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

№ 10 (жовтень)

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.– №10 (жовтень) . – 298 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 4
Національна система кібербезпеки 9
Правове забезпечення кібербезпеки в Україні 13
Кібервійна проти України 13
Боротьба з кіберзлочинністю в Україні 20
Міжнародне співробітництво у галузі кібербезпеки 26
Світові тенденції в галузі кібербезпеки 28
Сполучені Штати Америки 88
Країни ЄС та Великобританія 116
Китай 122
Російська Федерація та країни ЄАЕС 122
Австралія 125
Інші країни 129
Кібервійни та протидія зовнішній кібернетичній агресії 131
Створення та функціонування кібервійськ 138
Захист персональних даних 139
Кіберзлочинність та кібертерроризм 156
Діяльність хакерів та хакерські угруповування 196
Вірусне та інше шкідливе програмне забезпечення 203
Операції правоохоронних органів та судові справи проти кіберзлочинців 280
Технічні аспекти кібербезпеки 282
Виявлені вразливості технічних засобів та програмного забезпечення 285
Технічні та програмні рішення для протидії кібернетичним загрозам 291

«Торгово-промышленная палата Украины (ТППУ) совместно с Государственной службой специальной связи и защиты информации Украины объявили Месяц кибербезопасности.

Об этом Укринформу сообщили в Торгово-промышленной палате Украины.

Отмечается, что Месяц кибербезопасности направлен на борьбу с «киберэпидемией», выработку новой парадигмы поведения в киберпространстве, обеспечение устойчивой работы государственных учреждений, бизнеса, сервисов и систем.

Вице-президент Киевской торгово-промышленной палаты, председатель Антикризисного центра киберзащиты бизнеса ТППУ Владимир Коляденко рассказал, что Месяц кибербезопасности в формате государственно-частного взаимодействия проводится Палатой уже в четвертый раз.

«Все наши усилия, деятельность огромной громады, сотен компаний, академического сообщества, государственных органов, принимавших в этом участие, привели к тому, что нашу инициативу по проведению месяца кибербезопасности на общенациональном уровне поддержали», - подчеркнул Коляденко.

В этом году программа мероприятия предусматривает проведение круглых столов, региональных курсов и семинаров по вопросам кибербезопасности бизнеса. Также состоится общенациональный конкурс по кибербезопасности для студентов учащейся молодежи «Кибер Ниндзя», турнир по кибербезопасности для учеников г. Киева «Кибергерой», презентация и вебинар по киберпсихологии и много других мероприятий.

Месяц кибербезопасности стартовал со Дня кибербезопасности, в котором приняли участие студенты из более чем 50 университетов Украины. Цель такого мероприятия - рассказать молодежи о возможностях профессионального роста в этой сфере, ведь, согласно новой Стратегии кибербезопасности Украины, важное значение уделяется развитию образования.

По словам заместителя главы Госспецсвязи Александра Потия, успех в сфере кибербезопасности, как и в любой другой отрасли, зависит от трех составляющих: образования, прагматичности и честности. В частности, студенты могут получить компетенции на уровне управления государства, предприятий; риск-менеджмента, реагирования на инциденты и киберугрозы, разработки технических решений киберзащиты, защиты компьютерных систем и тому подобное. Для этого Госспецсвязи включает в Государственный классификатор Министерства экономики Украины 46 профессий в сфере кибербезопасности.

«Добавление профессий дает возможность выбрать свою карьеру специалиста по кибербезопасности: криминалиста-расследователя или аналитика уязвимостей либо рисков, системного инженера или программного архитектора. В общей сложности 46 профессий, которые составят современный кадровый потенциал Украины», - рассказал Потий.

В Украине специалистов по кибербезопасности готовят 52 кафедры в высших учебных заведениях, которые ежегодно выпускают около двух тысяч студентов…».

(Торгово-промышленная палата и Госспецсвязь объявили месяц кибербезопасности // Укринформ (https://www.ukrinform.ru/rubric-economy/3328106-torgovopromyslennaa-palata-i-gosspecsvaz-obavili-mesac-kiberbezopasnosti.html). 06.10.2021).

***

«Український сервіс Prozorro запросив спеціалістів з кібербезпеки та хакерів обговорити як покращити програму Prozorro Bug Bounty. Півтора року тому в Prozorro запустили програму пошуку вразливостей, відтоді сім багхантерів знайшли 68 вразливостей, 43 з них виявилися не критичного рівня.

