя за счета DocuSign…

Когда получатель нажимает ссылку «Подписать документ», он загружает вредоносный документ Word, который пытается убедить цель отключить защиту.

После отключения защиты запускаются вредоносные макросы для загрузки и установки загрузчика Hancitor.

Куба-вымогатель объединилась с Hancitor

Подобно тому, как Рюк и Конти сотрудничали с TrickBot, а Egregor и ProLock работали с QBot, Cuba Ransomware заключил партнерство с Hancitor, чтобы получить доступ к взломанным сетям.

В новом отчете компании по кибербезопасности Group-IB исследователи обнаружили, что недавние кампании Hancitor сбрасывали маяки Cobalt Strike на зараженные компьютеры.

Cobalt Strike - это законный набор инструментов для тестирования на проникновение, который использует развернутые маяки или клиенты на скомпрометированных устройствах для удаленного «создания оболочек, выполнения сценариев PowerShell, выполнения эскалации привилегий или создания нового сеанса для создания прослушивателя в системе жертвы».

Банды программ-вымогателей обычно используют взломанные версии Cobalt Strike как часть своих атак, чтобы закрепиться и распространиться по сети.

Исследователи Group-IB говорят, что после развертывания маяков Cobalt Strike злоумышленники используют этот удаленный доступ для сбора сетевых учетных данных, информации о домене и распространения по сети.

«Возможности Beacon также использовались для сканирования скомпрометированной сети. Кроме того, группа использовала некоторые специальные инструменты для сетевой разведки. Первый инструмент называется Netping - это простой сканер, способный собирать информацию о живых хостах в сети и сохранять ее. в текстовый файл, другой инструмент, Protoping, для сбора информации о доступных сетевых ресурсах».

«Встроенные инструменты также подвергались злоупотреблениям. Например, злоумышленник использовал команду net view для сбора информации о хостах в сети и утилиту nltest для сбора информации о взломанном домене», - поясняет Group-IB в опубликованном сегодня отчете.

Для горизонтального перемещения с машины на машину злоумышленники используют удаленный рабочий стол, а в случае обнаружения их маяков Cobalt Strike - через другие вредоносные программы-бэкдоры, такие как SystemBC.

«Ficker stealer был не единственным публично рекламируемым инструментом в арсенале злоумышленников. Другой инструмент, который становится все более популярным среди различных операторов программ-вымогателей - SystemBC. Такие дополнительные бэкдоры позволяли злоумышленникам загружать и выполнять дополнительные полезные нагрузки, даже если Cobalt Забастовки были обнаружены и заблокированы», - предупреждают исследователи.

При перемещении по сети незашифрованные данные собираются и отправляются на удаленные серверы под контролем злоумышленника для использования в рамках стратегии двойного вымогательства.

Когда участники, наконец, получают доступ к учетным данным администратора домена, они развертывают исполняемый файл программы-вымогателя через PsExec для шифрования устройств в сети.

Партнерство может ускорить атаки

С момента запуска в конце 2019 года Cuba Ransomware не проявляет особой активности по сравнению с другими операциями, такими как REvil, Avaddon, Conti и DoppelPaymer.

На момент написания они опубликовали данные по девяти компаниям на своем сайте утечки данных.

Их наиболее разрекламированная атака была направлена на ATFS, широко используемый платежный процессор для органов местного самоуправления и правительства штата.

Поскольку их атаки теперь подпитываются кампаниями по рассылке спама, мы должны ожидать скорого увеличения числа жертв.

Следует также отметить, что, хотя Cuba Ransomware использует изображение Фиделя Кастро и названо в честь страны Куба, в отчете фирмы Profero, занимающейся кибербезопасностью, говорится, что они базируются за пределами России. Это связано с тем, что Проферо обнаружил русский язык на сайте утечки данных банды и во время переговоров». ***(Lawrence Abrams. Cuba Ransomware partners with Hancitor for spam-fueled attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/cuba-ransomware-partners-with-hancitor-for-spam-fueled-attacks/). 07.05.2021).***

***

«Федеральное бюро расследований (ФБР) и Австралийский центр кибербезопасности (ACSC) предупреждают о продолжающейся кампании вымогателей Avaddon, нацеленной на организации из широкого спектра секторов в США и во всем мире.

ФБР сообщило в сообщении TLP: GREEN flash alert на прошлой неделе, что филиалы по вымогательству Avaddon пытаются взломать сети производственных, медицинских и других организаций частного сектора по всему миру.

Сегодня ACSC расширил информацию о таргетинге, заявив, что филиалы банды вымогателей нацелены на организации из широкого спектра секторов, включая, помимо прочего, правительство, финансы, правоохранительные органы, энергетику, информационные технологии и здравоохранение.

В то время как ФБР только упоминает о продолжающихся атаках, ACSC также предоставляет список стран, подвергшихся атаке, включая США, Великобританию, Германию, Китай, Бразилию, Индию, ОАЭ, Францию и Испанию, и это лишь некоторые из них.

«Австралийский центр кибербезопасности (ACSC) осведомлен о продолжающейся кампании вымогателей с использованием вредоносного ПО Avaddon Ransomware [..], активно нацеленного на австралийские организации в различных секторах», - добавили в ACSC [PDF].

«ACSC известно о нескольких случаях, когда программа-вымогатель Avaddon напрямую влияла на организации в Австралии».

ФБР: Avaddon создает пустые DDoS-угрозы

ACSC также упоминает злоумышленников Avaddon, которые угрожают атаками типа «отказ в обслуживании» (DDoS), чтобы убедить жертв заплатить выкуп (в дополнение к утечке украденных данных и шифрованию их системы).

Однако, как заявило ФБР, никаких доказательств DDoS-атак после атак вымогателя Avaddon обнаружено не было.

Группа вымогателей Avaddon впервые объявила в январе 2021 года, что они будут запускать DDoS-атаки для уничтожения сайтов или сетей жертв, пока они не обратятся к ним и не начнут переговоры о выплате выкупа.

BleepingComputer впервые сообщил об этой новой тенденции в октябре 2020 года, когда группы программ-вымогателей начали использовать DDoS-атаки против своих жертв в качестве дополнительного рычага воздействия.

В то время двумя операциями вымогателей, которые использовали эту новую тактику, были SunCrypt и RagnarLocker.

Украденные данные используются в качестве кредитного плеча

Образцы программ-вымогателей Avaddon были впервые обнаружены в феврале 2019 года, а в июне 2020 года компания начала привлекать аффилированных лиц после того, как запустила массовую спамерскую кампанию, нацеленную на пользователей по всему миру.

Аффилированные лица, которые присоединяются к этой операции RaaS, несут ответственность за компрометацию сетей для развертывания полезных нагрузок или распространения программ-вымогателей через спам или наборы эксплойтов. В то же время его операторы несут ответственность за разработку вредоносного ПО и работу сайта оплаты TOR.

Операция Avaddon RaaS также требует от филиалов следовать набору правил, одно из которых - не преследовать цели из Содружества Независимых Государств (СНГ).

Avaddon выплачивает каждому партнеру 65% выкупа, который они вносят, при этом операторы получают долю в 35%. Однако, как и в случае с другими программами RaaS, более крупные филиалы обычно могут договариваться о более высокой доле доходов в зависимости от размера своих атак.

Средняя сумма выкупа, которую требуют филиалы Avaddon, составляет примерно 0,73 биткойна (примерно 41 000 долларов США) в обмен на инструмент дешифрования (Avaddon General Decryptor).

Филиалы программы-вымогателя Avaddon также известны тем, что крадут данные из сетей своих жертв, прежде чем шифровать системы для двойного вымогательства.

Эта стратегия стала обычным явлением почти для всех активных операций с программами- вымогателями, когда жертвы обычно уведомляют своих клиентов или сотрудников о возможных утечках данных после атак программ-вымогателей». ***(Sergiu Gatlan. US and Australia warn of escalating Avaddon ransomware attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/us-and-australia-warn-of-escalating-avaddon-ransomware-attacks/). 10.05.2021).***

***

«Город Талса, штат Оклахома, подвергся атаке с использованием программ-вымогателей, в результате чего городские власти отключили свои системы, чтобы предотвратить дальнейшее распространение вредоносного ПО.

Талса - второй по величине город в Оклахоме с населением около 400 000 человек.

В минувшие выходные злоумышленники развернули атаку с использованием программ-вымогателей на сеть города Талса, в результате чего городские власти отключили все свои системы и нарушили работу онлайн-сервисов.

«Мы обнаружили вредоносное ПО на наших серверах, и как только мы это сделали, с большой осторожностью, мы отключили все наши системы». Об этом сообщил местным СМИ в интервью KRMG мэр Талсы Г.Т. Байнум.

Байнум говорит, что сотрудники вернулись к работе, и инцидент не повлиял на работу служб 911 или службы экстренной помощи.

Однако отключение городских систем лишает жителей доступа к онлайн-системам оплаты счетов, выставлению счетов за коммунальные услуги и услугам по электронной почте. Веб-сайты города Талса, городского совета Талсы, полиции Талсы и веб-сайта 311 Талсы также не работают.

Городские телефонные системы работают, и любой, кому нужно вести дела с городскими властями, может сделать это по телефону.

В сообщении на Facebook городские власти заявляют, что информация о клиентах не была скомпрометирована. Поскольку большинство программ-вымогателей крадут данные перед развертыванием своих программ-вымогателей, некоторое количество файлов было украдено.

"Город Талса испытывает технические трудности со многими внешними программами, которые помогают обслуживать жителей Талсы из-за атаки программы-вымогателя. Информация о клиентах не собрана, но жители не смогут получить доступ к веб-сайтам города, и будут задержки в сетевых служб», - говорится в сообщении на странице департамента полиции Талсы в Facebook.

Программы-вымогатели стали бичом для интересов США: новые атаки раскрываются ежедневно, а жертвы платят выкуп в миллионы долларов.

Чтобы помочь бороться с растущей угрозой программ-вымогателей, была создана Целевая группа по программам-вымогателям, которая анализирует проблему и предоставляет законодателям рекомендуемые решения.

Эти решения варьируются от обязательного раскрытия выкупа до согласованных на международном уровне усилий по предотвращению атак программ-вымогателей и реагированию на них.

Атаки на критически важную инфраструктуру также стали серьезной проблемой в свете кибератаки на крупнейший в США топливопровод, совершенной на прошлой неделе бандой вымогателей DarkSide». ***(Lawrence Abrams. City of Tulsa's online services disrupted in ransomware incident // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/city-of-tulsas-online-services-disrupted-in-ransomware-incident/). 10.05.2021).***

***

«Попытка студента украсть дорогостоящее программное обеспечение для визуализации данных привела к полномасштабной атаке программы-вымогателя Ryuk на европейский институт биомолекулярных исследований.

BleepingComputer давно предостерегает от взломов программного обеспечения не только потому, что они незаконны, но и потому, что они являются частым источником заражения вредоносными программами.

Злоумышленники обычно создают поддельные сайты для загрузки программ взлома, видеоролики на YouTube и торренты для распространения вредоносного ПО…

В прошлом мы видели, как сайты-взломщики распространяют программы-вымогатели, такие как STOP и программы- вымогатели Exorcist, майнеры криптовалюты и трояны, ворующие информацию.

Поддельный взлом приводит к атаке программы-вымогателя Ryuk

После того, как научно-исследовательский институт подвергся атаке программы-вымогателя Ryuk, команда быстрого реагирования Sophos отреагировала и нейтрализовала кибератаку.

В результате этой атаки институт потерял недельные исследовательские данные и недельное отключение сети, поскольку серверы были восстановлены с нуля, а данные восстановлены из резервных копий.

После проведения криминалистической экспертизы атаки компания Sophos определила, что исходной точкой входа для злоумышленников был сеанс RDP с использованием учетных данных учащегося.

Институт работает со студентами университетов, которые помогают в исследованиях и других задачах. В рамках этого сотрудничества институт предоставляет студентам учетные данные для удаленного входа в свою сеть.

Получив доступ к ноутбуку студента и проанализировав историю браузера, они узнали, что студент искал дорогостоящее программное обеспечение для визуализации данных, которое они использовали на работе, и хотели установить на своем домашнем компьютере.

Вместо того, чтобы покупать лицензию за несколько сотен долларов, студент искал взломанную версию и скачал ее с сайта Warez.

Однако вместо получения ожидаемого программного обеспечения они были заражены трояном, крадущим информацию, который регистрировал нажатия клавиш, крал историю буфера обмена Windows и крал пароли, включая те же учетные данные, которые использовались злоумышленниками Ryuk для входа в институт.

«Маловероятно, что операторы, стоящие за «пиратским программным обеспечением», те же, что и те, кто запустил атаку Ryuk, - сказал Питер Маккензи, менеджер Rapid Response в Sophos. «Подпольный рынок ранее скомпрометированных сетей, предлагающий злоумышленникам простой начальный доступ, процветает, поэтому мы полагаем, что операторы вредоносных программ продали свой доступ другому злоумышленнику. Соединение RDP могло использоваться брокерами доступа, проверяющими их доступ».

Торговые площадки, посвященные продаже учетных данных удаленного доступа, процветали за последние пару лет и стали обычным источником учетных записей, используемых бандами вымогателей для получения доступа к корпоративным сетям.

Многие из этих украденных учетных данных собираются с помощью троянов, ворующих информацию, а затем продаются один за другим на этих торговых площадках всего за 3 доллара.

Совсем недавно BleepingComputer получил доступ к просочившимся данным для UAS, одного из крупнейших рынков учетных данных для удаленного рабочего стола Windows.

Эти данные показали, что за последние три года на рынке БПЛА было выставлено на продажу 1,3 миллиона учетных записей, что предоставило злоумышленникам огромный пул жертв.

К сожалению, человеческая ошибка всегда возможна. Пользователи будут продолжать открывать фишинговые электронные письма и загружать программные средства взлома, как бы мы им ни говорили.

Однако правильная настройка безопасности в сети, такая как требование MFA для подключений к удаленному рабочему столу и ограничение доступа из определенных мест или IP-адресов, предотвратила бы эту атаку». ***(Lawrence Abrams. A student pirating software led to a full-blown Ryuk ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/a-student-pirating-software-led-to-a-full-blown-ryuk-ransomware-attack/). 06.05.2021).***

***

«…По оценкам компании по кибербезопасности Emisoft, настоящая глобальная стоимость программ-вымогателей, включая прерывание бизнеса и выплаты выкупа в 2020 году, составила минимум 42 миллиарда долларов США и максимум почти 170 миллиардов долларов.

Опрос, проведенный Veritas Technologies, показал, что 66 процентов жертв признались в уплате части или всего выкупа, согласно отчету, опубликованному в среду фирмой eSentire, занимающейся управляемым обнаружением и реагированием.

В отчете, подготовленном группой исследователей безопасности eSentire, которую она называет Threat Response Unit (TRU), было обнаружено, что в этом году шесть банд вымогателей заявили о не менее 290 новых жертвах. Суммарная добыча потенциально принесла хакерам 45 миллионов долларов.

Исследователи компании eSentire объединились с исследователем даркнета Майком Мэйсом, чтобы отследить группы программ-вымогателей Ryuk / Conti, Sodin / REvil, CLOP и DoppelPaymer. Они также отслеживали двух появляющихся киберганг, известных как DarkSide и Avaddon.

Банда DarkSide должна позвонить в некоторые знакомые. Это организация, ответственная за атаку вымогателя Colonial Pipeline в начале этого месяца.

TRU из Esentire и Хейс обнаружили, что определенные группы собрали сотни жертв в 2020 году и коллективно скомпрометировали 292 новые организации жертв в период с 1 января по 30 апреля этого года. По оценкам исследователей, средняя сумма, выплачиваемая организациями, выкупающими выкуп, увеличилась со 115 123 долларов в 2019 году до 312 493 долларов в 2020 году, что на 171 процент больше по сравнению с аналогичным периодом прошлого года.

«Существует гораздо больше успешных атак программ-вымогателей, которые скомпрометировали компании, чем общественность может представить. На самом деле нет отрасли / бизнеса, которые не были бы потенциальной целью этих групп», - сказал TechNewsWorld вице-президент eSentire Марк Сангстер.

Бурно развивающийся бизнес для хакеров

Атаки программ-вымогателей часты. Их выплаты часто не раскрываются жертвами из-за смущения или потери общественного доверия. Однако хакерские группы не стесняются сообщать о своих успешных эксплойтах на своих личных блогах / сайтах утечек.

В отчете eSentire отмечены три новых атаки за последние три месяца:

Tata Steel - взломана группой вымогателей Sodin / REvil в апреле. Tata Steel отказалась выплатить выкуп в размере 4 миллионов долларов.

Школьный округ округа Бровард - скомпрометирован бандой Рюк / Конти в марте. Злоумышленники потребовали 40 миллионов долларов, и в округе заявили, что не будут платить.

Quanta Computer - производитель MacBook следующего поколения от Apple, также атакованный Sodin / REvil. Сообщается, что в апреле хакеры потребовали 50 миллионов долларов сначала у Quanta, которая отказалась от вымогательства, а затем у Apple.

Но исследователи отметили, что, несмотря на увеличение количества сообщений об атаках программ-вымогателей в СМИ, организации-жертвы, о которых сообщают СМИ, - это капля в море по сравнению с реальными событиями.

Один инцидент с вымогательством, который произошел в прошлом месяце, но так и не стал достоянием общественности, касался небольшой частной американской компании. По словам высокопоставленного сотрудника организации, попросившего не называть его имени, злоумышленники потребовали 12 миллионов долларов, которые компания заплатила.

Поскольку кибератаки развиваются с головокружительной скоростью, разведка киберугроз (CTI) стала важнейшим компонентом программ кибербезопасности. «Без разведки организации летят вслепую в очень грозовое небо», - сказал Дов Лернер, руководитель отдела исследований в области безопасности в Sixgill.

«На стратегическом уровне CTI позволит руководителям понять ландшафт угроз и оценить риски для своих организаций. На более тактическом уровне CTI используется для блокировки злонамеренных индикаторов взлома и обнаружения скомпрометированных данных», - сказал Лернер TechNewsWorld.

Он добавил, что по мере оцифровки все большего количества повседневных дел и деятельности у участников темной сети появляется больше возможностей потреблять и использовать конфиденциальные данные, размещенные на подпольных платформах. Подполье киберпреступности только продолжает расти, а пандемия и экономический кризис могут побудить все больше субъектов угрозы искать незаконную финансовую деятельность, а в последнее время - радикальный политический дискурс.

Никаких сомнений в успехе

Сангстер сказал, что его исследователи полностью верят в то, что организации, которые, по утверждениям этих групп, скомпрометировали, правдивы по нескольким причинам, в том числе:

Каждая из групп программ-вымогателей, в подробностях отчета приводятся многочисленные примеры различных файлов и документов, которые, по их утверждениям, были украдены у компаний-жертв. К тому же все они выглядят аутентично.

Исследователи видели, как группы угроз размещали жертву на своих сайтах утечки. Позже, возможно, через несколько недель, цель публично заявляет о том, что она подверглась атаке с помощью программы-вымогателя.

Этим группам вымогателей не выгодно лгать о жертвах, которых, по их утверждениям, взломали. Если бы они опубликовали на своем сайте утечки информацию о жертвах, которые не скомпрометировали, то слух распространится очень быстро, и ни одна жертва не будет им платить.

«Наша группа по исследованию безопасности, TRU и исследователь темной сети Майк Мэйс вошли в темную сеть и потратили много времени на анализ блогов / сайтов утечек этих шести групп вымогателей, а также проанализировали TTP этих групп, которые мы собрали отслеживая их с тех пор, как они начали свою преступную деятельность ", - сказал Сангстер.

Он добавил, что исследователи только что завершили все свои выводы и сейчас делятся деталями с различными правоохранительными органами.

Расширенный список атак

Esentire и Mayes обнаружили, что шесть групп программ-вымогателей, которые они отслеживали для этого отчета, продолжают нацеливаться не только на обычных подозреваемых - органы власти штата и местного самоуправления, школьные округа, юридические фирмы, больницы и медицинские организации. Они расширили свой хит-лист, включив в него производителей, транспортные / логистические компании и строительные фирмы в США, Канаде, Южной Америке, Франции и Великобритании.

Вот краткое изложение новых жертв в результате этого расширенного списка атак:

Рюк / Конти

Группа вымогателей Ryuk / Conti впервые появилась в августе 2018 года. Первыми их жертвами, как правило, были организации, базирующиеся в США. В их число входят технологические компании, поставщики медицинских услуг, образовательные учреждения, поставщики финансовых услуг, а также многочисленные государственные и местные правительственные организации.

Банда поразила в общей сложности 352 организации, скомпрометировав 63 компании и организации частного сектора только в этом году. TRU обследовало 37 из 63 жертв Рюка, и среди них 16 были производителями, которые производили все, от медицинских устройств до промышленных печей, оборудования для электромагнитного излучения и программного обеспечения для школьной администрации.

Сообщается, что в 2021 году Рюк скомпрометировал транспортные / логистические компании, строительные компании и организации здравоохранения.

Sodin / REvil

Sodin / REvil перечислил 161 новую жертву в этом году, 52 из которых были производителями, а также несколькими организациями здравоохранения, транспортными / логистическими компаниями и строительными фирмами. В марте группа напала на производителя компьютеров и электроники Acer и потребовала выкуп в размере 50 миллионов долларов.

Когда компания Quanta Computer, производящая ноутбуки для Apple, отказалась вести переговоры, как упоминалось выше, преступники Sodin, как сообщается, обратились к Apple за выкупом. Хакеры Sodin разместили в своем блоге «Счастливый блог» предупреждение о том, что, если им не заплатят, они

опубликуют то, что, по их утверждениям, является техническими деталями для текущего и будущего оборудования Apple.

ДоппельПаймер

Группа вымогателей DoppelPaymer появилась в 2019 году. На веб-сайте группы DoppelPaymer утверждается, что они скомпрометировали 186 жертв с момента своего дебюта, 59 из которых только в 2021 году. Среди жертв - многочисленные государственные и местные правительственные организации, а также несколько учебных заведений.

В декабре 2020 года ФБР выпустило предупреждение о том, что «с конца августа 2019 года неустановленные лица использовали программу-вымогатель DoppelPaymer для шифрования данных от жертв в критически важных отраслях по всему миру, таких как здравоохранение, экстренные службы и образование, прерывая доступ граждан к услугам».

Многие малые и средние предприятия, которые группа называет потерпевшими, никогда не освещались в прессе, равно как и многие организации государственного сектора. Одним из исключений является Генеральная прокуратура Иллинойса, которая впервые обнаружила атаку DoppelPaymer 10 апреля 2021 года.

Clop (Cl0p)

Программа-вымогатель Clop впервые появилась в феврале 2019 года и стала более известной в октябре 2020 года, когда ее операторы стали первой группой, потребовавшей выкуп в размере более 20 миллионов долларов. Жертва, немецкая технологическая фирма Software AG, отказалась платить.

В этом году Клоп попал в заголовки газет за то, что отбирал украденные данные жертв, извлекал контактную информацию клиентов и партнеров компании и отправлял им электронные письма с призывом заставить компанию-жертву заплатить выкуп.

Темная сторона

DarkSide - относительно новая группа программ-вымогателей. TRU Esentire начал отслеживать его в декабре прошлого года, примерно через месяц после того, как, как сообщается, он появился. Операторы заявляют в своем блоге / на сайте утечки, что всего заразили 59 организаций, скомпрометировав 37 из них в 2021 году.

Жертвы находятся в США, Южной Америке, на Ближнем Востоке и в Великобритании. Среди них производители всех видов продукции, такие как энергетические компании, компании по производству одежды, туристические компании.

Поздно 13 мая сайт блога / утечки DarkSide отключился, и злоумышленники заявили, что они потеряли доступ к инфраструктуре, которую использует для работы, и будут закрыты. В уведомлении упоминались сбои со стороны правоохранительных органов и давление со стороны США. До того, как веб-сайт DarkSide был закрыт, операторы всегда заявляли, что они распространяли свое вредоносное ПО с помощью модели «вымогатель как услуга».

Операторы DarkSide заявили, что они похожи на Робин Гуда, преследуя только прибыльные компании, которые могут позволить себе заплатить выкуп.

Операторы группы также отметили, что они не будут атаковать больницы, учреждения паллиативной помощи, дома престарелых, похоронные бюро и компании, занимающиеся разработкой и распространением вакцины Covid-19, согласно отчету eSentire.

Аваддон

Операторы Avaddon, чьи требования к программам-вымогателям впервые появились в феврале 2019 г., утверждают, что за свою жизнь они заразили 88 жертв, из них 47 - в 2021 г. Девять атак программ-вымогателей проводились по модели «программа-вымогатель как услуга».

Его операторы позволяют аффилированным лицам использовать программу-вымогатель, при этом часть прибыли выплачивается разработчикам Avaddon. По сообщениям Esentire, злоумышленники Avaddon также предлагают своим жертвам круглосуточную поддержку и ресурсы по покупке биткойнов, тестированию файлов для расшифровки и другим проблемам, которые могут помешать жертвам уплатить выкуп.

Как избежать атак программ-вымогателей

По данным eSentire, группы программ-вымогателей наносят ущерб гораздо большему количеству организаций, чем общественность осознает. Ни одна отрасль не застрахована от этого бедствия программ-вымогателей, которое происходит во всех регионах и секторах.

Esentire рекомендует следующие советы по защите от атак программ-вымогателей:

Сделайте резервную копию всех важных файлов и храните их в автономном режиме

Требовать многофакторную аутентификацию для доступа к службам виртуальной частной сети (VPN) или протокола удаленного рабочего стола (RDP) вашей организации

Разрешить только администраторам доступ к сетевым устройствам с помощью службы VPN.

Контроллеры домена являются ключевой целью для злоумышленников. Убедитесь, что ваша группа безопасности имеет видимость ваших ИТ-сетей с помощью агентов обнаружения конечных точек и ответа (EDR) и централизованной регистрации на контроллерах домена (DC) и других серверах.

Применяйте принцип наименьших привилегий по отношению к сотрудникам

Отключите RDP, если он не используется

Регулярно исправляйте системы, отдавая приоритет вашим ключевым ИТ-системам

Реализовать сегментацию сети

Обязательное обучение пользователей для всех сотрудников компании

«С точки зрения индустрии кибербезопасности компаниям доступны несколько очень эффективных служб, инструментов и политик безопасности, которые значительно помогают им защитить свои ценные данные и приложения от киберугроз, таких как программы-вымогатели, компрометация корпоративной электронной почты, кибершпионаж и уничтожение данных», Сангстер посоветовал». ***(Jack M. Germain. New Report Profiles Ransomware Cybergangs //***

ECT News Network, Inc. (https://www.technewsworld.com/story/New-Report-Profiles-Ransomware-Cybergangs-87139.html). 21.05.2021).

***

«Национальное агентство по борьбе с преступностью Великобритании (NCA) предупредило, что резкое увеличение количества атак с использованием программ-вымогателей и их серьезность наносят значительный ущерб.

Ежегодная Национальная стратегическая оценка серьезной и организованной преступности NCA подробно описывает, как общая угроза киберпреступности увеличилась за последний год с более серьезными и громкими атаками на жертв.

В частности, в течение последнего года количество атак программ-вымогателей возросло, и их влияние возросло до такой степени, что они стали одними из других серьезных преступлений, «причиняющих значительный ущерб нашим гражданам и сообществам», - говорится в отчете.

Одна из вещей, которые сделали программы-вымогатели намного более опасными, - это рост атак, которые не просто шифруют сети и требуют выкупа в биткойнах или другой криптовалюте в обмен на расшифровку, но также видят, как киберпреступники крадут конфиденциальную информацию у жертвы. организации, что мошенники угрожают опубликовать ее, если их требования о вымогательстве не будут выполнены, что может подвергнуть сотрудников и представителей общественности риску дополнительного мошенничества.

Согласно отчету NCA, более половины атак программ-вымогателей сейчас используют эту технику двойного вымогательства.

В дополнение к этому, требования выкупа растут, часто достигая миллионов фунтов стерлингов, а возросшая серьезность атак отражается в их воздействии на предприятия и другие организации, которые не могут предоставлять общественные услуги после того, как стали жертвами программ-вымогателей.

В документе подробно описывается атака программ-вымогателей на Redcar и городской совет Кливленда в феврале 2020 года в качестве примера того, как киберпреступность может иметь последствия для общества. В результате атаки программы-вымогателя местные власти на короткое время были не в состоянии предоставлять услуги на переднем крае, в том числе функции по уходу за уязвимыми детьми и взрослыми. Атака зашифровала данные о приеме в школы, что задержало процесс зачисления учащихся.

NCA работало с Национальным центром кибербезопасности (NCSC), правоохранительными органами и местными властями, чтобы помочь восстановить услуги.

С тех пор киберугроза возросла, поскольку преступники использовали пандемию COVID-19 и распространение удаленной работы как средства получения доступа к сетям с помощью фишинговых атак или взлома облачных сервисов, сервисов протокола удаленного рабочего стола и VPN. «Увеличение числа работающих на дому увеличило риски для частных лиц и предприятий», - говорится в отчете.

Университеты и школы стали постоянными целями для вымогателей атак, в то время как организации, в то числе в Агентстве шотландской защиты окружающей среды (SEPA) и Великобритания исследования и инновации (UKRI) стали жертвами громких вымогателей атак против Великобритании целевых показателей в этом году.

Но, несмотря на растущую угрозу программ-вымогателей и масштаб ущерба, который может быть нанесен, можно принять меры, чтобы вообще не стать жертвой этих программ.

NCA рекомендует организациям обновлять программное обеспечение, применяя исправления, чтобы не дать киберпреступникам использовать известные уязвимости для получения доступа к сети.

Организации также должны гарантировать, что сотрудники используют надежные уникальные пароли, чтобы предотвратить их взлом при атаках методом грубой силы, и чтобы по возможности применялась двухфакторная аутентификация, чтобы обеспечить дополнительный барьер для киберпреступников, если они успешно взломают учетную запись.

Также рекомендуется, чтобы организации создавали резервные копии важных данных на внешнем жестком диске или в облачном хранилище, чтобы в худшем случае, когда они подверглись атаке программы-вымогателя, данные можно было восстановить, не платя киберпреступникам за ключ дешифрования. ***(Danny Palmer. Ransomware: Dramatic increase in attacks is causing harm on a significant scale // ZDNet (https://www.zdnet.com/article/ransomware-dramatic-increase-in-attacks-is-causing-harm-on-a-significant-scale/). 26.05.2021).***

***

«Почта Канады сообщила 44 своим крупным коммерческим клиентам, что атака программы-вымогателя на стороннего поставщика услуг раскрыла информацию о доставке для их клиентов.

Почта Канады - основной почтовый оператор в Канаде, обслуживающий 16,5 миллионов канадских жилых и рабочих адресов.

Вчера Canada Post сообщила, что сторонний поставщик Commport Communications подвергся атаке с использованием программ-вымогателей, когда злоумышленники получили доступ к данным, хранящимся в их системах.

Эти данные, к которым был осуществлен доступ, включают данные манифеста доставки для клиентов, занимающихся крупными посылками, включая контактную информацию, имена и почтовые адреса отправителя и получателя.

В общей сложности от взлома пострадали 44 коммерческих клиента Почты Канады и 950 000 клиентов-получателей.

«После подробного судебно-медицинского расследования нет никаких доказательств того, что какая-либо финансовая информация была нарушена. В целом, затронутые грузовые манифесты для 44 коммерческих клиентов содержали информацию, касающуюся чуть более 950 тысяч клиентов-получателей. После тщательного изучения файлов транспортных манифестов, мы определили следующее:

Информация с июля 2016 г. по март 2019 г.

Подавляющее большинство (97%) содержало имя и адрес получателя.

Остальные (3%) содержали адрес электронной почты и / или номер телефона »- Canada Post.

Программа-вымогатель Lorenz, ответственная за взлом

В декабре 2020 года программа-вымогатель, известная как Lorenz, опубликовала на своем сайте утечки данных, что они взломали Commport Communications во время атаки вымогателя.

С тех пор группа вымогателей утекла в утечку 35,3 ГБ данных, предположительно украденных во время атаки.

Хотя Canada Post заявляет, что во время атаки Commport не верил, что к каким-либо из их данных был осуществлен доступ, на основании просочившихся данных, похоже, что это не так.

Почта Канады заявляет, что они наняли внешних экспертов по кибербезопасности для помощи в расследовании и уведомили Управление комиссара по конфиденциальности Канады». ***(Lawrence Abrams. Canada Post hit by data breach after supplier ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/canada-post-hit-by-data-breach-after-supplier-ransomware-attack/). 27.05.2021).***

***

«Доступ к мексиканским лотерейным сайтам Lotería Nacional и Pronósticos теперь заблокирован для IP-адресов за пределами Мексики после того, как банда вымогателей пригрозила провести атаки типа «отказ в обслуживании».

Lotería Nacional - это государственная национальная лотерейная система Мексики, работающая под управлением Министерства финансов Мексики. Pronósticos - это программа от Loteria Nacional, в которой мексиканцы могут делать ставки на азартные игры или спорт.

Вчера сотрудники программы-вымогателя Avaddon заявили, что они успешно провели атаку на «Pronosticos Deportivo», где они утверждают, что украли данные, а затем зашифровали устройства. Банда программ-вымогателей также пригрозила выпустить дополнительные документы и провести DDoS-атаки на веб-сайт жертвы, если переговоры не начнутся в течение 240 часов.

В рамках этого объявления банда вымогателей слила скриншоты того, что, по их утверждениям, является украденными во время атаки документами, на бланках которых находятся Lotería Nacional и Pronósticos.

Участки Lotería Nacional и Pronósticos обнесены стеной

Когда мы узнали об этой предполагаемой атаке вчера вечером, мы смогли получить доступ к сайтам Lotería Nacional (https://www.lotenal.gob.mx/) и Pronósticos (https://www.pronosticos.gob.mx/).

Однако сегодня эти сайты больше не доступны для IP-адресов за пределами Мексики, и теперь время ожидания подключения к сайту истекает...

С помощью Хирама Алехандро, директора по информации компании по кибербезопасности Seekurity, BleepingComputer подтвердил, что эти сайты доступны только с IP-адресов в Мексике.

После того, как BleepingComputer переключился на VPN, используя IP-адрес в Мексике, мы снова смогли получить доступ к сайтам.

Считается, что мексиканское правительство намеренно заблокировало веб-сайты Lotería Nacional и Pronósticos, чтобы предотвратить распределенные атаки отказа в обслуживании (DDoS) со стороны банды вымогателей Avaddon.

Поскольку DDoS-атаки обычно проводятся с устройств по всему миру, их трудно предотвратить из-за широкой и разнообразной правовой юрисдикции стран, в которых находятся эти устройства. Блокируя международный доступ к сайтам мексиканских лотерей, правительство может эффективно противодействовать атакам и легко блокировать любые устройства в Мексике, которые могут быть частью атаки.

Если это так, то это интересное смягчение последствий DDoS-атаки, которую BleepingComputer не видел в прошлом со стороны правительства.

BleepingComputer связался с электронным письмом правительства Мексики, но пока не получил ответа». ***(Lawrence Abrams. Mexico walls off national lottery sites after ransomware DDoS threat // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/mexico-walls-off-national-lottery-sites-after-ransomware-ddos-threat/). 28.05.2021).***

***

«Было замечено, что новая угроза вымогателей, называющая себя Red Epsilon, использует уязвимости сервера Microsoft Exchange для шифрования машин в сети.

Атаки программ-вымогателей Epsilon Red основываются на более чем дюжине сценариев, прежде чем они достигнут стадии шифрования, а также используют коммерческую утилиту удаленного рабочего стола.

Попадание в уязвимый сервер Microsoft Exchange

Специалисты по реагированию на инциденты в компании по кибербезопасности Sophos обнаружили новую программу-вымогатель Epsilon Red на прошлой неделе во время расследования атаки на довольно крупную американскую компанию в сфере гостеприимства.

Исследователи обнаружили, что злоумышленник проник в корпоративную сеть, используя незащищенные уязвимости на локальном сервере Microsoft Exchange.

Эндрю Брандт, главный исследователь Sophos, сообщает сегодня в отчете, что злоумышленники, возможно, использовали набор уязвимостей ProxyLogon для доступа к машинам в сети.

Ошибки ProxyLogon получили широкую огласку, поскольку хакеры ухватились за это дело и начали сканировать Интернет на предмет уязвимых устройств и компрометировать системы.

Из-за критической опасности организации по всему миру поспешили установить исправления, и менее чем за месяц около 92% уязвимых локальных серверов Microsoft Exchange получили обновление.

Уникальный набор инструментов

Epsilon Red написан на языке Golang (Go), и ему предшествует набор уникальных сценариев PowerShell, которые подготавливают почву для процедуры шифрования файлов, каждый из которых имеет определенную цель:

убить процессы и службы для средств безопасности, баз данных, программ резервного копирования, приложений Office, почтовых клиентов

удалить теневые копии тома

украсть файл диспетчера учетных записей безопасности (SAM), содержащий хеши паролей

удалить журналы событий Windows

отключить Защитник Windows

приостановить процессы

удалить инструменты безопасности (Sophos, Trend Micro, Cylance, MalwareBytes, Sentinel One, Vipre, Webroot)

расширить разрешения в системе

Большинство скриптов пронумерованы от 1 до 12, но есть несколько, которые названы одной буквой. Один из них, c.ps1, похоже, является клоном инструмента тестирования на проникновение Copy-VSS.