За півтора року існування програми відбулося багато змін – від формату програми до розміру нагород. Спочатку програма була у дводенному форматі, тепер перейшла на постійну основу. На початку програми хантери отримували символічні подарунки – наразі ж винагороди збільшено до $1000 за вразливість.

Тож Prozorro вирішила запросити фахівців з кібербезпеки та хакерів до обговорення майбутнього програми. Зокрема, на заході обговорять, чому саме важливо тестувати державні цифрові системи на міцність. Розкажуть, як все працює зсередини (погляд проєктного менеджера) та зовні (погляд учасника)…» ***(Сергей Кулеш. Prozorro запросив «білих хакерів» обговорити програму bug bounty // ООО «ХОТЛАЙН» (https://itc.ua/news/prozorro-zaprosiv-bilih-hakeriv-obgovoriti-programu-bug-bounty/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 26.10.2021).***

***

«У жовтні 2021 року оператор мобільного зв’язку «Київстар» провів серед своїх абонентів опитування щодо ставлення до власної кібербезпеки. Результати демонструють, що 85% респондентів стикалися з викликами у цій сфері.

Ключові результати опитування:

7% користувачів мобільного зв’язку й інтернет-послуг вважають недоцільним вдаватися до додаткових заходів, аби упередити кібершайхрайство;

51% клієнтів у разі виявлення злочину змінять паролі до найважливіших облікових записів або одразу заблокують банківські картки, а 33% звертатимуться до правоохоронних органів або безпосередньо до фінансових установ та оператора мобільного зв’язку;

66% опитуваних абонентів захищають свій фінансовий номер;

32% респондентів планують захищати свій мобільний номер за допомогою реєстрації його на паспорт, а 12% опитаних уже авторизувалися.

З найпоширеніших видів шахрайства більшість опитаних виділила:

повідомлення про перемогу в неіснуючій акції;

дзвінок чи SMS із обіцянкою виграшу після сплати комісії;

дзвінок начебто з банку чи від оператора з проханням назвати одноразовий пароль із SMS, що надійде;

повідомлення про отримання невеликого грошового переказу із подальшою спробою вилучення даних кредитної картки.

«Такий результат дослідження доводить, що атаки на платоспроможних користувачів у сучасному світі стали агресивнішими, а технології для цього — досконалішими. Київстар постійно інвестує свої ресурси у запровадження культури кібергігієни, слідує світовим трендам і практикам у сфері цифрової безпеки, регулярно проводить інформування користувачів і бізнес-клієнтів щодо кібербезпеки та пропонує відповідні рішення. Сьогодні кожен має знати, як себе захистити, дотримуючись базових правил і принципів цифрової гігієни та кібербезпеки», — прокоментував Юрій Прокопенко, директор з кібербезпеки та DPO Київстар.

Компанія рекомендує абонентам в цілях безпеки персоніфікувати свій номер і прив'язати SIM-картку до паспорта або укласти контракт із телеком-оператором. В цьому разі заміна картки після викрадення потребує верифікації особи…»***(Сергей Кулеш. Київстар провів опитування абонентів щодо кібербезпеки — 85% респондентів стикалися з викликами у цій сфері (найпоширеніші види шахрайства) // ООО «ХОТЛАЙН» (https://itc.ua/news/ki%d1%97vstar-proviv-opituvannya-abonentiv-shhodo-kiberbezpeki-85-respondentiv-stikalisya-z-viklikami-u-czij-sferi/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 25.10.2021).***

***

«Оператор мобільного зв'язку «Київстар» пропонує бізнес-клієнтам комплекс сервісів для кіберзахисту до якого увійшли інструменти, розроблені постачальниками рішень у сфері інформаційного захисту Fortinet та Barracuda. Вони допоможуть компаніям захищати від загроз різних типів мережеві інфраструктури, сервіси та хмарні рішення.

Кіберзахист від Київстар можуть використовувати будь-які компанії, незалежно від індустрії, форми власності чи розміру: державні установи, банки, фінансові організації, IT-бізнеси, промисловість, компаній, що працюють з персональними даними, сервісні підприємства, ритейл, стартапи тощо.

В залежності від потреб та пріоритетів компаній, кожне з рішень може надаватися окремо або в комплексі з іншими інструментами для кібербезпеки. Це допоможе не лише захистити інфраструктуру, а й оптимізувати її.

Фунціонал інструментів для кіберзахисту дозволяє організувати:

Захист корпоративної пошти (Email Security) від шкідливого програмного забезпечення, фішингових атак, спаму та інших кіберзагроз. Запобігає втраті даних, шифрує й архівує електронну пошту.

Захист від різнорівневих атак, фільтрацію корпоративного трафіку (Next Generation Firewall). Виявляються та блокуються нові складні загрози, при цьому не зменшується продуктивність та пропускна здатність мережі.

Захист вебдодатків (Web Application Firewall (WAF)) від шкідливого трафіку з інтернету. Аналізується http-трафік між вебдодатком та мережею інтернет, відфільтровуються виявлені загрози.

Захист корпоративної мережі (Network Access Control (NAC)) від неавторизованих користувачів і зловмисників. Надається мережевий доступ відповідно до профілю користувача та з'ясовується, чи безпечно під'єднувати до мережі той чи інший пристрій.

Роботу систем захисту даних для аналізу поведінки користувачів (User and Entity Behavioral Analytics (UBA / UEBA)). Виявляється будь-яка аномальна поведінка в мережі та порушення правил, встановлених компанією.

Захист кінцевих точок (Endpoint Security) IT-інфраструктури компанії (серверів, ПК, ноутбуків, смартфонів) від відомих і невідомих атак. Виявляються, аналізуються та блокуються різноманітні загрози — злом пристрою, зараження вірусом, спам інших пристроїв тощо.

В Київстар зазначили, що запропоновані рішення працюють у будь-якому середовищі – у хмарі, на віртуальній машині чи на наявному обладнанні компанії. Вони сумісні з іншими сервісами для інформаційного захисту та можуть поєднуватися з ними. А використання сучасних технологій на основі машинного навчання (machine learning) дозволяє точно визначати вразливі місця системи та блокувати не лише відомі, а й нові загрози…»***(Сергей Кулеш. Київстар пропонує бізнес-клієнтам комплекс сервісів для кіберзахисту від Fortinet та Barracuda // ООО «ХОТЛАЙН» (https://itc.ua/news/ki%d1%97vstar-proponu%d1%94-biznes-kli%d1%94ntam-kompleks-servisiv-dlya-kiberzahistu-vid-fortinet-ta-barracuda/). 22.10.2021).***

***

«Підрозділи забезпечення кібербезпеки «Нової пошти» провели розслідування випадків шахрайства з використанням фейкового сайту, на якому пропонувалося взяти участь у розіграші призів.

Як повідомляє «Нова пошта», її кібербезпекою був виявлений шахрайський веб-сайт, на якому пропонувалося взяти участь у розіграші призів нібито від компанії. Користувач повинен був розповсюдити посилання на цей сайт та/або завантажити мобільний додаток з Google Play. Цей додаток є платним. Коли користувач його встановлює, оформлюється підписка та тестовий період, по закінченню якого з рахунку списується сума близько 1900 грн.

Фахівці Нової пошти встановили, що користувачі потрапляли на шахрайський веб-сайт через масове розповсюдження повідомлень із посиланнями, створеними з використанням доменів.ml,.cf,.tk, а для їхнього функціонування використовувався сервіс CloudFlare.

Крім того, спеціалісти виявили більше 100 шахрайських доменних імен, які використовувалися для аналогічних атак стосовно інших відомих українських брендів. Тому потрібно з осторогою ставитися до подібних розіграшів призів». ***(«Нова пошта» попередила про шахрайство із «розіграшем призів» // UA.NEWS (https://ua.news/ua/nova-poshta-predupredyla-o-moshennychestve-s-rozygryshem-pryzov/). 22.10.2021).***

***

«Французька компанія Thales, що спеціалізується на розробці високотехнологічної продукції для оборони і безпеки, аерокосмічної промисловості і транспортування має намір відкрити офіс в Україні.

Про це повідомили в Telegram-каналі Міністерства цифрової трансформації.

У Thales вже є офіси та науково-дослідні центри в 56 країнах світу.

Під час зустрічі з представниками компанії Thales в Парижі, українська сторона обговорила створення цифрових документів і кібербезпеки на основі штучного інтелекту.

Представники компанії розповіли, як в Україні можна поліпшити сферу кіберзахисту і якісно виявляти та протидіяти кіберзагрозам.