После взлома сети хакеры достигают компьютеров через RDP и используют инструментарий управления Windows (WMI) для установки программного обеспечения и запуска сценариев PowerShell, которые в конечном итоге развертывают исполняемый файл Epsilon Red.

Исследователи Sophos заметили, что злоумышленник также устанавливает копию Remote Utilities - коммерческого программного обеспечения для работы с удаленными рабочими столами, а также браузер Tor. Этот шаг должен гарантировать, что у них все еще будет открыта дверь, если они потеряют доступ через начальную точку входа.

Модель записки с требованием выкупа REvil

Питер Маккензи, менеджер группы Sophos Rapid Response, сказал BleepingComputer, что, хотя эта версия Epsilon Red, похоже, не является работой профессионалов, она может вызвать большой беспорядок, поскольку она не имеет ограничений на шифрование типов файлов и папок.

Вредоносная программа имеет небольшую функциональность, кроме шифрования файлов и папок, но включает в себя код из инструмента с открытым исходным кодом godirwalk, библиотеки для просмотра дерева каталогов в файловой системе.

Эта функция позволяет Epsilon Red сканировать жесткий диск и добавлять пути к каталогам в список мест назначения для дочерних процессов, которые шифруют вложенные папки по отдельности. В конце концов, на зараженных машинах будет запущено большое количество копий процесса вымогателя.

Он шифрует все в целевых папках, добавляя суффикс «.epsilonred», не щадя исполняемые файлы или библиотеки DLL, которые могут нарушить работу важных программ или даже операционной системы.

Типичным способом вымогателей Epsilon Red помещает в каждую обработанную папку записку о выкупе с инструкциями о том, как связаться со злоумышленниками для согласования цены за расшифровку данных.

Если инструкции кажутся вам знакомыми, это потому, что злоумышленники используют обновленную версию записки о выкупе, используемой вымогателем REvil. Однако Epsilon Red постаралась исправить исходные грамматические и орфографические ошибки русской банды.

Хотя происхождение хакеров на данный момент остается неизвестным, ясно, откуда они взяли свое имя. Эпсилон Ред - малоизвестный персонаж из вселенной Marvel, российский суперсолдат с четырьмя щупальцами, способный дышать в космосе.

Несмотря на то, что банда вымогателей Epsilon Red была новичком в бизнесе программ-вымогателей, она атаковала несколько компаний, и эти инциденты расследуются несколькими фирмами, занимающимися кибербезопасностью.

Хакеры тоже неплохо заработали. Sophos обнаружил, что одна жертва этой угрозы вымогателя 15 мая заплатила злоумышленникам 4,28 BTC (около 210 000 долларов США)». ***(Ionut Ilascu. New Epsilon Red ransomware hunts unpatched Microsoft Exchange servers // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-epsilon-red-ransomware-hunts-unpatched-microsoft-exchange-servers/). 29.05.2021).***

***

Програми-трояни

«Microsoft предупреждает, что в последние месяцы организации в аэрокосмическом и туристическом секторах стали объектами кампании, направленной на заражение жертв троянами удаленного доступа (RAT) и другими типами вредоносного ПО.

Атаки начинаются с целевых фишинговых сообщений, в которых используются приманки, относящиеся к целевым организациям, таким как авиация, путешествия и грузы, и доставляется изображение, которое выдает себя за файл PDF и содержит встроенную ссылку.

Злоумышленники злоупотребляют законными веб-службами и используют недавно идентифицированный загрузчик, получивший название Snip3, для доставки RAT.

На прошлой неделе исследователи безопасности с поставщиком решений для безопасности конечных точек Morphisec показали, что, как только жертва нажимает на ссылку, загружается сценарий VBScript, который, в свою очередь, отбрасывает сценарий PowerShell второго уровня, отвечающий за уклонение от обнаружения и удаление конечной полезной нагрузки.

Snip3 все еще находится в стадии активной разработки, и Morphisec за несколько месяцев определил около дюжины версий.

Последней полезной нагрузкой в этих атаках обычно является RevengeRAT или AsyncRAT, но наблюдались и дополнительные полезные нагрузки, включая Agent Tesla и NetWire RAT. Основная цель атак заключается в сборе и краже данных.

«RAT подключаются к серверу C2, размещенному на сайте динамического хостинга, для регистрации у злоумышленников, а затем используют PowerShell в кодировке UTF-8 и бесфайловые методы для загрузки трех дополнительных этапов с pastebin [.] Com или аналогичных сайтов», - Microsoft говорит.

На скомпрометированных системах трояны пытаются внедрить компоненты в такие процессы, как RegAsm, InstallUtil или RevSvcs, и Microsoft объясняет, что они постоянно повторно запускают компоненты, пока внедрение процесса не будет успешным.

«Они крадут учетные данные, снимки экрана и данные веб-камеры, данные браузера и буфера обмена, систему и сеть, а также часто пересылают данные через SMTP-порт 587», - также отмечает технический гигант». ***(Ionut Arghire. Microsoft Warns of Attacks on Aerospace, Travel Sectors // Wired Business Media (https://www.securityweek.com/microsoft-warns-attacks-aerospace-travel-sectors). 13.05.2021).***

***

«Новый троян Android был обнаружен исследователями безопасности, которые в понедельник заявили, что после его успешной установки на устройство жертвы те, кто стоит за ним, могут получать прямую трансляцию экрана устройства, а также взаимодействовать с ним через свои службы доступности.

Вредоносная программа, которую исследователи из Cleafy назвали Teabot, использовалась для перехвата учетных данных пользователей и SMS-сообщений с целью облегчения мошеннических действий против банков в Испании, Германии, Италии, Бельгии и Нидерландах.

Группа Cleafy по анализу угроз и реагированию на инциденты впервые обнаружила банковского трояна в январе и обнаружила, что он обеспечивает возможность мошенничества в отношении более чем 60 банков по всей Европе. К 29 марта аналитики Cleafy обнаружили, что троян используется против итальянских банков, а к маю банки Бельгии и Нидерландов также боролись с ним.

Исследования показывают, что Teabot все еще находится в стадии разработки, но первоначально был ориентирован только на испанские банки, а затем перешел к банкам в Германии и Италии. В настоящее время вредоносная программа поддерживает 6 различных языков, включая испанский, английский, итальянский, немецкий, французский и голландский.

Первоначально приложение называлось TeaTV, а затем неоднократно меняло названия на «VLC MediaPlayer», «Mobdro», «DHL», «UPS» и «bpost».

«Когда вредоносное приложение загружается на устройство, оно пытается быть установленным как «служба Android», которая представляет собой компонент приложения, который может выполнять длительные операции в фоновом режиме. TeaBot злоупотребляет этой функцией, чтобы скрыть от после установки пользователь также предотвращает обнаружение и обеспечивает его постоянство», - говорится в отчете Cleafy.

После установки TeaBot будет запрашивать разрешения Android для наблюдения за вашими действиями, получения содержимого окна и выполнения

произвольных жестов. Когда разрешения будут предоставлены, приложение удалит свой значок с устройства, согласно исследованию Клефи.

Саумитра Дас, технический директор компании Blue Hexagon, занимающейся кибербезопасностью, заявила, что Teabot представляет собой переход мобильного вредоносного ПО от второстепенной проблемы к основной проблеме, такой же как вредоносное ПО на традиционных конечных точках.

«Злоумышленники осознают истинный потенциал мобильных устройств и угрозу, которую они могут представлять для конечного пользователя», - сказал Дас.

«Важно помнить, что даже несмотря на то, что приложений нет в Google Play, тактика фишинга / социальной инженерии, используемая участниками Teabot / Flubot, ничем не уступает любому семейству угроз на стороне ПК. им удастся получить огромную базу заражения. Эти угрозы нельзя недооценивать». ***(Jonathan Greig. New Android malware targeting banks in Italy, Spain, Germany, Belgium, and the Netherlands // ZDNet (https://www.zdnet.com/article/new-android-malware-targeting-banks-in-italy-spain-germany-belgium-and-the-netherlands/). 11.05.2021).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«На этой неделе Министерство юстиции Соединенных Штатов объявило о вынесении приговора гражданину России за его роль в группе, которая пыталась получить 1,5 миллиона долларов в виде возмещения налогов от Министерства финансов.

Мужчина, 35-летний Антон Богданов, который использовал онлайн-прозвище «Кусок», был арестован в Таиланде в ноябре 2018 года и экстрадирован в США в марте 2019 года. В мае 2019 года ему были предъявлены обвинения в мошенничестве с использованием электронных средств связи, краже личных данных при отягчающих обстоятельствах и вторжении в компьютер. и признал себя виновным в январе 2020 года.

Согласно судебным документам, в период с июня 2014 года по ноябрь 2016 года Богданов и его сообщники взломали компьютеры частных налоговых компаний в США и украли личную информацию, включая номера социального страхования и даты рождения.

Затем, используя незаконно присвоенную информацию, они изменили информацию о налоговых декларациях своих жертв, так что возмещение было отправлено на дебетовые карты, контролируемые мошенниками. Богданов также использовал украденные данные на веб-сайте IRS Transcript System, чтобы получить предыдущие налоговые декларации жертв, а затем подал новые налоговые декларации, чтобы вернуть деньги на предоплаченные дебетовые карты злоумышленников.

Хотя дебетовые карты обналичивались в Соединенных Штатах, часть выручки переводилась Богданову, который проживал в России.

Используя эту схему, Богданов и его сообщники попытались украсть около 1,5 млн долларов в виде налоговых возмещений из Министерства финансов.

Богданов был приговорен к 60 месяцам лишения свободы с уплатой 476 713 долларов конфискации.

«Богданов использовал изощренные средства для кражи двух ценных вещей: личной информации людей и средств, принадлежащих американскому налогоплательщику», - сказал Джонатан Ларсен из отдела уголовных расследований IRS. «IRS-Criminal Investigation будет продолжать работать бок о бок с нашими партнерами из правоохранительных органов, чтобы выявлять и преследовать международных киберпреступников, которые проникают в нашу налоговую систему для личной выгоды». ***(Ionut Arghire. Member of Russian Gang That Hacked Tax Prep Firms Sentenced to Prison in U.S. // Wired Business Media (https://www.securityweek.com/member-russian-gang-hacked-tax-prep-firms-sentenced-prison-us). 20.05.2021).***

***

«За последний год было заблокировано больше веб-сайтов, на которых размещены фишинговые домены и другие виды онлайн-мошенничества, чем за предыдущие три года вместе взятые.

В четвертом ежегодном отчете об активной киберзащите Национального центра кибербезопасности Великобритании (NCSC) подробно описывается, как он помог удалить еще много мошенников из Интернета: в общей сложности более 1,4 миллиона URL-адресов, ответственных за 700000 онлайн-мошенников, были удалены службой удаления NCSC во время последние 12 месяцев.

В прошлом году наблюдался большой рост киберпреступности на тему COVID-19, и NCSC помог удалить тысячи URL-адресов, связанных с фишингом и атаками вредоносных программ, с помощью предупреждений о COVID-19 или ложных предложений вакцин.

NCSC также помогал блокировать фальшивые интернет-магазины, размещенные в Великобритании, а также фальшивые рекламные объявления знаменитостей, которые использовались в попытке заманить людей стать жертвами кибератак. Часто эти мошенничества начинаются с фишинговых сообщений, в которых жертвы проходят через несколько URL-адресов, прежде чем они попадут на последний вредоносный сайт.

Мошенничество и фишинговые кампании, которые выглядели так, как будто они исходили от правительства, NHS, HMRC и многих других известных организаций, были заблокированы в рамках программы активной киберзащиты NCSC (ACD), которая, по его словам, направлена на защиту «большинство людей в Великобритании от большей части вреда, причиненного большинством кибератак большую часть времени».

Инструменты в арсенале ACD включают службу удаления для поиска вредоносных сайтов и отправки уведомлений хосту для их удаления из Интернета. Он также включает в себя Службу сообщений о подозрительных электронных

письмах - функцию, представленную в прошлом году, которая позволяет представителям общественности пересылать электронные письма, подозреваемые в мошенничестве, непосредственно в NCSC для дальнейшего расследования.

На сегодняшний день служба получила более четырех миллионов электронных писем и помогла идентифицировать более 1,5 миллиона вредоносных URL-адресов и помогла устранить десятки тысяч мошенников, которые ранее не были идентифицированы. Тем не менее, в отчете отмечается, что процент атак, заблокированных в течение 24 часов, также снизился с 64,6% в 2019 году до 55,5% в 2020 году.

«Программа ACD - это действительно совместные усилия, и именно благодаря нашим совместным усилиям с партнерами как внутри страны, так и за рубежом мы смогли значительно активизировать наши усилия по защите Великобритании», - сказал д-р Ян Леви, технический директор NCSC.

«Смелый защитный подход, принятый программой ACD, продолжает обеспечивать нашу национальную устойчивость, и поэтому я призываю государственные органы, компании и широкую общественность подписаться на доступные услуги, чтобы помочь всем оставаться в безопасности в сети», - добавил он». ***(Danny Palmer. This security project has taken down 1.5 million scam, phishing and malware URLs in just one year // ZDNet (https://www.zdnet.com/article/this-security-project-has-taken-down-1-5-million-scam-phishing-and-malware-urls-in-just-a-year/). 10.05.2021).***

***

«Высокий суд Ирландии издал судебный запрет против банды Conti Ransomware, требуя, чтобы украденные данные HSE были возвращены, а не проданы или опубликованы.

На прошлой неделе Управление здравоохранения Ирландии (HSE) пострадало от атаки программы-вымогателя Conti, которая серьезно нарушила работу служб здравоохранения в стране.

Сегодня Conti выпустила дешифратор для зашифрованных файлов, но предупредила, что они по-прежнему намерены публиковать или продавать данные, украденные во время атаки на HSE.

Чтобы попытаться предотвратить разглашение личных и потенциально конфиденциальных медицинских данных, HSE снова получил судебный запрет против программы-вымогателя Conti от Высокого суда Ирландии.

Не имея формального способа выполнения постановления Суда, представители правительства загрузили его на темный веб-сайт Tor, связанный с атакой программы-вымогателя Conti HSE.

Этот приказ запрещает злоумышленникам публиковать, продавать или делиться украденными данными с общественностью

Он также требует, чтобы злоумышленники вернули украденные данные и идентифицировали себя, указав свои имена, адреса электронной почты и физические адреса.

Хотя не предполагается, что злоумышленники Conti уступят требованиям, есть надежда, что страны-субъекты угроз помогут отследить и предотвратить утечку данных злоумышленниками.

Аналогичный судебный запрет был предоставлен производителю проводов и кабелей SouthWire против операции Maze Ransomware и интернет-провайдеру в Ирландии, который размещал сайт утечки данных группы вымогателей.

Этот судебный запрет привел к временному удалению сайта утечки данных Maze, но данные SouthWire в конечном итоге были утекли, когда злоумышленники вернули сайт в сеть.

Обновление 21.05.21, 8:39 по восточному стандартному времени: хотя судебный запрет направлен против банды Conti Ransomware и доставлен им через переговорный чат на их сайте Tor, редактор Irish Times по вопросам безопасности и преступности Конор Лалли объясняет, что судебный запрет не предназначен для предотвратить утечку данных злоумышленниками.

Вместо этого он был выпущен, чтобы помешать прессе или кому-либо еще публиковать содержимое украденных данных в случае их утечки бандой вымогателей». ***(Lawrence Abrams. Irish High Court issues injunction to prevent HSE data leak // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/irish-high-court-issues-injunction-to-prevent-hse-data-leak/). 20.05.2021).***

***

«Четырем лицам из Восточной Европы грозит 20 лет тюрьмы по обвинению в организации коррумпированных рэкетиров (RICO) после того, как они признали себя виновными в использовании пуленепробиваемого хостинга в качестве убежища для киберпреступных операций, нацеленных на американские организации.

Пуленепробиваемый хостинг был основан гражданами России Александром Гричишкиным и Андреем Скворцовым, которые наняли литовца Александра Скородумова и эстонец Павла Стасси в качестве системного администратора и администратора организации соответственно.

Гричишкин и Скворцов курировали маркетинг, управление персоналом и поддержку клиентов, а Скородумов и Стасси отвечали за поддержание работы всех систем и помогали клиентам, стоящим за вредоносными программами и ботнетами, оптимизировать их «услуги».

Безопасное убежище для вредоносных программ

Согласно опубликованному сегодня пресс-релизу Министерства юстиции, их служба предоставила нескольким клиентам, связанным с киберпреступностью, инфраструктуру, необходимую для злонамеренных кампаний, проводившихся в период с 2008 по 2015 год.

«Группа арендовала IP-адреса, серверы и домены для клиентов-киберпреступников, которые использовали эту техническую инфраструктуру для распространения вредоносных программ, используемых для получения доступа к компьютерам жертв, формирования ботнетов и кражи банковских учетных данных для использования в мошенничестве», - Министерство юстиции сказал.

«Вредоносное ПО, размещенное организацией, включало Zeus, SpyEye, Citadel и Blackhole Exploit Kit, которые в период с 2009 по 2015 год безудержно атаковали американские компании и финансовые учреждения и причинили или пытались причинить миллионы долларов убытков американским жертвам».

Другие услуги, предоставляемые их пуленепробиваемой службой хостинга, включали регистрацию новой инфраструктуры с использованием ложных или украденных идентификационных данных, чтобы помочь клиентам обойти усилия правоохранительных органов по блокированию их атак.

Основная услуга, оказываемая обвиняемыми, заключалась в том, чтобы помочь своим клиентам избежать обнаружения правоохранительными органами и непрерывно продолжать свои преступления; обвиняемые сделали это, отслеживая сайты, используемые для блокирования технической инфраструктуры, используемой для совершения преступлений, перемещая «помеченный» контент в новую инфраструктуру и регистрируя всю такую инфраструктуру под ложными или украденными именами. - Министерство юстиции

Ответственный за убытки в миллионы долларов

«В течение многих лет обвиняемые способствовали транснациональной преступной деятельности обширной сети киберпреступников по всему миру, предоставляя им убежище для анонимности их преступной деятельности», - сказал специальный агент ФБР Тимоти Уотерс.

«Это привело к потерям в миллионы долларов для жертв из США. Сегодняшнее признание вины посылает киберпреступникам по всему миру сигнал о том, что они находятся в пределах досягаемости ФБР и его международных партнеров и что любой, кто содействует преступной кибер-деятельности или извлекает из нее прибыль, будут привлечены к ответственности».

Все четверо обвиняемых признали себя виновными по одному пункту обвинения в сговоре с RICO в феврале, марте и мае 2021 года.

Стасси, Скородумов, Гричишкин и Скворцов будут приговорены к приговору 3 июня, 29 июня, 8 июля и 16 сентября.

Каждому из четырех обвиняемых грозит максимальное наказание в виде 20 лет лишения свободы, которое судья федерального окружного суда назначит после рассмотрения Руководства по вынесению приговоров и других установленных законом факторов.

ФБР расследовало дело при содействии партнеров правоохранительных органов из Великобритании, Германии и Эстонии». ***(Sergiu Gatlan. Bulletproof hosting admins plead guilty to running cybercrime safe haven // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/bulletproof-hosting-admins-plead-guilty-to-running-cybercrime-safe-haven/). 07.05.2021).***

***

Технічні аспекти кібербезпеки

«Наша цивилизация привязана к Интернету. Подстегиваемое этой зависимостью, массовое внедрение 5G неизбежно. Несмотря на безграничный

потенциал, который 5G может принести человечеству (от электронного здравоохранения, умных транспортных средств до энергоснабжения умных городов), также ожидается, что киберпреступники будут использовать 5G.

В частности, среди ожидаемых угроз, связанных с 5G, стоит отметить атаку ботнета с помощью 5G. В этом сценарии ожидается, что киберпреступники будут использовать свой беспрецедентный потенциал для подключения большого количества устройств, использовать такие захваченные устройства, разделенные на подгруппы со специальными навыками, которые, в свою очередь, могут использовать такую силу для атаки и преодоления защиты одной цели.

Киберпреступники могут нацеливаться на сети и / или устройства как на интегрированную систему и обмениваться данными в режиме реального времени, чтобы совершенствовать свои атаки по мере того, как они происходят. Этот эффект усиливается там, где целью является конкретная организация, где повышенная вычислительная мощность 5G может захватить все устройства в сети этой конкретной организации и нанести невообразимый ущерб.

В конце концов, технологиям роя требуется большая вычислительная мощность для включения отдельных роевых ботов и эффективного обмена информацией в рое ботов, а 5G вместе со слабым протоколом защиты сети обеспечат именно такие атаки. В результате рой 5G позволит своим операторам (например, киберпреступникам) быстро обнаруживать, делиться и соотносить уязвимости, а затем переключать свои методы атаки, чтобы лучше использовать обнаруженные ими уязвимости. Ожидается, что у большинства организаций не будет средств защиты, готовых к защите от таких атак.

Как подготовить вашу организацию

Несмотря на вышеупомянутый разрушительный потенциал, организации должны помнить о следующем:

Наблюдать и сориентировать: ИТ-персоналу организаций крайне важно на раннем этапе понять природу технологии 5G, чтобы знать, как она работает, распознавать угрозы и планировать непредвиденные действия. Это особенно верно для многонациональных организаций, которые должны знать, где находятся их технологические уязвимости, и принимать меры. В Гонконге, где финансовое учреждение хранит любую информацию своих клиентов в мягких условиях, ожидается, что они предпримут соответствующие действия для защиты своих данных.

Важен внутренний контроль: необходима глубокая защита. Организация должна иметь установленную процедуру внутреннего контроля ИТ и планы действий в чрезвычайных ситуациях, которые будут включать автоматизированные шаги в отношении того, какие действия автоматически требуются в случае атаки.

Баланс: хотя внутренний контроль необходим, крайне важно, чтобы такие руководства не были слишком обременительными для передовых, чтобы свести на нет любое положительное влияние, которое технология 5G может оказать на организацию.

Познай себя: хотя многие знают, что 5G предложит организациям множество преимуществ, чтобы позволить себе надлежащее планирование, каждая

организация должна знать и учитывать следующие вопросы в ходе технологической адаптации:

(i) Какова роль адаптации 5G в адаптации бизнеса вашей организации и какую пользу она принесет вашей организации в бизнес-среде?

(ii) Имеет ли технология 5G, которую ваша организация желает внедрить, какие-либо встроенные функции безопасности для защиты своих пользователей, и является ли такая функция адекватной? Как устранить уязвимости?

(iii) Какие дополнительные уровни безопасности можно использовать после адаптации? Как можно изолировать открытую зону от остальной части производственно-сбытовой цепочки вашей организации, чтобы свести к минимуму возможные нарушения.

5. Безопасность конвергентных сетей. Конвергенция сетей и безопасности создает очень гибкую и адаптивную стратегию безопасности. Три важных функции для эффективной безопасности конвергентной сети включают в себя:

(i) Контролируемый доступ. Этого можно добиться с помощью:

а. Аутентификация или обнаружение всех устройств, подключенных к сети;

б. Контролируемая авторизация устройств, подключенных к сети; а также

с. Связывание политики один раз (i) происходит аутентификация и (ii) авторизация.

(ii) Защитите устройства и приложения. Уязвимые приложения могут привести к последствиям в реальном мире (хакеры уже нашли способы использовать носимые аксессуары). Таким образом, вторым элементом является проактивная защита используемых устройств и приложений. Три элемента такой защиты включают:

а. Определите политику допустимого использования для сети;

б. Возможность защиты устройств от другого протокола; а также

с. Примените правильное определение услуги.

(iii) Как и любая другая политика защиты, она не будет полной без плана реагирования, ключевой элемент которого должен включать:

а. Обнаружение атак (знать, когда и как так действовать);

б. Возможность сообщить о такой входящей атаке (вызвать ответ); а также

с. Измените поведение сети, чтобы устранить слабые места.

Заключение

Внедрение все более сложных технологий приведет к появлению еще более изощренных угроз. Организации должны быть начеку и быть готовы противостоять такой угрозе. Это ситуация жизни и смерти для организации (и ее руководства), если и когда это все-таки произойдет!» ***(Latest Cybersecurity & Law Update: 5G Enabled BotNet Attack – How Organizations Can Defend and Mitigate Risks from 5G BotNet Attacks? // Thomson Reuters (http://www.hk-lawyer.org/content/latest-cybersecurity-law-update-5g-enabled-botnet-attack-%E2%80%93-how-organizations-can-defend-and). 12.05.2021).***

***

«…Хотя двухфакторная аутентификация (2FA) с использованием push-текстовых уведомлений стала де-факто стандартом безопасности входа в систему, злоумышленники нашли множество способов ее обойти.

Фактически, существует кустарная индустрия, ориентированная на победу над 2FA. Akamai недавно опубликовал сообщение в блоге, описывающее фишинговую кампанию, нацеленную на банковских клиентов в Соединенном Королевстве путем уклонения от 2FA. Исследователи из группы Global Threat Intelligence Team в WMC недавно раскрыли, что они отслеживают злоумышленника под псевдонимом «Kr3pto», который создает и продает фишинговые комплекты, предназначенные для получения кодов безопасности в реальном времени и данных 2FA, нацеленных на финансовые учреждения Великобритании.

Также прошлым летом были арестованы двое мужчин, которым было предъявлено обвинение в использовании учетных данных сотрудников Twitter для захвата нескольких известных учетных записей Twitter, которые они использовали для мошенничества с биткойнами. В отчете, опубликованном Департаментом финансовых услуг штата Нью-Йорк, говорится, что злоумышленники легко обошли фактор аутентификации push-уведомлений, используемый Twitter. В отчете рекомендуется использовать физические ключи безопасности для блокировки таких атак.

Аппаратный подход

Ключи физической безопасности вносят новый поворот в двухфакторную аутентификацию. Вместо кода, доставленного на ваш телефон, аппаратный ключ представляет собой электронный ключ, который вы вставляете в свой корпоративный портативный компьютер или другое зарегистрированное устройство доступа. Он генерирует уникальный код, когда вы нажимаете кнопку или биометрический считыватель, аутентифицируя пользователя.

Хотя некоторые решения push-MFA могут быть уязвимы для обхода, последнее поколение ключей на основе биометрических данных использует стандарты FIDO2 и WebAuthn. соответственно, разработанный Альянсом FIDO и Консорциумом World Wide Web. FIDO2 основан на криптографических учетных данных, которые уникальны для каждого веб-сайта. Закрытый ключ остается на устройстве, а открытый ключ отправляется на сайт, на котором он зарегистрирован. Поскольку нет «общих секретов», невозможно получить полезную информацию для аутентификации, если сайт будет взломан. Чтобы использовать аналогию, это похоже на безопасность в ракетной шахте, где две отдельные стороны должны повернуть пару уникальных ключей одновременно, чтобы разрешить запуск (сценарий, который, как мы надеемся, никогда не произойдет!).

Стандарты FIDO2 и WebAuthn представляют собой интеллектуальные решения для аутентификации, эффективно предотвращающие большинство форм фишинга и других атак с захватом. Сюда входят изощренные атаки, такие как атаки «человек посередине» (MiTM), когда злоумышленник перехватывает учетные данные, манипулируя или перенаправляя сетевой трафик на поддельный портал входа в систему. Самое главное, они не используют пароли, которые являются основным источником уязвимостей.

Стоимость, сложность и человеческий фактор

Но у физических ключей есть и недостатки. Развертывание тысяч этих устройств на предприятии - дорогостоящее и сложное мероприятие. Когда требуются обновления безопасности, нет возможности выпустить патч - вам придется заменить ключи новыми. Даже если основной поставщик поставляет новые бесплатно, распространение - это головная боль с точки зрения логистики. Кроме того, список служб, поддерживаемых физическими ключами, растет, но все еще ограничен.

Наконец, есть человеческий фактор: кто никогда не терял и не терял свои ключи? В этом случае ключ аутентификации должен быть аннулирован и заказан новый. Пользователь может ждать несколько дней, прежде чем получить замену, тем временем заблокировав доступ к корпоративным ресурсам. На предприятии с десятками тысяч сотрудников неуместные ключи могут существенно повлиять на производительность.

Превращение телефона в ключ

Есть еще один способ обеспечить такую строгую аутентификацию - тот, который сочетает в себе простоту и привычность двухфакторной аутентификации на базе смартфонов с надежной безопасностью, предлагаемой стандартами FIDO2 и WebAuthn. Почему бы не использовать устройство, с которым все знакомы и постоянно носят с собой - смартфон, - чтобы обеспечить надежную криптографическую аутентификацию аналогично физическому ключу, за исключением высокой стоимости и сложности?

Чтобы увидеть, как это может работать, важно немного больше узнать о FIDO2. В стандарте задействованы три участника: веб-сайт (известный как проверяющая сторона или RP), браузер и средство проверки подлинности (ключ). WebAuthn - это протокол между RP и браузером; отдельный протокол клиент-аутентификатор (CTAP), также определенный FIDO2, существует между браузером и аутентификатором. Действия строгой аутентификации (зарегистрировать этот ключ, аутентифицировать этот вызов) работают между ключом и RP, при этом браузер передает сообщения и добавляет контекст.

CTAP определяет три транспортных уровня для роуминговых аутентификаторов: USB, Bluetooth с низким энергопотреблением (BLE) и связь ближнего поля (NFC). Однако использование транспортного уровня, не охватываемого CTAP, необходимо, чтобы браузер мог передавать сообщения FIDO2 по криптографически безопасному каналу на смартфон. Это нововведение позволяет «соединить» смартфон с браузером по этому каналу так же, как физический ключ «соединяется» с браузером по USB.

В результате получилось защищенное от фишинга решение, использующее смартфон в качестве ключа. Так что это «ракетная шахта» в безопасности. Но как насчет другой стороны уравнения - простоты?

Удобство работы с пользователем

Прелесть этого подхода заключается в том, что корпоративные пользователи уже используют свои телефоны на этапе аутентификации. Так что это без трения. В некотором смысле он просто добавляет защиту FIDO2 к уже знакомому и простому процессу. И это исключает ошибку пользователя. С существующими push-

уведомлениями MFA злоумышленник может отправить ложное уведомление, которое может облегчить захват учетной записи сотрудника. Аутентификация FIDO2 с использованием описанного выше подхода со смартфоном предотвращает это.

Хотя этот подход предлагает значительные преимущества как по сравнению с традиционными push-уведомлениями MFA, так и с физическими ключами безопасности, он не устраняет необходимости в целостном подходе к безопасности. Это включает в себя управление мобильными устройствами. Компаниям необходимо уделять пристальное внимание любым потенциальным уязвимостям самих смартфонов, включая все программное обеспечение, развернутое на них. Важно постоянно проверять каждое звено в цепочке безопасности, чтобы выявить потенциальные уязвимости. В конце концов, киберпреступники проводят дни и ночи в поисках крошечных трещин в этой цепочке, которые они могут использовать.

При правильном развертывании стратегия аутентификации, которая заменяет аппаратные ключи подходом на базе смартфона с использованием стандарта FIDO2, может устранить риск, связанный с методами обхода MFA, без ущерба для удобства. С ростом числа кибератак сочетание силы и простоты может стать лучшей защитой». ***(Tony Lauro. Beyond MFA: Rethinking the Authentication Key // Threatpost (https://threatpost.com/mfa-rethinking-authentication-key/166136/). 13.05.2021).***

***

«Google Chrome вчера неожиданно начал давать сбой для многих пользователей Windows по всему миру, что сделало браузер непригодным для использования.

Google выпустил Chrome 90.0.4430.212 10 мая, и по большей части до вчерашнего дня не было сообщений о проблемах с выпуском.

Как впервые сообщалось в Windows Latest, со вчерашнего утра пользователи начали сообщать, что расширения и вкладки Google Chrome внезапно начали давать сбой при использовании браузера.

Из-за этих сбоев субреддит Chrome и форумы продуктов Chrome начали заполняться сообщениями от людей, испытывающих эти проблемы.

«Кажется, из ниоткуда ~ 15 минут назад у меня перестал работать Google Chrome. Мои расширения разбились, и все страницы (включая страницы Chrome, такие как настройки) не загружаются. Экран полностью пустой, а вкладка просто помечена как «Без названия» с хмурящаяся папка рядом с ней», - написал вчера на Reddit пользователь.

Хотя BleepingComputer не испытывал этих сбоев, пользователи сообщают, что Chrome отображает серый экран и не может открыть страницы настроек или расширений браузера.

Кроме того, пользователи сообщают, что эти сбои происходят как в обычном режиме просмотра, так и в режиме инкогнито.

Считается, что сбои вызваны проблемой с папкой Google Chrome «% UserProfile% \ AppData \ Local \ Google \ Chrome \ User Data», которая используется

для хранения ваших данных, расширений и настроек конфигурации для браузера…». ***(Lawrence Abrams. Google Chrome is crashing worldwide on Windows 10 PCs, how to fix // Bleeping Computer® (https://www.bleepingcomputer.com/news/google/google-chrome-is-crashing-worldwide-on-windows-10-pcs-how-to-fix/). 21.05.2021).***

***

«Slack испытывает всемирный сбой, из-за которого пользователи не могут публиковать сообщения, загружать изображения или подключаться к своим серверам.

Когда некоторые пользователи пытаются подключиться к Slack, они получают сообщение об ошибке: «Что-то пошло не так, и у нас возникли проблемы с загрузкой вашего рабочего пространства».

Если вы все еще подключены к серверу Slack и пытаетесь опубликовать сообщение или загрузить изображение, вы увидите сообщение «Slack не удалось отправить это сообщение, попробуйте еще раз | Отменить»…

Slack знает о сбоях и работает над их устранением:

Проблемы с загрузкой Slack

Перезагрузка Slack (Command + R / Ctrl + R) может помочь Slack загрузиться должным образом. Однако мы еще не вышли из леса и продолжим делиться новостями здесь, когда они станут доступны.

20 мая, 17:27 UTC

У некоторых пользователей могут возникать проблемы с загрузкой Slack. Мы активно занимаемся этой проблемой и сообщим, как только у нас появятся обновления. Приносим извинения за неудобства.

20 мая, 17:17 UTC

В наших тестах перезагрузка Slack не устранила проблемы.

Обновление 20.05.21, 14:57 EST: Slack заявили, что они решили проблему, и пользователи могут перезапустить Slack для подключения к своим серверам.

Мы выпустили исправление для этой проблемы, и Slack снова работает. Если у вас по-прежнему возникают какие-либо проблемы, полностью выйдите из приложения или браузера Slack с помощью Command + Q (Mac) или Ctrl + Q (Windows / Linux), а затем снова откройте его.

Большое спасибо за то, что вы поделились с нами этим, и если у вас все еще возникают какие-либо проблемы после перезапуска, сообщите нам об этом по адресу feedback@slack.com.

20 мая, 14:36 EDT

В наших тестах BleepingComputer снова смог подключиться к серверам Slack. ***(Lawrence Abrams. Slack is down, massive outage blocks user logins and messages // Bleeping Computer® (https://www.bleepingcomputer.com/news/technology/slack-is-down-massive-outage-blocks-user-logins-and-messages/). 20.05.2021).***

***

«После восьмимесячного аудита кода новейшей информационно-развлекательной системы в автомобилях Mercedes-Benz исследователи безопасности из Tencent Security Keen Lab выявили пять уязвимостей, четыре из которых могут быть использованы для удаленного выполнения кода.

Уязвимости были обнаружены в Mercedes-Benz User Experience (MBUX), информационно-развлекательной системе, первоначально представленной на автомобилях A-класса в 2018 году, но с тех пор внедренной во всей линейке автомобилей производителя.

Уязвимости, отслеживаемые как CVE-2021-23906, CVE-2021-23907, CVE-2021-23908, CVE-2021-23909 и CVE-2021-23910, позволяют хакерам удаленно управлять некоторыми функциями автомобиля, но не с доступом к физическим функциям, таким как рулевое управление или тормозная система.

Помимо нацеливания на главное головное устройство информационно-развлекательной системы, исследователи безопасности также проанализировали T-Box Mercedes-Benz, успешно использовали некоторые из выявленных сценариев атаки и даже объединили некоторые из них для компрометации головного устройства даже в реальных транспортных средствах.

Исследователи Keen Team обнаружили использование устаревшего ядра Linux, которое было подвержено определенным атакам, уязвимости через встроенный движок JavaScript браузера и потенциальное воздействие недостатков в микросхеме Wi-Fi, стеке Bluetooth, функциях USB или включенных сторонних приложения, которые обмениваются данными с удаленными серверами.

Анализ головного устройства выявил ряд уязвимостей, связанных с переполнением кучи, в том числе две, которые могут привести к утечке памяти и выполнению кода; возможность настроить удаленную оболочку с использованием уязвимости в предоставленном браузере; отсутствие SELinux или AppArmor, что позволило использовать ошибку ядра Linux для повышения привилегий; и несколько дополнительных вопросов.

После первоначального компромисса, который включал настройку постоянной веб-оболочки с привилегиями root, исследователи смогли разблокировать определенные функции автомобиля и его противоугонную защиту, внедрить постоянный бэкдор и даже выполнить действия по управлению автомобилем.

Отправляя определенные сообщения CAN, исследователи смогли управлять окружающим освещением в автомобиле, управлять лампами для чтения, открывать солнцезащитный козырек и управлять освещением для пассажиров на заднем сиденье, но не смогли взять под контроль автомобиль.