Відзначається, що в компанії вже призначили директора українського офісу…» ***(Марина Конопльова. Французька компанія з кіберзахисту Thales відкриває офіс в Україні // #ШоТам (https://shotam.info/frantsuzka-kompaniia-z-kiberzakhystu-thales-vidkryvaie-ofis-v-ukraini/). 23.10.2021).***

***

«…Компанія Київстар пропонує своїм бізнес-клієнтам комплексний кіберзахист, сервіси для якого розробили провідні постачальники рішень у цій сфері – Fortinet і Barracuda. Із цими інструментами клієнти Київстар ефективно захищають свої хмарні дані та мережеву інфраструктуру загалом.

Київстар допомагає своїм клієнтам організовувати:

Захист корпоративної пошти (Email Security) від шкідливого програмного забезпечення, фішингових атак, спаму та інших кіберзагроз. Запобігається втрата даних, шифрується й архівується електронна пошта.

Захист від різнорівневих атак, фільтрацію корпоративного трафіку (Next Generation Firewall). Виявляються й блокуються нові складні загрози, при цьому продуктивність мережі не зменшується.

Захист вебдодатків (Web Application Firewall – WAF) від шкідливого зовнішнього трафіка. Аналізується HTTP-трафік між вебдодатком та інтернет-мережею, відфільтровуются виявлені загрози.

Захист корпоративної мережі (Network Access Control – NAC) від неавторизованих користувачів і зловмисників. Надається мережевий доступ відповідно до профілю користувача й з'ясовується, чи безпечно під'єднувати до мережі той чи інший пристрій.

Роботу систем захисту даних для аналізу поведінки користувачів (User and Entity Behavioral Analytics – UBA / UEBA). Виявляється будь-яка аномальна поведінка в мережі та порушення правил, установлених компанією.

Захист кінцевих точок (Endpoint Security) IT-інфраструктури (серверів, ПК, ноутбуків, смартфонів) від відомих і невідомих атак. Виявляються, аналізуються й блокуються різноманітні загрози: злом пристроїв, зараження вірусами, спам інших пристроїв тощо.

Зброя проти DDoS-атак

Київстар пропонує бізнес-клієнтам також сервіс AntiDDoS, який протидіє DDoS-нападам різних рівнів. Адже це дуже поширений тип кібератаки: лише в першій половині 2021 року у світі було зафіксовано 5,4 мільйона випадків.

Фахівці компанії Київстар разом із клієнтом визначають його потреби та пріоритети й на основі цього пропонують окреме рішення або цілий комплекс інструментів для кібербезпеки.

Для кого ці рішення

Щотижня в Україні фіксують близько 60 тисяч кібератак. Їхніми об'єктами стають як державні установи, так і бізнес – великий і малий, старожили ринку та стартапи. Тож кіберзахисту потребують будь-які структури, що працюють із цифровими даними, у тому числі персональними, незалежно від сфери діяльності, форми власності чи масштабу:

державні установи;

банки;

фінансові організації;

IT-агенції;

промислові підприємства;

сервісні підприємства;

торговельні компанії.

Звертаємо вашу увагу: рішення від Київстар сумісні з іншими сервісами для інформаційного захисту. Тож, якщо ваш бізнес використовує інший захисний сервіс, – із запровадженням нового не виникне проблем. Серед інших вагомих переваг:

Використання машинного навчання, що дає змогу визначати вразливі місця системи та блокувати не лише відомі, а й нові загрози.

Робота у будь-якому середовищі, що дозволяє запускати рішення там, де потрібно – у хмарі, на віртуальній машині чи на наявному обладнанні компанії.

Дібрати оптимальне рішення для кіберзахисту вашій компанії допоможуть експерти Київстар. Також телекомунікаційний оператор надаватиме підтримку в процесі роботи вже підключених сервісів. Отримати більше інформації й замовити консультацію можна на офіційному сайті Київстар». ***(Атаки кожні 39 секунд: як убезпечитися від кіберзлочинців // 24 Канал (https://business.24tv.ua/ataki-kozhni-39-sekund-yak-ubezpechitisya-vid-kiberzlochintsiv_n1778328). 25.10.2021).***

***

Національна система кібербезпеки

«Асимметричный отпор стране-агрессору могут дать кибервойска, которые следовало создать еще в начале гибридной агрессии.

Об этом сказала руководитель службы по вопросам информационной безопасности и кибербезопасности Аппарата СНБО Украины Наталья Ткачук во время круглого стола в Укринформена тему «Обсуждение вопросов киберобороны государства и перспективы создания кибервойск».