Сценарии атак с использованием T-Box будут использовать включенный чип Wi-Fi; микросхема STA8090, работающая как ИС приемника; CAN-шина; или LTE-соединение (через базовую полосу пропускания Huawei Balong). Однако меры

безопасности, внедренные Mercedes-Benz, предотвратили атаки от базовой полосы или перехода LTE на GSM (до команд управления транспортным средством).

В ходе своего анализа исследователи обнаружили в T-Box две проблемы, которыми можно злоупотреблять при атаках. Один из них может быть использован для выполнения кода на микросхеме, которая принимает сообщения от ЦП, преобразует их и отправляет на шину CAN. Таким образом, они могли отправлять произвольные сообщения CAN на шину CAN. Они также смогли прошить прошивку на чипе с пропатченной версией для сохранения.

В своем отчете исследователи описывают как успешные, так и неудачные попытки атак, а также предоставляют подробные технические детали протестированного оборудования и программного обеспечения.

Об обнаруженных уязвимостях было сообщено поставщику (Daimler, владеющему Mercedes-Benz) в ноябре 2020 года. Патчи начали развертываться в конце января 2021 года…». ***(Ionut Arghire. Researchers Find Exploitable Bugs in Mercedes-Benz Cars // Wired Business Media (https://www.securityweek.com/researchers-find-exploitable-bugs-mercedes-benz-cars). 18.05.2021).***

***

«Во вторник Adobe предупредила, что зияющая дыра в безопасности в одном из наиболее широко используемых программных продуктов была использована в «ограниченных атаках, нацеленных на пользователей Adobe Reader в Windows».

Подтверждение Adobe атаки нулевого дня было похоронено в бюллетене по безопасности, в котором задокументировано не менее 11 уязвимостей безопасности, затронувших Adobe Acrobat и Reader на платформах Windows и MacOS.

«Эти обновления устраняют множество критических и важных уязвимостей. Успешная эксплуатация может привести к выполнению произвольного кода в контексте текущего пользователя», - говорится в бюллетене.

Adobe Acrobat Reader - широко используемая бесплатная программа для просмотра, создания, заполнения, печати и форматирования файлов в формате Portable Document Format (PDF). Программное обеспечение уже давно является хорошей мишенью для продвинутых злоумышленников, проводящих целевые атаки.

Недостаток уязвимости - CVE-2021-28550 - описывается как проблема повреждения памяти, связанная с использованием после освобождения, которая была обнаружена и анонимно сообщена в Adobe. Никаких дополнительных сведений об активной эксплуатации компания не предоставила.

Мега-патч от Adobe фиксирует по крайней мере 23 недостатка в ряде продуктов, включая пару дыр в безопасности в Adobe Experience Manager, три изъяна в безопасности в Adobe InDesign и пять серьезных ошибок в Adobe Illustrator.

Компания также исправила уязвимости системы безопасности в Adobe InCopy и Adobe Genuine Service». ***(Ryan Naraine. Adobe: Windows Users Hit by PDF***

Reader Zero-Day // Wired Business Media (https://www.securityweek.com/adobe-windows-users-hit-pdf-reader-zero-day). 11.05.2021).

***

«По словам исследователей, киберпреступники начали поиск уязвимых серверов Exchange в Интернете в течение пяти минут после публикации рекомендаций Microsoft по безопасности.

Согласно обзору данных об угрозах, собранных корпоративными компаниями в период с января по март этого года, составленному в отчете Palo Alto Networks об угрозах Cortex Xpanse Attack Surface за 2021 год и опубликованному в среду, злоумышленники быстро не смогли найти сервер созрели для эксплуатации.

Когда критические уязвимости в широко распространенном программном обеспечении становятся общедоступными, это может вызвать гонку между злоумышленниками и ИТ-администраторами: одна цель - найти подходящие цели - особенно когда доступен проверочный код (PoC) или ошибка тривиальна для использования - и ИТ-персонал для оценки рисков и внедрения необходимых исправлений.

В отчете говорится, что, в частности, уязвимости нулевого дня могут вызвать сканирование злоумышленником в течение всего 15 минут после публичного раскрытия информации.

Исследователи из Пало-Альто говорят, что злоумышленники «работали быстрее», когда дело касалось Microsoft Exchange, и сканирование было обнаружено не более чем за пять минут.

2 марта Microsoft сообщила о существовании четырех уязвимостей нулевого дня в Exchange Server. Четыре проблемы безопасности, совокупно влияющие на локальный Exchange Server 2013, 2016 и 2019, были использованы китайской группой расширенных постоянных угроз (APT) Hafnium - и другие APT, включая LuckyMouse, Tick и Winnti Group, быстро последовали ее примеру.

Раскрытие информации о системе безопасности вызвало волну атак, и спустя три недели они все еще продолжались. В то время исследователи F-Secure заявили, что уязвимые серверы «взламывают быстрее, чем мы можем сосчитать».

Возможно, что общедоступность дешевых облачных сервисов помогла не только APT, но и более мелким группам киберпреступников и отдельным лицам воспользоваться преимуществами новых уязвимостей по мере их появления.

«Вычисления стали настолько недорогими, что потенциальному злоумышленнику нужно потратить всего около 10 долларов на аренду облачных вычислительных мощностей, чтобы провести неточное сканирование всего Интернета на предмет уязвимых систем», - говорится в отчете. «Из большого количества успешных атак мы знаем, что злоумышленники регулярно выигрывают гонки, чтобы исправить новые уязвимости».

В исследовании также подчеркивается, что протокол удаленного рабочего стола (RDP) является наиболее частой причиной слабости безопасности корпоративных сетей, на которую приходится 32% общих проблем безопасности, что является особенно проблемной областью, поскольку многие компании за

последний год быстро перешли на облачные технологии. чтобы позволить своим сотрудникам работать удаленно.

«Это вызывает беспокойство, потому что RDP может обеспечить прямой административный доступ к серверам, что делает его одним из наиболее распространенных шлюзов для атак программ-вымогателей», - отмечается в отчете. «Они представляют собой низко висящие плоды для злоумышленников, но есть повод для оптимизма: большинство обнаруженных нами уязвимостей можно легко исправить». ***(Charlie Osborne. Cybercriminals scanned for vulnerable Microsoft Exchange servers within five minutes of news going public // ZDNet (https://www.zdnet.com/article/cybercriminals-scanned-for-vulnerable-microsoft-exchange-servers-within-five-minutes-of-news-going-public/). 19.05.2021).***

***

«Миллионы домашних хозяйств в Великобритании используют старые широкополосные маршрутизаторы, которые могут стать жертвой хакеров, согласно новому исследованию, проведенному наблюдательной службой потребителей Which? в сотрудничестве с исследователями безопасности.

Что после опроса более 6000 взрослых? идентифицировала 13 старых маршрутизаторов, которые до сих пор широко используются потребителями по всей стране, и отправила их специалистам по безопасности из консалтинговой компании Red Maple Technologies. Было обнаружено, что девять из этих устройств не соответствуют современным стандартам безопасности.

По оценкам Which?, до 7,5 миллионов пользователей в Великобритании потенциально могут быть затронуты, поскольку уязвимые маршрутизаторы предоставляют злоумышленникам возможность шпионить за людьми во время их просмотра или направлять их на спамерские веб-сайты.

Одна из основных проблем связана с отсутствием обновлений, которые получают старые маршрутизаторы. Некоторые модели, которые использовали респонденты, не обновлялись с 2018 года, а в некоторых случаях даже с 2016 года.

Из-за отсутствия обновлений были отмечены устройства Sky SR101 и SR102, Virgin Media Super Hub и Super Hub 2, а также TalkTalk HG523a, HG635 и HG533.

Большинство провайдеров, когда с ними связались с компанией Which?, сказали, что они регулярно отслеживают устройства на предмет угроз и обновляют их при необходимости.

Virgin отклонила это исследование, заявив, что 90% ее клиентов используют маршрутизаторы более позднего поколения. TalkTalk сообщил ZDNet, что ему нечего добавить к релизу.

Исследователи также обнаружили уязвимость локальной сети в Brightbox 2 от EE, которая могла позволить хакеру получить полный контроль над устройством.

Представитель EE сказал ZDNet: «Мы очень серьезно относимся к безопасности наших продуктов и услуг. Как подробно описано в отчете, это уязвимость с очень низким уровнем риска для небольшого числа наших клиентов, которые все еще используют EE Brightbox 2. (…) Мы хотели бы заверить клиентов EE Brightbox 2 в том, что мы работаем над исправлением службы, которое мы

будем распространять на затронутые устройства в предстоящем фоновом обновлении».

Вдобавок BT Group, которой принадлежит EE, сообщила Which? что старые маршрутизаторы по-прежнему получают исправления безопасности при обнаружении проблем. Исследователи Red Maple обнаружили, что недавно были обновлены старые устройства BT, а также маршрутизаторы Plusnet.

Служба контроля потребителей сообщила, что потребители, которые все еще используют одну из моделей маршрутизаторов, которые больше не обновляются, как можно скорее попросили своих поставщиков новое устройство.

Однако это ни в коем случае не является данностью: хотя Virgin Media заявляет, что предоставляет бесплатные обновления для клиентов со старыми маршрутизаторами, политика не всегда так ясна с другими поставщиками.

«Не повредит спросить», - сказала Холли Хеннесси, старший научный сотрудник компании Which?. «Хотя интернет-провайдер не обязан предоставлять вам новый маршрутизатор бесплатно, если вы позвоните и объясните свои опасения, вам может повезти, особенно если ваш маршрутизатор довольно старый».

Для потребителей, чьи контракты скоро истекают, Хеннесси предложил запросить новый маршрутизатор в качестве условия для работы с данным провайдером - и рассмотреть возможность переключения, если запрос не будет выполнен.

СЛАБЫЕ ПАРОЛИ ОСТАЮТСЯ ГЛАВНОЙ ПРОБЛЕМОЙ

Помимо отказа в регулярных обновлениях, было обнаружено, что многие старые маршрутизаторы поставляются со слабыми паролями по умолчанию, которые могут быть легко угаданы хакерами и предоставлять доступ посторонним.

Так было с теми же маршрутизаторами TalkTalk и Sky, а также с Virgin Media Super Hub 2 и Vodafone HHG2500.

Первое, что нужно сделать для потребителей, владеющих одной из этих моделей, - это сменить пароль на более надежный вместо пароля по умолчанию, сказал Which?.

Организация, по сути, призывает правительство запретить пароли по умолчанию и запретить производителям разрешать потребителям устанавливать слабые пароли в рамках нового законодательства, предложенного в прошлом месяце.

В рамках усилий по обеспечению безопасности устройств британский департамент цифровых технологий, культуры, средств массовой информации и спорта объявил о новом законе, который запрещает производителям использовать пароли по умолчанию, такие как «пароль» или «администратор», чтобы лучше защитить потребителей от кибератак.

Будущий закон также сделает обязательным сообщать клиентам, как долго их новый продукт будет получать обновления безопасности. Кроме того, производители должны будут предоставить общедоступные контактные данные, чтобы упростить сообщение об уязвимостях безопасности в продуктах.

В том же духе, Which? призвала к большей прозрачности от интернет-провайдеров. Организация заявила, что провайдеры должны быть более

откровенными в отношении того, как долго маршрутизаторы будут получать обновления прошивки и безопасности, и должны активно обновлять клиентов, которые подвергаются риску.

Похоже, что только Sky, Virgin Media и Vodafone имеют веб-страницу, позволяющую исследователям сообщать об уязвимостях, обнаруженных в продуктах компаний, согласно Which?». ***(Daphne Leprince-Ringuet. Millions of older broadband routers have these security flaws, warn researchers // ZDNet (https://www.zdnet.com/article/millions-of-older-broadband-routers-have-these-security-flaws-warn-researchers/). 06.05.2021).***

***

«Профессор информатики из Швеции обнаружил уязвимость выполнения произвольного кода в универсальной машине Тьюринга, одной из самых ранних компьютерных разработок в истории, хотя он признает, что это «не имеет никакого отношения к реальному миру».

В статье, опубликованной в академическом репозитории ArXiv, Понтус Джонсон, профессор Королевского технологического института KTH в Стокгольме, Швеция, весело объяснил, что его результаты не могут быть использованы в реальном сценарии, потому что они относились конкретно к реализации моделируемой Универсальной машины Тьюринга (UTM) 1967 года, разработанной покойным Марвином Мински, соучредителем академической дисциплины искусственного интеллекта.

И все же то, что на самом деле представляет этот забавный маленький каперз, - это философский вопрос: если одна из простейших концепций компьютера уязвима для вмешательства пользователя, где в процессе проектирования мы должны начать попытки реализовать функции безопасности?

«Универсальная машина Тьюринга обычно считается простейшей и самой абстрактной моделью компьютера», - писал Джонсон в своей статье. Воспользовавшись отсутствием проверки ввода в UTM спецификации Мински, он смог обманом заставить его запустить созданную им программу.

Спецификация Мински описывает ленточную машину, которая считывает и выполняет очень простые программы с имитированной ленты. Инструкции на ленте перемещают имитацию головки чтения ленты влево или вправо по самой «ленте», которая представлена в виде однострочной буквенно-цифровой строки. Хотя пользователи могут вводить данные в начале ленты, в модели UTM они не должны изменять следующую программу.

«Независимо от исторического аспекта, факт [состоит] в том, что самый простой [компьютер], который мы можем описать, похоже, имел склонность к уязвимости», - сказал Джонсон The Register.

Безопасность (если ее можно так назвать) для UTM состоит из одной цифры, которая сообщает машине, что «пользовательский ввод здесь заканчивается, все, что находится после этой точки, является исполняемым с параметрами, которые вы только что прочитали».

Эксплойт Джонсона был так же прост, как написать символ «здесь заканчивается ввод» в поле ввода пользователя, а затем написать свою

собственную программу после него. UTM выполняет это и пропускает намеченную программу.

Параллели с современными уязвимостями очевидны: немного увеличьте ее сложность, и это имеет все признаки уязвимости SQL-инъекции, например, или любого другого незащищенного или неэкранированного поля ввода пользователя.

Джонсон сказал The Register сегодня: «В этом случае, как и во многих случаях, уязвимость основана на сбивании с толку машины... в академических кругах мы, ученые, любим начинать с основного принципа: продемонстрировать что-то для небольшой системы, тогда, может быть, это правда для система большего размера. Мне кажется, что для самой маленькой системы существует эта внутренняя уязвимость, эта склонность к уязвимости».

Compsci prof продолжил: «Очевидно, Марвин Мински не имел намерения [создать] безопасную или уязвимую систему. Тем не менее, то, что произошло, было [она] была уязвимой».

С философской точки зрения уязвимость Джонсона (получившая обозначение CVE-2021-32471) вызывает более глубокие вопросы, над которыми должны задуматься разработчики аппаратного и микропрограммного обеспечения, он сказал нам: «Некоторые люди говорят, что безопасность должна быть встроена с самого начала; вы можете не добавлю это позже, но в данном случае, все возможные средства смягчения этого воздействия, которые я мог придумать, должны быть надстройками, вы не можете встроить их в эту машину.

«И если это мать всех компьютеров, то мне кажется, что вы не можете встроить безопасность с самого начала».

Профессор Алан Вудворд из Университета Суррея высказал мнение Эль Регу: «Это интересная и провокационная мысль о том, существует ли какая-то фундаментальная причина количества конкретных атак, которые мы наблюдаем. Я не думаю, что нам нужно паниковать, что там это некий фундаментальный недостаток современной компьютерной архитектуры, скорее это напоминание о том, что сложность несет в себе собственные угрозы».

Глядя конкретно на уязвимость Джонсона, он прокомментировал: «Интересно, что это, кажется, больше указывает на проблемы с интерпретациями / реализациями машины Тьюринга. Кажется, это подтверждает пословицу о том, что ничто не является полностью безопасным после того, как оно действительно реализовано». ***(Gareth Corfield. Compsci boffin publishes proof-of-concept code for 54-year-old zero-day in Universal Turing Machine // The Register(https://www.theregister.com/2021/05/11/turing_machine_0day_no_patch_available/). 11.05.2021).***

***

«Злоумышленники могут использовать недавно обнаруженную уязвимость сервера доменных имен (DNS), широко известную как TsuNAME, в качестве вектора усиления в крупномасштабных атаках распределенного отказа в обслуживании (DDoS) на основе отражения, нацеленных на авторитетные DNS-серверы.

Проще говоря, авторитетные DNS-серверы переводят веб-домены в IP-адреса и передают эту информацию рекурсивным DNS-серверам, которые запрашиваются веб-браузерами обычных пользователей при попытке подключения к определенному веб-сайту.

Авторитетные DNS-серверы обычно управляются как государственными, так и частными организациями, включая интернет-провайдеров (ISP) и мировых технологических гигантов.

Использование DNS-запросов к авторитетным серверам DDoS

Злоумышленники, пытающиеся использовать уязвимость TsuNAME DNS, нацелены на уязвимые рекурсивные распознаватели и заставляют их перегружать авторитетные серверы большим количеством вредоносных DNS-запросов.

«Резолверы, уязвимые для TsuNAME, будут отправлять непрерывные запросы на авторитетные серверы, у которых есть циклические зависимые записи», - поясняют исследователи в своих рекомендациях по безопасности. [PDF]

«В то время как один преобразователь вряд ли перегрузит авторитетный сервер, совокупный эффект от множества зацикливающихся уязвимых рекурсивных преобразователей тоже может сработать».

Возможное воздействие после такой атаки может заключаться в удалении непосредственно затронутых авторитетных DNS-серверов, что может привести к отключению Интернета по всей стране, если затронут домен верхнего уровня с кодом страны (ccTLD).

«Что делает TsuNAME особенно опасным, так это то, что его можно использовать для проведения DDoS-атак на критически важную инфраструктуру DNS, такую как крупные TLD или ccTLD, что может повлиять на сервисы конкретной страны», - поясняет исследовательский документ [PDF], опубликованный после раскрытия информации.

По словам исследователей, популярные DNS-преобразователи, такие как Unbound, BIND и KnotDNS, не подвержены ошибке TsuNAME DNS.

Доступны меры по смягчению последствий

«Мы наблюдали 50% -ное увеличение трафика из-за использования TsuNAME в трафике.nz, что было связано с ошибкой конфигурации, а не с реальной атакой», - добавили исследователи.

В отчетах также упоминаются события TsuNAME, влияющие на ccTLD в EC, которые увеличили входящий трафик DNS в 10 раз из-за всего лишь двух доменов с неправильной конфигурацией циклической зависимости.

Однако злоумышленники, имеющие доступ к нескольким доменам и ботнету, могут нанести гораздо больший ущерб, если неправильно настроят свои домены и начнут проверять открытые резолверы.

К счастью, доступны средства защиты от TsuNAME, и они требуют изменений в программном обеспечении рекурсивного преобразователя, «путем включения кодов обнаружения петель и кэширования циклически зависимых записей».

Авторитетные операторы серверов также могут снизить влияние атак TsuNAME с помощью инструмента CycleHunter с открытым исходным кодом,

который помогает предотвратить такие события, обнаруживая и упреждающе исправляя циклические зависимости в их зонах DNS.

Исследователи уже использовали CycleHunter для проверки около 184 миллионов доменов в семи TLD, что позволило им обнаружить 44 циклически зависимые записи NS (вероятно, вызванные неправильной конфигурацией) примерно на 1400 доменных именах, которые могут быть использованы в атаках». ***(Sergiu Gatlan. New TsuNAME DNS bug allows attackers to DDoS authoritative DNS servers // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-tsuname-dns-bug-allows-attackers-to-ddos-authoritative-dns-servers/). 06.05.2021).***

***

«Исследователи из компании Claroty, занимающейся промышленной кибербезопасностью, выявили серьезную уязвимость, которая может быть использована удаленным злоумышленником, не прошедшим проверку подлинности, для взлома некоторых программируемых логических контроллеров (ПЛК) производства Siemens.

Уязвимость отслеживается как CVE-2020-15782 и описывается как проблема обхода защиты памяти с высокой степенью серьезности, которая позволяет злоумышленнику с сетевым доступом к TCP-порту 102 записывать или читать данные в защищенных областях памяти.

Siemens заявляет, что дыра в безопасности влияет на его процессоры SIMATIC S7-1200 и S7-1500. Немецкий промышленный гигант выпустил обновления прошивки для некоторых затронутых устройств и предоставил обходные пути для продуктов, для которых еще не выпущены исправления.

По словам Claroty, уязвимость может быть использована для выполнения собственного кода на ПЛК Siemens S7 путем обхода песочницы, в которой обычно выполняется инженерный код, и получения прямого доступа к памяти устройства.

Исследователи компании показали, как злоумышленник может обойти защиту и записать шелл-код прямо в защищенную память. Исследователи утверждают, что атаку, использующую эту уязвимость, будет сложно обнаружить.

«Выход из песочницы означает, что злоумышленник сможет читать и писать из любого места на ПЛК, а также может исправить существующий код операции виртуальной машины в памяти с помощью вредоносного кода для получения root-прав на устройстве», - пояснили исследователи Claroty в сообщении в блоге, опубликованном в пятницу.

«Claroty, например, смогла внедрить шелл-код ARM / MIPS непосредственно во внутреннюю структуру операционной системы таким образом, что, когда операционная система использует определенный код операции, который мы выбрали, наш вредоносный шелл-код выполнялся, давая нам возможность удаленного выполнения кода. Мы использовали эту технику для установки программы уровня ядра с некоторыми функциями, которые полностью скрыты от операционной системы», - добавили они». ***(Eduard Kovacs. Newly Disclosed Vulnerability Allows Remote Hacking of Siemens PLCs // Wired Business Media (https://www.securityweek.com/newly-disclosed-vulnerability-allows-remote-hacking-siemens-plcs). 28.05.2021).***

***

«Google подробно описал свою работу по обнаружению новой уязвимости Rowhammer, получившей название «Half-Double», которая развивает стиль атаки на память DRAM, о котором впервые было сообщено в 2014 году, и предполагает, что проблема Rowhammer не исчезнет в ближайшее время.

Атака Rowhammer необычна, потому что она направлена на то, чтобы вызвать «перевороты битов» путем быстрого и многократного доступа к данным в одной строке памяти на микросхеме RAM, чтобы создать электрический заряд, который изменяет данные, хранящиеся в других адресах в соседней «строке памяти» на кристалле. Атакующие строки памяти называются «агрессорами», а строки, в которых происходят перевороты битов, называются «жертвами».

За годы, прошедшие с момента обнаружения первой атаки Rowhammer, исследователи продемонстрировали множество способов использования этой техники для изменения данных, хранящихся на картах RAM, включая поколения DDR3 и DDR4.

Первоначально ограничиваясь сценариями, в которых злоумышленник имел физический доступ к цели, исследователи в конечном итоге показали, что атака Rowhammer может быть проведена удаленно через Интернет и использовать эту технику для получения контроля над виртуальными машинами Linux в облаке.

Как объяснили исследователи Google Project Zero (GPZ) в 2015 году, злоумышленники Rowhammer работают, потому что ячейки DRAM постепенно становятся меньше и ближе друг к другу. Миниатюризация и возможность упаковать больший объем памяти усложнили предотвращение электрического взаимодействия ячеек DRAM друг с другом.

«Доступ к одному месту в памяти может нарушить соседние места, вызывая утечку заряда в соседние ячейки или из них. При достаточном количестве обращений это может изменить значение ячейки с 1 на 0 или наоборот», - объяснили исследователи GPZ относительно переворота битов.

Half-Double, который Google подробно описывает в PDF-файле на GitHub, «использует ухудшающуюся физику некоторых из новых чипов DRAM для изменения содержимого памяти», - объясняют исследователи Google в новом блоге.

Стиль атаки сравним со спекулятивным исполнением атак на ЦП (Spectre и Meltdown), но скорее сосредоточен на проектных уязвимостях в DRAM. Последствия могут быть довольно неприятными, если злоумышленник успешно воспользуется этими проблемами проектирования.

«В качестве электрического соединительного явления внутри самого кремния, Rowhammer позволяет потенциальному обход политики защиты оборудования и памятей программного обеспечения. Это может позволить ненадежному коду, чтобы вырваться из его песочницы и взять полный контроль над системой,» запись исследовательской группы компании Google, которая включает Салмана Кази, Юнгу Кима, Николаса Бойча, Эрика Шиу и Маттиаса Нисслера.

Ким, ныне инженер-программист в Google, была одним из исследователей, сообщивших о первой уязвимости Rowhammer.

Half-Double расширяет исходную атаку Rowhammer, которая может вызвать перевороты битов на расстоянии одного ряда DRAM. Полудабль показывает, что ряды агрессоров могут вызывать перевороты битов в более удаленных рядах жертв.

«С помощью Half-Double мы наблюдали, как эффекты Роухаммера распространяются на ряды за пределами соседних соседей, хотя и с меньшей силой», - отмечает команда.

«Учитывая три последовательных строки A, B и C, мы смогли атаковать C, направив очень большое количество обращений к A, а также всего несколько (~ десятков) к B. На основании наших экспериментов, доступы к B имели нелинейный эффект стробирования, при котором они, кажется, «переносят» эффект Роухаммера A на C.»

Half-Double интересен тем, что это свойство основной кремниевой подложки, и предполагает, что увеличение плотности ячеек означает, что уязвимости Rowhammer сохранятся. Они добавляют, что Half-Double также отличается от атаки TRRespass на ОЗУ DDR4, описанной в 2020 году, которая опиралась на обратный инжиниринг, чтобы подорвать некоторые меры защиты Rowhammer, которые поставщики DRAM внедрили для предотвращения этих атак в DDR4.

«Вероятно, это указывает на то, что электрическая связь, ответственная за Роухаммер, является свойством расстояния, которое эффективно становится сильнее и увеличивает дальность действия по мере уменьшения геометрии ячеек. Возможны расстояния, превышающие два», - отмечают исследователи.

Кроме того, Google сотрудничает с торговой организацией полупроводниковой техники JEDEC, чтобы найти способы смягчения последствий для Rowhammer». ***(Liam Tung. This weird memory chip vulnerability is even worse than we realised // ZDNet (https://www.zdnet.com/article/this-weird-memory-chip-vulnerability-is-even-worse-than-we-realised/). 26.05.2021).***

***

«Apple выпустила обновления безопасности для macOS, которые исправляют ошибку в настройках конфиденциальности и, по словам Apple, «могли активно эксплуатироваться», что могло позволить вредоносным приложениям записывать экран Mac.

Это довольно крупное обновление, устраняющее 73 уязвимости, в том числе одну в структуре Transparency Consent and Control (TCC), которая позволяет вредоносным программам обходить средства контроля конфиденциальности системы. Apple обратилась к обходу TCC в macOS Big Sur версии 11.4.

«Apple известно об отчете о том, что эта проблема могла активно использоваться», - говорится в сообщении об ошибке CVE-2021-30713, влияющей на TCC.

TCC предоставляет диалоговые подсказки для действий, чувствительных к безопасности и конфиденциальности, таких как приложение, записывающее экран компьютера, или когда приложениям предоставляется доступ к веб-камере и микрофону.

Фирма по безопасности Jamf опубликовала отчет об ошибке и сообщает, что обнаружила, что обход активно используется при анализе вредоносного ПО XCSSET.

«Группа обнаружения отметила, что после установки в системе жертвы XCSSET использовал этот обход специально для того, чтобы делать скриншоты рабочего стола пользователя, не требуя дополнительных разрешений», - говорится в сообщении.

В августе Trend Micro обнаружила, что XCSSET нацелен на разработчиков Mac через зараженные проекты Xcode.

Вредоносная программа находит приложение в системе и подключается к нему, унаследовав его разрешения.

«Во время тестирования Jamf было определено, что эта уязвимость не ограничивается разрешениями на запись экрана. Множество различных разрешений, которые уже были предоставлены приложению-донору, могут быть переданы злонамеренно созданному приложению», - отметил Джамф.

«Рассматриваемый эксплойт может позволить злоумышленнику получить полный доступ к диску, запись экрана или другие разрешения, не требуя явного согласия пользователя - что является поведением по умолчанию».

Apple также выпустила исправления безопасности в обновлении iOS 14.6 для iPhone и iPad, которое включало 30 исправлений безопасности.

Национальный центр кибербезопасности Великобритании (NCSC) предоставил один отчет об уязвимости для ошибки CVE-2021-30715, которая позволяла вредоносному сообщению создать отказ в обслуживании на устройстве iOS.

Обновления Apple от 24 мая включают Safari 14.1.1, в котором исправлено 10 недостатков безопасности, которые могут быть использованы вредоносными веб-сайтами». ***(Liam Tung. Apple just fixed a security flaw that allowed malware to take screenshots on Macs // ZDNet (https://www.zdnet.com/article/apple-just-fixed-a-security-flaw-that-allowed-malware-to-take-screenshots-on-macs/). 26.05.2021).***

***

«Сертифицированные файлы в формате переносимых документов (PDF) используются для безопасного подписания соглашений между двумя сторонами, сохраняя при этом целостность содержимого, но новый отчет показал, что средства защиты в большинстве сертифицированных PDF-приложений были недостаточными, и организации подвергались ряду атак.

Исследователи из Рурского университета в Бохуме объяснили, что в сертифицированных PDF-файлах для аутентификации документа используются две определенные подписи: подпись утверждения и подпись сертификации. Сертификационные подписи являются более гибкими и предназначены для обработки сложных соглашений между несколькими сторонами и позволяют вносить некоторые изменения в документ в пределах набора параметров, сохраняя при этом его действительность.

Неудивительно, что в сертифицированных сигнатурах команда обнаружила уязвимости к двум конкретным новым атакам, которые они назвали: «Evil

Annotation» (EAA) и «Sneaky Signature» (SSA). Оба позволяют злоумышленнику накладывать вредоносный контент (PDF) поверх сертифицированной информации, не показывая никаких признаков того, что она была изменена.

Новые сертифицированные атаки на PDF

EAAs отображает вредоносный контент в аннотациях документа, а затем отправляет его с неповрежденной цифровой подписью. SSA добавляют вредоносное содержимое поверх легитимного содержимого самого PDF-файла.

Команда заявила, что результаты оценки 26 самых популярных PDF-приложений вызывают «тревогу».

«Только в 2 случаях мы не смогли найти уязвимости; 15 зрителей были уязвимы для EAA, 8 - для SSA, включая Adobe, Foxit и LibreOffice», - говорится в отчете. «Мы дополнительно проанализировали реализацию приложений сертификации PDF в соответствии со стандартами и обнаружили проблемы в 11 из них».

У Adobe был дополнительный недостаток, который позволял сертифицированным документам выполнять код JavaScript, открывая этим пользователям возможность выполнять атаки путем внедрения кода.

«Например, высокоуровневый JavaScript может вызывать произвольный URL без подтверждения пользователя, чтобы деанонимизировать пользователя. Наше исследование показывает, что такой код также выполняется, если он добавляется как разрешенное инкрементное обновление. Мы первыми обнаружили, что такое поведение позволяет злоумышленникам напрямую внедрять вредоносный код в сертифицированный документ.

Команда заявила, что раскрыла свои выводы соответствующим поставщикам и предоставила CERT-Bund (BSI) исчерпывающий отчет об уязвимостях, включая эксплойты. В отчете также перечислены конкретные сертифицированные недостатки безопасности PDF, обнаруженные в каждом приложении.

«Adobe, Foxit и LibreOffice быстро отреагировали и предоставили исправления на конец 2020 года (CVE-2020-35931) или начало 2021 года (CVE2021-28545, CVE-2021-28546)», - говорится в отчете. «Adobe устранила уязвимость внедрения кода в начале ноября 2020 года в патче, выходящем за рамки обычного цикла обновления (CVE-2020-24432). В настоящее время мы участвуем в процессе стандартизации через Немецкую национальную организацию по стандартизации (DIN) и Международную организацию по стандартизации (ISO), чтобы устранить указанные атаки в следующей спецификации PDF».

Остановка сертифицированных атак на PDF-файлы

Чтобы предотвратить злонамеренные атаки на аннотации, исследователи рекомендуют администраторам запретить три особо рискованных аннотации, позволяющих добавлять текст или изображения в сертифицированный PDF-файл: «FreeText, Stamp and Redact».

Скрытые подписи можно заблокировать за счет уменьшения разрешений, но это не гарантия того, что SSA не пройдут. В отчете говорится, что определенные поля подписи предлагают дополнительный уровень защиты.

«Поля подписи должны быть настроены в определенных местах в документе PDF до того, как документ будет сертифицирован», - поясняется в отчете.

«Последующее добавление полей подписи должно наказываться недействительным статусом сертификации. В противном случае его всегда можно использовать для добавления текста или изображений, включенных в подпись, в любом месте».

Внедрение кода Adobe JavaScript сложнее, поскольку в большинстве случаев выполнение начинается в момент открытия документа. «Единственное требование - жертва полностью доверяет сертификату, который используется для удостоверения PDF-документа», - говорится в сообщении.

Ранее в этом месяце Adobe Acrobat выпустила патч для устранения ошибки нулевого дня, нацеленной на пользователей Windows. Всего через несколько дней исследователи из Microsoft Security Intelligence (MSI) обнаружили, что PDF-файлы использовались злоумышленниками для доставки инструмента удаленного доступа StrRAT на основе Java (RAT), используемого для кражи учетных данных, регистрации нажатий клавиш и удаленного управления зараженными системами.

Гибкость, обеспечиваемая сертифицированными подписями, представляет собой огромный, потенциально катастрофический риск безопасности для многих организаций, и в отчете содержится призыв к приложениям PDF работать быстро, чтобы предлагать широкомасштабные исправления.

«Исследовательское сообщество боролось с аналогичными проблемами с другими форматами данных, такими как XML или электронная почта, но пока не нашло удовлетворительного решения», - заявили они. «В случае PDF, спецификация должна быть обновлена, чтобы решить эти проблемы». ***(Becky Bracken. PDF Feature 'Certified' Widely Vulnerable to Attack // Threatpost (https://threatpost.com/pdf-certified-widely-vulnerable-to-attack/166505/). 26.05.2021).***

***

«Компания Hewlett Packard Enterprise (HPE) исправила критическую ошибку удаленного выполнения кода нулевого дня (RCE) в своем программном обеспечении HPE Systems Insight Manager (SIM) для Windows, о котором она первоначально сообщила в декабре.

HPE SIM - это инструмент, который обеспечивает автоматизацию удаленной поддержки и управление для различных серверов HPE, включая HPE ProLiant Gen10 и HPE ProLiant Gen9, а также для систем хранения и сетевых продуктов.

В четверг компания обновила свои первоначальные рекомендации по безопасности. Более месяца назад, 20 апреля, HPE выпустила более ранний комплект исправлений для SIM-карты, устраняющий уязвимость.

Это уязвимость с чрезвычайно высоким риском, которая может позволить злоумышленникам без прав удаленно выполнять код: отслеживается как CVE-2020-7200, он имеет рейтинг 9,8 из максимумов 10. Он обнаружен в последних версиях (7.6.x) HPE Программное обеспечение SIM-карты и влияет только на версию Windows.

Эта ошибка допускает атаки низкой сложности, не требующие взаимодействия с пользователем. Как объяснил Packet Storm, он позволяет злоумышленникам выполнять код в контексте процесса hpsimsvc.exe HPE SIM, который выполняется с административными привилегиями.

Проблема возникает из-за невозможности проверить данные во время процесса десериализации, когда пользователь отправляет запрос POST на страницу / simsearch / messagebroker / amfsecure. «Этот модуль использует эту уязвимость, используя устаревшую копию Commons Collection, а именно 3.2.2, которая поставляется с HPE SIM, чтобы получить удаленное выполнение кода в качестве административного пользователя, работающего с HPE SIM», - сообщает Packet Storm. Отсутствие надлежащей проверки данных, предоставленных пользователем, может привести к десериализации ненадежных данных, что позволит злоумышленникам выполнить код на серверах, на которых запущено уязвимое программное обеспечение SIM-карты.

Есть обходной путь

HPE рекомендует как можно скорее перейти на него, когда дело доходит до развертывания этого исправления. Для тех, кто не может немедленно развернуть обновление безопасности CVE-2020-7200 на уязвимых системах, HPE предоставила меры по смягчению последствий, которые включают удаление функции «Федеративный поиск» и «Федеративная конфигурация CMS», которые позволили уязвимость.

Обходной путь для существующей системы до пакета обновления исправлений, выпущенного 20 апреля:

Остановить службу HPE SIM

Удалить <C:\Program Files\HP\Systems Insight Manager\jboss\server\hpsim\deploy\simsearch.war>файл из установленного пути SIMdel /Q /F C:\Program Files\HP\Systems Insight Manager\jboss\server\hpsim\deploy\simsearch.war

Перезапустите службу HPE SIM.

Подождите, пока откроется веб-страница HPE SIM «https: // SIM_IP: 50000», и выполните следующую команду из командной строки: mxtool -r -f tools\multi-cms-search.xml 1>nul 2>nul

Пользователи HPE SIM больше не смогут использовать функцию федеративного поиска после использования обходного пути». ***(Lisa Vaas. HPE Fixes Critical Zero-Day in Server Management Software // Threatpost (https://threatpost.com/hpe-fixes-critical-zero-day-sim/166543/). 28.05.2021).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Компания Softprom анонсировала подписание дистрибьюторского контракта с Red Sift, разработчиком решения для защиты и идентификации почтовых сообщений. Соглашение охватывает территорию Армении, Австрии, Азербайджана, Беларуси, Болгарии, Чехии, Эстонии, Грузии, Германии, Венгрии, Казахстана, Кыргызстана, Латвии, Литвы, Молдовы, Польши, Румынии, России, Словакии, Швейцарии, Таджикистана, Туркменистана, Украины и Узбекистана.