«Этот вопрос чрезвычайно актуален. Мы должны были создать такие силы и подразделения еще с началом гибридной агрессии. Ибо деятельность кибервойск может стать асимметричным ответом стране-агрессору», - отметила Ткачук.

В то же время она считает главной проблемой для создания кибервойск отсутствие кадров и высказалась за создание кадрового резерва из числа молодых и талантливых айтишников.

«Главная проблема национальной системы кибербезопасности - отсутствие кадров в каждом органе, который отвечает за эту сферу. Этот вопрос следует решить путем построения киберрезерва специалистов - молодых парней и девушек, которые будут проходить, в том числе, срочную службу. Это будет такой своеобразный пул кадров, который затем смогут использовать все субъекты сектора безопасности и обороны, задействованные в задачах кибербезопасности. Украина имеет для этого огромный потенциал, ни в одной стране нет такого количества молодых, талантливых айтишников, которые при этом являются настоящими патриотами своей страны и готовы защищать киберпространство», - считает Ткачук.

Другой проблемой для создания эффективных кибервойск она назвала отсутствие соответствующего правового поля, над чем сейчас работает СНБО.

«Для того, чтобы проводить специальные кибероперации, надо сформировать правовое поле, которое на сегодняшний день отсутствует. И одной из задач рабочей группы, созданной при аппарате СНБО, является наработка таких предложений, какие именно изменения в законодательство мы должны внести, чтобы такие кибервойска могли функционировать более эффективно», - сказала Ткачук.

Во время круглого стола, в частности, обсуждались вопросы необходимости внесения изменений и дополнений в законодательство Украины по направлению кибербезопасности, киберобороны, создания кибервойск.

Мероприятие организовали Министерство обороны Украины, Центр стратегических коммуникаций и информационной безопасности, ГО «Центр военной политики и политики безопасности», Укринформ». ***(В СНБО назвали главные проблемы национальной системы кибербезопасности // Укринформ (https://www.ukrinform.ru/rubric-polytics/3331655-v-snbo-nazvali-glavnye-problemy-nacionalnoj-sistemy-kiberbezopasnosti.html). 12.10.2021).***

***

«Украинские госучреждения будут повышать защищенность от киберугроз благодаря проекту ОБСЕ по продвижению кибергигиены среди госслужащих.

…соответствующий проект был презентован в четверг в Киеве.

«Новые наработки по популяризации кибергигиены среди работников госучреждений в Украине были представлены сегодня, 30 сентября 2021, на мероприятии в Киеве, организованном Координатором проектов ОБСЕ в Украине в сотрудничестве с Национальным агентством Украины по вопросам государственной службы и Украинской школой управления (УШУ). В частности, среди этих наработок - программа онлайн и очного обучения по основам кибергигиены, оборудованный мобильный тренинговый центр и пул тренеров, готовых к обучению госслужащих», - говорится в сообщении.

Краткосрочный курс «Основы кибергигиены» состоит из 9 онлайн-модулей, размещенных на платформе «Действие. Цифровое образование» и онлайн-ресурсе DESPRO, а также он дополняется 2-дневным глазным тренингом в УШУ, официальном провайдере образовательных услуг по повышению квалификации должностных лиц. Курс охватывает ряд тем по распространенным угрозам киберпространства (таких как взлом, фишинг) и освещает способы их избежания.

Для возможности проводить тренинги в различных локациях Координатор проектов ОБСЕ в Украине обеспечил УШУ 20 комплектами ноутбуков с соответствующим лицензионным программным обеспечением. Также были разработаны методическое пособие тренера и рабочая тетрадь госслужащего-участника тренинга с кибергигиены. Кроме этого был сформирован пул из 52 тренеров, прошедших методологическое и практическое обучение с последующим пилотированием тренинговой программы…». ***(Украинские госучреждения повысят кибербезопасность благодаря проекту ОБСЕ // Укринформ (https://www.ukrinform.ru/rubric-polytics/3325275-ukrainskie-gosucrezdenia-povysat-kiberbezopasnost-blagodara-proektu-obse.html). 01.10.2021).***

***

«Министерство обороны создало ситуационный центр кибербезопасности.