Red Sift предлагает автоматизированные инструменты – от мониторинга сети до анализа электронной почты и аутентификации, предназначенные для защиты пользователей и репутации бренда. Red Sift Open Cloud – это платформа для анализа данных, специально созданная для защиты электронной почты.

Используя возможности искусственного интеллекта, Red Sift может безопасно сопоставлять, вычислять и визуализировать данные из тысячи отдельных сигналов, помогая организациям оптимизировать свою кибербезопасность.

SaaS решения OnDMARC и OnINBOX работают вместе, чтобы закрыть сеть от проблемы фишинга, блокируя исходящие фишинговые атаки и анализируя безопасность входящих сообщений для анализа угроз электронной почты в масштабах компании». ***(Softprom становится дистрибьютором решений для защиты электронной почты Red Sift // Компьютерное Обозрение (https://ko.com.ua/softprom_stanovitsya_distribyutorom_reshenij_dlya_zashhity_jelektronnoj_pochty_red_sift_137390). 18.05.2021).***

***

«CrowdStrike, лидер в области облачной защиты конечных точек и рабочих нагрузок, и Google Cloud объявили 10 мая о серии интеграций продуктов для обеспечения многоуровневой безопасности их общих клиентов. Такая интеграция улучшит обмен телеметрией и данными между двумя платформами безопасности — CrowdStrike Falcon и Google Chronicle — обеспечит высокий уровень видимости и защиты рабочих нагрузок во всей облачной или гибридной среде клиента.

Falcon — это флагманский продукт CrowdStrike, который предприятия используют для защиты серверов и устройств сотрудников. Благодаря большой инсталлированной базе, Falcon отслеживает около 5 триллионов точек данных безопасности в неделю.

Платформа облачной аналитики Google Chronicle позволяет экспертам по кибербезопасности обнаруживать признаки взлома в петабайтах исторических данных, даже спустя много месяцев после инцидента.

Добавление информации из Falcon должно позволить клиентам CrowdStrike выполнять более полный анализ комплексных угроз в Chronicle, а также быстро идентифицировать проблемы текущих операций в другом сервисе Google Cloud — Security Command Center.

Согласно обеим компаниям, они также будут работать вместе, чтобы упростить установку Falcon внутри виртуальных машин Google Cloud.

Программные сенсоры, которые собирают для Falcon данные безопасности виртуальных машин, можно будет устанавливать быстрее благодаря интеграции с инструментом Security Agent Deployment. Облачный гигант создал его специально для ускорения установки средств защиты от взлома.

В число других продуктов, на которые распространяется новое интеграционное партнёрство, входят также BeyondCorp Enterprise и Google Workspace. В комбинации с Falcon Zero Trust Assessment (ZTA) они позволят создавать и применять детализированные политики доступа к приложениям,

используя уникальные сигналы риска CrowdStrike и укрепляя инициативы «нулевого доверия».

VirusTotal — служба сканирования файлов на наличие вредоносных программ, управляемая Google, скоро станет доступна в качестве надстройки Falcon, чтобы администраторы могли проверять файлы из собственного интерфейса этой платформы». ***(Google и CrowdStrike улучшат защиту клиентов в гибридных облачных средах // Компьютерное Обозрение (https://ko.com.ua/google_i_crowdstrike_uluchshat_zashhitu_klientov_v_gibridnyh_oblachnyh_sredah_137305). 11.05.2021).***

***

«HP Inc. представила интегрированное решение HP Wolf Security, включающее портфолио защищенных ПК и принтеров, программно-аппаратный комплекс для защиты конечных устройств и сервисы для обеспечения безопасности.

В опубликованном отчёте HP Wolf Security Blurred Lines & Blindspots отмечается, что во время пандемии COVID-19 число кибератак во всём мире увеличилось на 238%, при этом самой распространенной мишенью для хакеров становятся сотрудники, работающие удаленно за пределами офиса.

Сообщается, что новая платформа HP Wolf Security, построенная на базе более чем 20-летних исследований и инноваций в области безопасности, предлагает клиентам унифицированный набор инструментов, ориентированных на комплексную защиту конечных устройств и повышение их устойчивости к атакам.

«В будущем всё шире будет распространяться модель распределенной организации рабочих процессов, — отметила директор по информационной безопасности (CISO) HP Inc. Джоанна Берки (Joanna Burkey). — Со временем всё больше сотрудников будут работать за пределами офисов и пользоваться удалённым доступом к корпоративным ресурсам, что приведёт к появлению новых уязвимостей».

Согласно глобальной статистике KuppingerCole, в 2020 году клиентские устройства, подключённые к Интернету, подвергались атакам с частотой полтора раза в минуту. В то же время 91% опрошенных ИТ-специалистов заявили, что сегодня они тратят на обеспечение безопасности конечных устройств больше времени, чем два года назад, кроме того, 91% сообщили, что защита конечных устройств стала задачей не менее важной, чем обеспечение безопасности сети.

Решение HP Wolf Security основано на принципах ZeroTrust и использует самые современные технологии для снижения нагрузки на ИТ-персонал. Комплексная защита обеспечивается за счёт самовосстанавливающихся микропрограмм, функции обнаружения утечек памяти и сдерживания угроз с помощью виртуализации и облачных интеллектуальных технологий. Решение сокращает зону, уязвимую для атак, и предоставляет возможность удалённого восстановления после атак на микропрограммное обеспечение, улучшает сбор данных об угрозах и обеспечивает точные и своевременные предупреждения об опасности.

Интегрированное портфолио решений HP Wolf Security подразделяется на следующие категории: HP Wolf Security for Home4 включает набор встроенных функций безопасности для потребительских устройств, а также программное обеспечение и сервисы HP Wolf Essential Security, которые продаются отдельно. HP Wolf Security for Business5 включает в себя набор аппаратных функций безопасности, которые входят в комплект поставки каждого корпоративного ПК и предназначены как для крупных, так и для малых предприятий. Программное обеспечение, устройства и сервисы6 HP Wolf Pro Security для малого и среднего бизнеса. Программное обеспечение, устройства и сервисы HP Wolf Enterprise Security для крупных предприятий и государственных органов.

Также HP Wolf Enterprise Security получила функцию Sure Access Enterprise, основанную на уникальной технологии изоляции HP, которая обеспечивает полную защиту критически важных приложений от любых вредоносных программ, скрывающихся на пользовательских ПК. HP Sure Access создаёт микро-виртуальные машины с использованием аппаратных средств (ВМ), которые способны защищать ключевые приложения, создавая виртуальный барьер между приложением и компьютером. Таким образом, приложения и данные надёжно изолированы от ОС и от любых злоумышленников. Этот уникальный аппаратный подход помогает: обеспечивать безопасность выполнения ключевых задач, таких как, например, удалённый доступ системного администратора к критически важным системам.

Предоставлять пользователям возможности безопасно работать на нескольких виртуальных рабочих станциях с привилегированным доступом (PAW) с одного устройства. Предоставлять доступ к критически важным приложениям через браузер.

Компания HP переопределяет защиту ПК для малого и среднего бизнеса, представляя платформу HP Wolf Pro Security. Платформа объединяет Threat Containment (Сдерживание угроз) на основе микровиртуализации, Malware Prevention (Проактивную защиту от вредоносных программ) на основе Антивируса нового поколения и Identity Protection (Защиту личных данных) с аппаратными возможностями защиты для построения, развёртывания и эксплуатации комплексной системы безопасности.

Особо подчеркивается, что Malware Prevention — полноценное антивирусное ПО нового поколения, использующее комбинацию методов на основе искусственного интеллекта, среди которых глубокое обучение и поведенческий анализ, которые обеспечивают расширенную защиту от вредоносных программ за счёт предиктивного обнаружения. Identity Protection отвечает за защиту учётных данных от фишинговых атак во всех популярных браузерах. Интеграция со встроенными аппаратными средствами безопасности HP, такими как: Application Persistence (Стабильность приложений), OS Resiliency (Отказоустойчивость ОС) и Physical Tamper Protection (Защита от физических изменений).

Также в рамках HP Wolf Security компания представила новое решение Flexworker. Технология повышает эффективность работы ИТ-отделов, помогая им обеспечивать безопасность корпоративных сетей и данных.

Это новое расширение сервиса управления печатью (MPS) позволяет ИТ-отделам предоставлять мобильным сотрудникам безопасные, утвержденные компанией сервисы и функции для печати, которые можно отслеживать и автоматически исправлять при нарушении корпоративных политик безопасности». ***(Представлено интегрированное решение HP Wolf Security — для информационной защиты ПК и принтеров // Компьютерное Обозрение (https://ko.com.ua/predstavleno_integrirovannoe_reshenie_dlya_informacionnoj_zashhity_hp_wolf_security_137386). 18.05.2021).***

***

«В рамках нового партнерства Microsoft и Darktrace стремятся повысить кибербезопасность клиентов, предоставляя самообучающийся искусственный интеллект (ИИ) масштаба предприятия, который обнаруживает киберугрозы и реагирует на них.

Согласно Darktrace, сотрудничество будет посвящено его самообучающемуся ИИ для использования в средах Microsoft, включая Microsoft 365 и облачные приложения, такие как Azure Sentinel. Вместе эти два предприятия помогут повысить безопасность в многоплатформенных и многооблачных средах и автоматизировать расследования угроз.

«По мере того, как кибератаки становятся все более изощренными, ИИ добавляет более глубокий уровень защиты при обнаружении этих угроз», - сказала Клэр Барклай, генеральный директор Microsoft UK. «Партнерство между Microsoft и Darktrace поможет обеспечить безопасность организаций, позволяя им сосредоточиться на своем основном бизнесе и клиентах».

В рамках партнерства две фирмы сотрудничают в ряде областей для поддержки клиентов. Microsoft Azure будет размещать Antigena Email, который использует технологию автономного ответа Darktrace для предотвращения сложных почтовых угроз. Darktrace теперь также интегрируется с Azure Sentinel для создания автоматических отчетов об исследовании угроз и Microsoft Defender для подключения возможностей обнаружения ИИ.

«Я горжусь тем, что сотрудничаю с Microsoft, внедряя Cyber AI и автономное реагирование Darktrace в совместные клиентские среды», - сказала Поппи Густафссон, генеральный директор Darktrace. «Везде, где работает Microsoft, Darktrace обеспечивает безопасность». ***(Elly Yates-Roberts. Microsoft and Darktrace partner to enhance cybersecurity // Tudor Rose (https://www.technologyrecord.com/Article/microsoft-and-darktrace-partner-to-enhance-cybersecurity-123858). 10.05.2021).***

***

«SpecTrust, стартап из Сан-Хосе, штат Калифорния, разрабатывающий платформу кибербезопасности без кода, сегодня вышел из скрытности с начальным финансированием в размере 4,3 миллиона долларов, возглавляемым Cyber Mentor Fund. Компания SpecTrust, основанная сотрудниками ThreatMetrix, eBay, Fastly и Akama, планирует направить

вырученные средства на исследования и разработки продуктов и глобальные усилия по найму.

Убытки от киберпреступности превысили 50 миллиардов долларов в 2019 году, и предприятия тратят более чем в три раза эту сумму на решения для цифровой защиты. Поскольку пандемия побуждает компании ускорять свои цифровые преобразования, кибербезопасность становится все более серьезной проблемой. Deloitte отмечает, что в период с февраля по май 2020 года более полумиллиона человек пострадали от нарушений, связанных с кражей данных видеоконференцсвязи. Между тем, растет число кибератак с использованием ранее невидимых вредоносных программ или методов, причем их доля возрастает с 20% до пандемии до 35% во время пандемии.

Платформа SpecTrust без кода позволяет группам безопасности развертывать, оптимизировать и применять многоуровневую защиту от киберпреступлений без инженерных решений. Потоковый процессор преобразует интернет-трафик в нормализованные данные и аналитические данные, а панель управления позволяет клиентам изолировать шаблоны злоупотреблений, автоматизировать моделирование решений и обеспечивать защиту.

«Сотни тысяч профессионалов в области защиты от рисков незаметно борются с многомиллиардной империей киберпреступников. Когда защитники рисков не настроены на успех с использованием единых данных и инструментов, страдают предприятия и потребители », - сказал в пресс-релизе соучредитель и генеральный директор Нейт Харрл. «Мы работали вместе с этими героями в течение многих лет и создали SpecTrust, чтобы дать им возможность, наконец, бороться с киберпреступностью и побеждать».

Рост кибербезопасности

Новые финтех-компании предлагают финансовые услуги миллионам потребителей, доходы от электронной торговли растут рекордными темпами, а предприятия переходят на облачные стратегии и стратегии гибридной цифровой трансформации. В результате 89% компаний полагаются на эффективную защиту от киберпреступлений, чтобы реализовать свои стратегии роста, сообщает Merchant Risk Council.

По данным Gartner, почти 70% предприятий планируют ускорить расходы на облачные сервисы в 2021 году. По мере того, как все больше данных перемещается в облако, атаки на облачные инфраструктуры значительно возрастают, что заставляет группы безопасности быстро реагировать.

«Уникальное сочетание таланта, технологий и времени выхода на рынок - вот что отличает SpecTrust от остальных стартапов, выходящих на арену борьбы с киберпреступностью», - заявил соучредитель Cyber Mentor Fund Джо Энди. «Подход SpecTrust к автоматическому сбору данных о поведении и идентичности на протяжении всего пути пользователя позволяет клиентам организовывать и оптимизировать защиту от рисков».

Помимо Cyber Mentor Fund, в последнем раунде финансирования SpecTrust приняли участие Rally Ventures, SignalFire, Dreamit Ventures и Legion Capital». ***(Kyle Wiggers. No-code cybersecurity platform SpecTrust emerges from stealth with $4.3M //***

VentureBeat (https://venturebeat.com/2021/05/19/no-code-cybersecurity-platform-spectrust-emerges-from-stealth-with-4-3m/). 19.05.2021).

***

«Google развертывает новые расширенные функции защитника безопасности для Google Workspace, чтобы помочь администраторам бороться с угрозами кибербезопасности.

Google использует VirusTotal материнской компании Alphabet, веб-сайт по исследованию вредоносных программ, который Google купил в 2012 году, для получения новой возможности в Центре оповещений Google Workspace.

Центр оповещений теперь будет отображать оповещения в реальном времени с информацией о событиях безопасности в домене администратора, которые поддерживаются VirusTotal.

Согласно Google, цель состоит в том, чтобы помочь снизить нагрузку на администраторов из-за шума уведомлений системы безопасности и обеспечить единое представление наиболее важных предупреждений.

В 2018 году VirusTotal перешел в подразделение Alphabet по корпоративной кибербезопасности Chronicle, которое теперь является частью Google Cloud. Chronicle предоставляет облачные сервисы информации о безопасности и управления событиями (SIEM), которые мало чем отличаются от Microsoft Sentinel SIEM.

Интеграция VirusTotal помогает администраторам глубже разбираться в событиях безопасности и охватывает поддерживаемые объекты VirusTotal, такие как домен, хэш прикрепленных файлов или IP-адрес.

Эта возможность последовала за выпуском VirusTotal VT Augment на прошлой неделе - способа отображения VirusTotal в сторонних продуктах безопасности, таких как недавняя интеграция CrowdStrike своего продукта Falcon с Google Cloud, включая Chronicle, VirusTotal Enterprise и Google Cloud Security Command Center.

Платные подписчики VirusTotal получат более подробные отчеты о поиске вредоносных программ, включая индикаторы компрометации, позволяющие увидеть связи между объектами в наборе данных VirusTotal, график угроз для визуализации взаимосвязей угроз и информацию о репутации, собранную краудсорсингом. Он также предоставляет информацию о том, как вредоносные программы распространяются по географическим регионам на основе отправки вредоносных программ в VirusTotal, а также варианты быстрого поиска.

«Никакая информация о клиентах не передается из Google в VirusTotal, кроме случаев, когда администратор нажимает, чтобы получить отчет VirusTotal для определенного объекта», - сообщает Google.

«Эти улучшения начнут внедряться в ближайшие недели для лицензий Google Workspace Business Plus, Enterprise Standard и Plus и Education Standard и Plus. Они помогут администраторам подробно изучить угрозы и потенциальные злоупотребления для лучшей защиты. свои организации».

Google также предлагает администраторам способ заблокировать учетные записи Google Диска, которыми злоупотребляют инсайдеры.

Администраторы смогут запретить другому пользователю делиться с вами любым контентом в будущем. Этот элемент управления может помочь, когда другой пользователь в домене рассылает спам или отправляет оскорбительный контент.

Администраторы также могут удалить все существующие файлы и папки, которыми совместно пользуется другой пользователь, и запретить другим лицам доступ к содержимому пользователя, даже если ранее информация была совместно использована между ними.

«Блокировка пользователей не только сохранит полезность совместного использования Диска, но и, что наиболее важно, сохранит безопасность пользователей Диска. Средства управления блокировкой пользователей Диска будут разворачиваться в ближайшие несколько месяцев», - сообщает Google.

Google также внедряет более детальные элементы управления, чтобы ограничить доступ к ресурсам Google Workspace, включая блокировку всего доступа к OAuth 2.0 API с помощью управления доступом к приложениям и нового контекстно-зависимого доступа для мобильных и настольных приложений Google. Это предназначено для решения ситуаций, когда мошенники или злоумышленники используют приложения, чтобы обманом заставить пользователей предоставить доступ к данным компании.

Контроль доступа к приложениям дает администраторам возможность выбирать, доверять, ограничивать или блокировать доступ к данным Google Workspace». ***(Liam Tung. Google beefs up Workspace security with these new features // ZDNet (https://www.zdnet.com/article/google-beefs-up-workspace-security-with-these-new-features/). 18.05.2021).***

***

«Comcast, один из крупнейших американских провайдеров широкополосного доступа, теперь развернул в своей сети RPKI для защиты от перехвата и утечки маршрутов BGP.

Перехват маршрутов BGP - это сетевая проблема, которая возникает, когда определенная сеть в Интернете ложно объявляет, что она поддерживает определенные маршруты или префиксы, которые на самом деле не поддерживает.

Это происходит либо из-за злонамеренной активности, либо из-за неправильной конфигурации (последнее лучше называть «утечкой BGP», а не захватом).

При отсутствии контроля перехват или утечка маршрута BGP может вызвать резкий всплеск неверно направленного интернет-трафика, что в конечном итоге приведет к глобальной перегрузке и отказу в обслуживании (DoS).

Comcast развертывает RPKI для защиты маршрутов BGP

На этой неделе, стремясь повысить безопасность и надежность своей сети, телекоммуникационный гигант Comcast развернул в своей сети Resource Public Key Infrastructure (RPKI).

RPKI - это структура, разработанная для защиты инфраструктуры маршрутизации Интернета, в первую очередь протокола пограничного шлюза (BGP).

В прошлом месяце BleepingComputer сообщил, что крупная утечка BGP нарушила работу тысяч сетей по всему миру.

Некоторые из префиксов Comcast также присутствовали в рекламируемых сетью Vodafone, пострадавшей от утечки.

Но с введением Comcast RPKI в свою сеть, похоже, что провайдер сделал шаг вперед:

«На практике это означает, что Comcast теперь криптографически подписывает информацию о маршруте и проверяет криптографические подписи информации о маршруте других сетей».

«Это помогает гарантировать, что пакеты дойдут до назначенных пунктов назначения в целости и сохранности и не могут быть перехвачены или переданы другим адресатам, что делает сеть - и Интернет-трафик в целом - более безопасным и устойчивым для всех пользователей», - говорит Джейсон Ливингуд, вице-президент по технологиям Политика и стандарты компании Comcast Cable.

«Учитывая размер и техническое разнообразие нашей сети, развертывание RPKI потребовало значительных усилий, однако мы смогли внедрить обновление без снижения производительности наших клиентов», - продолжил Ливингуд в своем блоге на этой неделе…

Что такое BGP, перехват BGP и утечки BGP?

BGP или Border Gateway Protocol - это то, что заставляет современный Интернет работать.

Это похоже на «почтовую систему» в Интернете, которая облегчает перенаправление трафика из одной (автономной) системы сетей в другую.

Интернет - это сеть сетей, и, например, пользователь, проживающий в одной стране, хотел получить доступ к веб-сайту, основанному в другой, должна быть система, которая знает, какие пути следует использовать при перенаправлении пользователя через несколько сетевых систем..

Это похоже на письмо, которое проходит через несколько почтовых отделений между его источником и местом назначения.

И это цель BGP: правильно направлять интернет-трафик по различным путям и системам между источником и местом назначения, чтобы Интернет функционировал.

Но BGP хрупок, и любые сбои или аномалии даже в нескольких промежуточных системах могут иметь длительное влияние на многие.

Чтобы Интернет работал, различные устройства (автономные системы) объявляют префиксы IP, которыми они управляют, и трафик, который они могут маршрутизировать. Тем не менее, это в значительной степени основанная на доверии система, предполагающая, что каждое устройство говорит правду.

Учитывая массивный взаимосвязанный характер Интернета, трудно добиться честности на каждом устройстве, присутствующем в сети.

Перехват маршрута BGP происходит, когда злоумышленник умудряется «ложно объявить» другим маршрутизаторам, что они владеют определенным набором IP-адресов, когда они этого не делают. Когда это происходит, возникает хаос.

Такая путаница в маршрутах создаст множество проблем в Интернете и приведет к задержкам, перегрузке трафика или полному отключению.

Но утечки маршрута BGP аналогичны перехвату маршрута BGP, за исключением того, что последнее более конкретно относится к случаям злонамеренной активности.

В то же время утечки на маршруте могут быть, скорее, случайными.

В любом случае утечки маршрута BGP или перехвата BGP автономная система (AS) объявляет, что она знает, «как» или «куда» направить трафик, предназначенный для определенных пунктов назначения (AS), о которых в действительности она не знает.

Это может привести к тому, что пользователь попадет по интернет-маршруту, который будет предлагать неоптимальную производительность или явным образом вызвать сбои и потенциально послужит прикрытием для действий по подслушиванию или анализу трафика в случае злонамеренного угона.

Например, в прошлом году, как сообщает BleepingComputer, глобальный сбой IBM был вызван ошибочной конфигурацией маршрутизации BGP.

До этого мы видели значительный случай BGP угона в 2008 году, когда YouTube ушел в автономном режиме для глобальной аудитории из - за некоторые его трафик перенаправляет через пакистанские сервера.

В течение следующих нескольких лет мы сообщали о подобных инцидентах.

Контрмеры, такие как RPKI, помогают путем добавления структур проверки с использованием криптографии с открытым ключом.

«RPKI позволяет операторам сети шифровать и подписывать рекламные объявления о маршрутизации в цифровом виде в протоколе пограничного шлюза (BGP), используя систему закрытых и открытых ключей».

«Информация может быть зашифрована и подписана закрытым ключом и может быть только расшифрована или ее подпись может быть проверена с использованием соответствующего открытого ключа».

«Цифровая подпись информации обеспечивает гарантию того, что рекламные объявления о маршрутизации, видимые в системе маршрутизации, могут быть проверены и являются подлинными», - говорится в руководстве APNIC по RPKI.

Это помогает сетям доверять целостности информации о маршрутах, которую они получают, и помогает предотвратить инцидент DoS, связанный с перехватом или утечкой маршрута BGP.

Проверьте, защищен ли ваш интернет-провайдер от взлома BGP

Около года назад Cloudflare запустила веб-сайт, на котором пользователи Интернета могли проверить, добавил ли их интернет-провайдер защиту от атак с перехватом BGP.

Cloudflare поделился некоторыми мыслями по этому поводу с BleepingComputer:

«Cloudflare запустила веб-сайт isBGPSafeYet.com более года назад, чтобы помочь потребителям определить, внедрил ли их интернет-провайдер (или находится в процессе внедрения) RPKI».

«Цель этого сайта - повысить осведомленность многих интернет-провайдеров, которые еще не внедрили RPKI и делают Интернет уязвимым для

утечек и перехватов маршрутов», - сказал BleepingComputer технический директор Cloudflare Джон Грэм-Камминг в интервью по электронной почте.

«Cloudflare уже некоторое время ведет переговоры с Comcast о внедрении RPKI для BGP».

«Они связались с нами недавно, чтобы сообщить нам об этих грядущих изменениях. Это важный шаг в обеспечении безопасности людей в сети, потому что по умолчанию BGP не встраивает никаких протоколов безопасности. Это может привести к практике, называемой перехватом BGP, состоящей из перенаправления трафика в другую автономную систему для кражи информации (например, с помощью фишинга или пассивного прослушивания)», - продолжил Грэм-Камминг.

С другой стороны, когда в следующий раз произойдет перехват BGP, подлинность объявленных маршрутов можно будет проверить с помощью RPKI, - объясняет Cloudflare.

«Сеть должна развернуть RPKI Origin Validation, чтобы отклонить недопустимые маршруты. Подписание их маршрутов Comcast означает, что они с меньшей вероятностью пострадают от взлома их IP-адреса».

«Внедрение Comcast проверки происхождения RPKI означает, что их клиенты с меньшей вероятностью пострадают от любого взлома в Интернете, такого как взлом myetherwallet в 2018 году», - заключил Грэм-Камминг в своем интервью». ***(Ax Sharma. Comcast now blocks BGP hijacking attacks and route leaks with RPKI // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/comcast-now-blocks-bgp-hijacking-attacks-and-route-leaks-with-rpki/). 20.05.2021).***

***

«Google запускает новую функцию Chrome для Android, чтобы помочь пользователям изменять пароли, скомпрометированные при утечке данных, одним нажатием.

Chrome уже помог вам проверить, не были ли скомпрометированы ваши учетные данные, а с развертыванием новой функции автоматической смены пароля он также позволит вам изменять их автоматически.

Теперь при проверке украденных паролей на поддерживаемых сайтах и в приложениях Google Assistant будет отображать кнопку «Изменить пароль», которая проинструктирует Chrome перейти на веб-сайт и самостоятельно пройти весь процесс смены пароля.

Вам также будет предоставлена возможность пройти весь процесс вручную на любом этапе процесса изменения учетных данных.

«Благодаря Duplex в Интернете, Assistant берет на себя утомительные части просмотра веб-страниц: прокрутку, щелчки и заполнение форм, и позволяет вам сосредоточиться на том, что для вас важно», - сказал Патрик Неппер, старший менеджер по продукту Google Chrome.

«И теперь мы расширяем эти возможности еще больше, позволяя вам быстро создавать надежные пароли для определенных сайтов и приложений, когда Chrome определяет, что ваши учетные данные просочились в сеть».

Duplex в Интернете был представлен еще в 2019 году, чтобы позволить Google Assistant облегчить пользователям выполнение различных веб-задач, включая заказ еды, регистрацию на рейсы, покупку билетов в кино, а теперь и автоматическую смену взломанных паролей.

Развертывание на устройства с включенной синхронизацией паролей

«Автоматическая смена паролей постепенно внедряется в Chrome на Android для пользователей, которые синхронизируют свои пароли», - добавил Неппер.

«Он начинается в США и в ближайшие месяцы станет доступен на большем количестве сайтов и в других странах».

Google также объявил сегодня, что менеджер паролей Chrome для Android также получит несколько улучшений, в том числе:

Новый инструмент, упрощающий импорт паролей из других менеджеров паролей.

Более глубокая интеграция с Chrome и Android для беспрепятственного ввода ваших паролей на сайтах и в приложениях, независимо от того, используете ли вы компьютер или мобильное устройство.

Уведомления о паролях, которые автоматически предупреждают вас о сохраненных паролях, которые были взломаны в результате взлома третьей стороной.

Самир Самат, вице-президент Google по управлению продуктами, сказал сегодня на ежегодной конференции разработчиков Google I / O в этом году, что ОС Android теперь работает на более чем 3 миллиардах устройств.

Эта статистика не включает устройства, использующие сторонние магазины, такие как Amazon Fire или китайские смартфоны и планшеты на базе Android». ***(Sergiu Gatlan. Chrome now automatically fixes breached passwords on Android // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/chrome-now-automatically-fixes-breached-passwords-on-android/). 18.05.2021).***

***

«Российские ученые разрабатывают устройство, способное считывать колебания в потоке данных и тем самым вычислять злоумышленников

Сложные системы, такие как сетевой трафик или живые организмы, не обладают детерминированными физическими законами для их точного описания и предсказания дальнейшего поведения. В этом случае важную роль играет корреляционный анализ, который описывает поведение системы в терминах наборов статистических параметров.

Описывают такие сложные системы бестрендовые последовательности, часто определяемые как долгосрочные временные ряды или «шум». Они представляют собой колебания, создаваемые совокупностью различных источников, и являются одними из наиболее сложных данных для анализа и извлечения надежной, стабильной информации.

Одной из метрик, используемых в экономике и естественных науках при анализе временных рядов, является показатель Хёрста. Он позволяет предположить, сохранится ли тренд, присутствующий в данных. Например, продолжат ли значения возрастать, или рост сменится убыванием. Это

предположение выполняется для многих природных процессов и объясняется инертностью природных систем. Скажем, изменение уровня воды в озере, которое согласуется с прогнозами, выведенным из анализа значения показателя Хёрста, определяется не только текущим количеством воды, но и интенсивностью испарения, выпадением осадков, таянием снега и т. д. Все перечисленное — растянутый во времени процесс.

Уловить кибератаку

Объем трафика, проходящего через сетевые устройства, чудовищен. Это касается и конечных аппаратов — домашних персональных компьютеров, но особенно — промежуточных, таких как маршрутизаторы, а также высоконагруженных серверов. Часть этого трафика, например, видеоконференцсвязь, необходимо отправить с максимальным приоритетом, тогда как отправка файлов может и подождать. А может быть, это торрент-трафик, который забивает узкий канал. Или вовсе — идет сетевая атака, и ее нужно блокировать.

Анализ трафика требует вычислительных ресурсов, места для хранения (буфера) и времени — задержки в передаче. Все это в дефиците, особенно если дело касается маломощных промежуточных устройств. В настоящее время используются либо относительно простые методы машинного обучения, которые страдают от недостатка точности, либо методы глубоких нейронных сетей, которые требуют достаточно мощных вычислительных станций с большим объемом памяти просто для разворачивания инфраструктуры для запуска, не говоря уже о самом анализе.

Идея, лежащая в основе работы группы ученых под руководством Равиля Нигматуллина, достаточно проста: обобщить показатель Хёрста, добавив в него большее количество коэффициентов, чтобы получить более полное описание изменяющихся данных. Это позволяет находить закономерности в данных, которые принято считать шумами и которые ранее было невозможно анализировать. Таким образом удается производить «на лету» выделение значимых признаков и применять элементарные методы машинного обучения для поиска сетевых атак. В совокупности получается точнее тяжелых нейронных сетей, и такой подход можно разворачивать на маломощных промежуточных устройствах.

«Шум» — это то, что принято отбрасывать, но выделение закономерностей в «шумах» может быть очень полезным. Так, учеными был проведен анализ тепловых шумов передатчика в системе связи. Данный математический аппарат позволил выделить из данных набор параметров, характеризующих конкретный передатчик. Это может стать решением одной из задач криптографии: Алиса посылает сообщения Бобу, Чак — злоумышленник, который пытается выдать себя за Алису и отправить Бобу сообщение. Бобу нужно отличить сообщение от Алисы от сообщения от Чака.

Работа с данными глубоко проникает во все сферы человеческой жизни, алгоритмы распознавания изображений и речи давно перешли из разряда научной фантастики во что-то, с чем мы сталкиваемся ежедневно. Данный метод описания позволяет получать признаки сигнала, которые могут использоваться в машинном

обучении, существенно упрощая и ускоряя системы распознавания и улучшая точность решений. Результаты работы опубликованы в журнале Mathematics.

Александр Ивченко, сотрудник лаборатории мультимедийных систем и технологий МФТИ, один из авторов разработки, говорит: «Развитие данного математического аппарата может решить вопрос параметризации и анализа процессов, для которых нет точного математического описания. Это открывает огромные перспективы в описании, анализе и прогнозировании сложных систем». ***(Василий Макаров. Как вычислить кибератаки по «шуму» в потоке данных // ООО «Фэшн Пресс» (https://www.popmech.ru/technologies/699963-kak-vychislit-kiberataki-po-shumu-v-potoke-dannyh/). 20.05.2021).***

***

«Rockwell Automation и Cisco продолжают укреплять долгосрочный стратегический альянс — теперь в пакет услуг LifecycleIQ по выявлению киберугроз от Rockwell Automation входит решение Cyber Vision от Cisco.

Как отмечается, Rockwell Automation и Cisco сотрудничают уже больше десяти лет, одними из первых сделав упор на более тесную интеграцию информационных технологий и производственных технологий. Без этой конвергенции невозможно представить путь промышленных предприятий к цифровой трансформации, но в то же время это сопряжено с большим количеством вызовов: разрозненными сетями, угрозами кибербезопасности, недостатком опыта и знаний у сотрудников, огромным количеством производственных данных и дублирующими друг друга решениями. Будучи признанными лидерами в своих отраслях, Rockwell Automation и Cisco разработали архитектуры, продукты и решения, призванные помочь заказчикам преодолевать эти трудности на пути к «Единому предприятию».

Более глубокая интеграция между IT, облачной средой и промышленными сетями связана с киберугрозами, которые могут стать препятствиями на пути к полноценной цифровизации. Решение Cyber Vision обеспечивает полную прозрачность систем управления для создания безопасных инфраструктур и усиления политик безопасности, тем самым позволяя сделать технологические процессы беспрерывными, более устойчивыми и безопасными. Включение решения Cyber Vision в пакет услуг по выявлению угроз LifecycleIQ позволит заказчикам, работающим с решениями Cisco, создающим новые сети или обновляющим свою сетевую инфраструктуру Cisco, строить уникальную архитектуру сети на базе коммутаторов.

«Мы рады расширению стратегического партнерства с Cisco, — заявила Анжела Рапко (Angela Rapko), директор по ассортименту и управлению бизнесом отдела сервиса и услуг (CSM) Rockwell Automation. — Сотрудничество позволяет объединять лучшие наработки мирового лидера в IT-инфраструктуре и безопасности Cisco и ведущего поставщика промышленной автоматизации и OT Rockwell Automation. Включение Cisco Cyber Vision в наш пакет услуг по выявлению угроз кибербезопасности принесет нашим заказчикам максимальные преимущества за счет более тесной интеграции экосистем Rockwell Automation и Cisco, в особенности в вопросах кибербезопасности».

«Включение решения Cyber Vision от Cisco в пакет услуг по выявлению киберугроз от Rockwell Automation подчеркивает наше совместное стремление помочь заказчикам повысить уровень кибербезопасности своей производственной деятельности», — отмечает Викас Бутани (Vikas Butaney), вице-президент и генеральный директор Cisco IoT. — С помощью Cyber Vision мы можем внедрить кибербезопасность в промышленные сети, облегчая защиту самых критически важных операций наших заказчиков. Мы гордимся тем, что можем предложить самый полный пакет решений и услуг для объединения усилий IT и OT-команд по борьбе с рисками кибербезопасности».

Новое предложение станет дополнением к тем мерам, которые Rockwell Automation и Cisco уже принимают для решения проблем заказчиков в области промышленных сетей и их безопасности. К таким решениям относятся совместно разработанные и находящиеся в свободном доступе Архитектуры единой сети Ethernet предприятия (CPwE), применяя которые заказчики могут разрабатывать и внедрять безопасные и масштабируемые промышленные сети, а также управляемые коммутаторы Allen-Bradley Stratix, надежные и безопасные сетевые коммутаторы для экстремальных условий эксплуатации». ***(Rockwell Automation включила в пакет услуг по выявлению угроз решение Cisco Cyber Vision // Компьютерное Обозрение (https://ko.com.ua/rockwell_automation_vklyuchila_v_paket_uslug_po_vyyavleniyu_ugrozreshenie_cisco_cyber_vision_137494). 27.05.2021).***

***

«DataDome, компания, предоставляющая SaaS-решение для защиты бизнеса от вредоносных ботов и мошенничества, на этой неделе объявила о привлечении 35 миллионов долларов в рамках раунда финансирования серии B.

Инвестиционный раунд, в результате которого общая сумма финансирования компании составляет почти 40 миллионов долларов, возглавила венчурная компания Elephant при участии ISAI. DataDome планирует инвестировать деньги в продажи, маркетинг и исследования и разработки.

DataDome разработала платформу на базе искусственного интеллекта, которая обрабатывает огромные объемы данных, чтобы обеспечить защиту от различных типов онлайн-угроз, включая мошенничество с платежами, DDoS-атаки, попытки захвата аккаунтов и веб-скрапинг.

Компания заявляет, что ее решение может обеспечить защиту от ботов в реальном времени для веб-сайтов, мобильных приложений и API. У DataDome есть офисы в Нью-Йорке, Сингапуре и Париже, и она утверждает, что у нее более 130 клиентов по всему миру». ***(Eduard Kovacs. DataDome Raises $35 Million for Its Anti-Bot Solution // Wired Business Media (https://www.securityweek.com/datadome-raises-35-million-its-anti-bot-solution). 27.05.2021).***

***