Об этом говорится в сообщении пресс-службы Минобороны…

«Министр обороны уже подписал соответствующие приказы о создании ситуационного центра МОУ. Одно из подразделений этой структуры будет заниматься проблематикой реагирования на киберугрозы военного характера непосредственно под общей координацией Национального координационного центра кибербезопасности во взаимодействии с другими субъектами обеспечения кибербезопасности государства. Не менее амбициозной задачей является создание кибервойск», - сказал заместитель генерального директора - руководителя экспертной группы планирования и внедрения политик директората политики цифровой трансформации и информационной безопасности в сфере обороны Министерства обороны полковник Сергей Глушко.

По его словам, киберпространство - это специфическая составляющая информационного пространства, и силы обороны должны овладеть этим доменом вооруженного противоборства на современном уровне.

Именно эта цель красной нитью проходит через положение стратегического оборонного бюллетеня и приложений к нему, где показаны механизмы достижения целей.

Глушко заявил, что Минобороны поставило амбициозную цель - овладение Вооруженными Силами Украины, и вообще силами обороны государства, информационным доменом вооруженного противоборства».(***Богдан Бронтерюк. Минобороны создало ситуационный центр кибербезопасности// Українські Новини (https://ukranews.com/news/807064-minoborony-sozdalo-situatsionnyj-tsentr-kiberbezopasnosti). 12.10.2021).***

***

«Національний координаційний центр кібербезпеки при Раді національної безпеки та оборони України ухвалив «Перелік категорій кіберінцидентів» і «Загальні правила обміну інформацією про кіберінциденти. Протокол TLP», розроблені Адміністрацією Держспецзв'язку.

Документи слугуватимуть основою для обміну інформацією про кіберінциденти між суб'єктами національної системи кібербезпеки.

«Єдиний підхід до класифікації кіберінцидентів та обмін інформацією про них дасть можливість підвищити стійкість держави до кіберзагроз», – зазначив Голова Держспецзв'язку Юрій Щиголь.

«Перелік категорій кіберінцидентів» упроваджує єдину термінологію для обміну інформацією про кіберінциденти, передання звітів до НКЦК, у тому числі за допомогою автоматизованих платформ для обміну інформацією про кіберзагрози.

«Загальні правила обміну інформацією про кіберінциденти. Протокол TLP» визначають спосіб класифікації повідомлень про кіберінциденти з урахуванням того, як і кому може надаватись така інформація.

Також протокол може застосовуватися для передання індикаторів компрометації урядовій команді реагування на комп'ютерні надзвичайні події України CERT-UA з метою інформування інших організацій про потенційні загрози». ***(Сергей Кулеш. Держспецзв'язку: Кіберінциденти в Україні класифікуватимуть за єдиним підходом // ООО «ХОТЛАЙН» (https://itc.ua/news/kiberinczidenti-klasifikuvatimut-za-%d1%94dinim-pidhodom/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 26.10.2021).***

***

«Совет нацбезопасности и обороны (СНБО) планирует создать в Украине отраслевой центр кибербезопасности топливно-энергетического комплекса.

Как сообщает пресс-служба ведомства, реализация этого проекта возложена на Министерство энергетики.

«Мы находимся в состоянии войны с Российской Федерацией, кибератаки на нашу критическую энергетическую инфраструктуру — один из ее методов», — заявил на заседании Национального координационного центра кибербезопасности (НКЦК) секретарь СНБО Алексей Данилов.

Он также добавил, что меры по обеспечению кибербезопасности отечественного топливно-энергетического комплекса актуальны в контексте плана присоединения Украины к европейской энергетической сети.

Во время заседания участники одобрили проект Плана реализации Стратегии кибербезопасности Украины, утвержденной указом президента от 26 августа 2021 года № 447, который будет направлен на рассмотрение СНБО.

Заместитель секретаря СНБО Украины Сергей Демедюк подчеркнул, что План реализации Стратегии, разработанный НКЦК, является основой для ежегодного планирования субъектами обеспечения кибербезопасности соответствующих мероприятий.

«План целесообразный и учитывает задачи и способности всех ключевых субъектов обеспечения кибербезопасности», — сказал он.

Участники заседания одобрили протокол обмена информацией о киберинцидентах (TLP-протокол) и их классификацию (таксономию), которые разработала Государственная служба специальной связи и защиты информации.

В СНБО также сообщили, что участники обсудили вопросы по созданию в Украине кибервойск и необходимости разработки в ближайшее время соответствующего законопроекта…». ***(В Украине хотят создать центр кибербезопасности топливно-энергетического комплекса // Delo.ua (https://delo.ua/econonomyandpoliticsinukraine/v-ukraine-hotjat-sozdat-centr-kiberbezopasnosti-387805/). 26.10.2021).***

***

Правове забезпечення кібербезпеки в Україні

«**План оборони України, що був затверджений на засіданні Ради національної безпеки й оборони (РНБО) учора, 15 жовтня**, є секретним і діятиме лише у воєнний час.

Документ розробляли протягом двох років за дорученням президента Володимира Зеленського. Про це заявив секретар РНБО Олексій Данілов в ефірі програми «Свобода слова».

Зокрема, у плані йдеться про «повну взаємодію всіх органів без винятку», а також є пункти про кібербезпеку та інформаційну безпеку.

Це стосується не тільки військових, але всіх органів центральної виконавчої влади, органів місцевої влади, це стосується того закону, який ми ухвалили влітку щодо територіальної оборони, який називається Закон про національний опір. Там усі ці компоненти зведені в єдину систему координат,— розкрив деталі Данілов.

Він наголосив, що з цього приводу будуть обов’язкові великі військові навчання за дорученням президента…» ***(План оборони України — Данілов розкрив деталі секретного документа // Ракурс (https://racurs.ua/ua/n161687-plan-oborony-ukrayiny-danilov-rozkryv-detali-sekretnogo-dokumenta.html). 16.10.2021).***

***

Кібервійна проти України

«В Украине хакеры взломали крупную сеть аптек – АНЦ, заблокировали работу сайта и «вырубили» интернет.

Злоумышленники требовали выкуп за то, чтобы работа аптек вернулась в прежнее русло, поделился в Facebook гендиректор холдинга аптечной сети АНЦ Николай Щербина.

По его словам, хакерам никто не собирался платить, и делается все возможное для того, чтобы злоумышленники были пойманы и привлечены к ответственности.

«...наша команда работает над восстановлением инфраструктуры, которое, скорее всего, займет несколько дней (чего стоит только покупка, доставка и настройка новых маршрутизаторов в более чем 1000 аптек)», – добавил управленец.

В пресс-службе киберполиции сообщили, что пока им ничего неизвестно об этой хакерской атаки.

Также в ведомстве отметили, что в любом случае заявитель должен обращаться в органы Национальной полиции, где дело будут расследовать следователи, которые обращаются в киберполицию, если необходима помощь именно специалистов, которые противодействуют подобным преступлениям…». ***(Елена Милосердова, Екатерина Присяжнюк. В Украине крупную сеть аптек взломали хакеры // UNIAN.NET (https://www.unian.net/science/v-ukraine-krupnuyu-set-aptek-vzlomali-hakery-novosti-11574715.html). 12.10.2021).***

***

«В Украине фиксируются 60 тысяч кибератак в неделю. Первое место занимают атаки на государственный сектор.

Об этом сообщил вице-президент Киевской торгово-промышленной палаты, председатель Антикризисного центра киберзащиты бизнеса Торгово-промышленной палаты Украины Владимир Коляденко в программе «5 вопросов» телеканала «Дом»…

По его словам, Украина - одна из первых сегодня по индикаторам цифровизации, потому что введено в действие приложение «Дія», есть больше 15 сервисов, которые доступны на платформе. То есть это расширяет возможности. Но это, конечно, расширяет и угрозы, сказал эксперт.

«В связи с геополитической ситуацией, в связи с вопросами международной безопасности, фактически войной, которая ведется у нас на востоке Украины. Все это является сегодня очень сильным полигоном, на котором отрабатываются различные технологии. Можете посмотреть по количеству кибератак... В Украине есть уникальные специалисты, уникальный опыт, которым мы можем поделиться со всем миром. Конечно, в условиях международной кооперации и сотрудничества с нашими международными партнерами, в первую очередь в секторе безопасности, в оборонном секторе, потому что атаки на этот сектор, государственный, занимают первое место», - проинформировал Коляденко.

Что касается бизнеса, то, безусловно, это атаки на финансовый сектор, банковский сектор, здесь бизнес тоже выстраивает свои системы. И все это требует координации, обмена информацией, подчеркнул эксперт.

«Очень важным в этом сотрудничестве является доверие прежде всего между органами власти, которые отвечают за это, и четкая координация их деятельности, и доверие между властью и бизнесом. Это должен быть диалог, имеющий равную долю ответственности, не имеющий дискриминации и направленный на то, чтобы бизнес понимал, что он тоже отвечает за это, отвечает перед государством. А

государство - это не только репрессивная машина. Государство - это также и инструмент, который может в сотрудничестве с бизнесом решать очень много вопросов», - подытожил эксперт». ***(Украина еженедельно подвергается 60 тысячам кибератак – эксперт// Укринформ (https://www.ukrinform.ru/rubric-technology/3327866-ukraina-ezenedelno-podvergaetsa-60-tysacam-kiberatak-ekspert.html). 05.10.2021).***

***

«Специалисты Ситуационного центра обеспечения кибербезопасности СБУ в сентябре прекратили и нейтрализовали 53 кибератаки на информационные системы органов власти.

Об этом сообщаетпресс-центр СБУ…

Как отметили в спецслужбе, «это произошло через непосредственный анализ более 33 000 критических событий информационной безопасности, выявленных в текущем месяце».

В СБУ добавили, что основными типами обнаруженных киберугроз (хакерских атак) были: соединение с командно-контрольными серверами (C&C Server) попытки получения несанкционированного доступа (Brute Force Attack); атаки на веб-приложения (Web App Attack); вредоносное программное обеспечение (Malware)…». ***(СБУ за месяц нейтрализовала более 50 хакерских атак на органы власти // Укринформ (https://www.ukrinform.ru/rubric-technology/3326711-sbu-za-mesac-nejtralizovala-bolee-50-hakerskih-atak-na-organy-vlasti.html). 04.10.2021).***

***

«В Украине с 29 сентября по 5 октября 2021 года зафиксировали и заблокировали 5 DDoS-атак на государственные информационные ресурсы. Об этом сообщает Госспецсвязь. Система защищенного доступа государственных органов к интернету заблокировала: 56 078 атак различных видов, что на 11% меньше чем на предыдущей неделе. В основном — это сетевые атаки прикладного уровня (97%); 5 DDoS-атаки — хакерское "нападение" на компьютерную систему с целью сделать ее ресурсы недоступными для пользователей. Система обнаружения уязвимостей и реагирования на киберинциденты и кибератаки на объектах мониторинга зафиксировала 336 403 подозрительных действий (на 30% меньше чем на предыдущей неделе): попытки получения прав пользователя - 9% попытки получения прав администратора - 14% нарушение корпоративной политики безопасности - 51% выявление сетевого ШПЗ - 17% другие - 9% "Правительственной командой реагирования на компьютерные чрезвычайные события Украины CERT-UA в этот период зарегистрировано и обработано 3615 киберинцидентив, что на 18% меньше чем на предыдущей неделе. Подавляющее большинство обработанных инцидентов принадлежит доменной зоне UACOM (примерно 99%). Основное количество инцидентов касается распространения вредоносного программного обеспечения — 99%", — говорится в сообщении».***(За неделю на государственные инфоресурсы осуществили пять хакерских атак //информационный портал "ua.today"***

(https://ua.today/news/politics/za_nedelyu_na_gosudarstvennye_inforesursy_osushestvili_pyat_hakerskih_atak). 08.10.2021).

***

«Попри те, що змагатися з Росією в кількості озброєння Україна поки що не може, є напрям, в якому ми здатні не тільки вирівняти баланс сил, але й нанести агресору «неприйнятних втрат» в разі загострення ситуації. Йдеться про війну у кіберпросторі. Як інформує видання «Коментар» про це у себе в Facebook повідомив нардеп Єгор Чернєв.

«Якби у Кремлі знали, що в разі зіткнення з Україною ми «покладемо» всю їх критичну інфраструктуру, обвалимо енергосистему, зупинимо логістичну галузь, транспорт і т.д., вони б не наважилися на широкомасштабну агресію. Саме тому я вважаю, що одним з головних завдань України на найближчі роки має стати створення потужного «кіберщита», в який входили б не тільки «кібервійська», а й інші неофіційні структури, здатні вести війну у кіберпросторі. Перемогти Росію ми поки можемо тільки там», — зазначив нардеп.

За його словами, наші ІТ-фахівці є одними з кращих у світі. Тисячі українців працюють сьогодні у Кремнієвій долині й на найвідоміші світові компанії, і вони залишаються патріотами. Це величезний ресурс для перетворення України в одну з найпотужніших країн у сфері кібервійни. Треба тільки правильно організувати процес.

«Вважаю, що всі ми повинні розуміти величезне значення війни у кіберпросторі й активно працювати над зміцненням цього напряму. Для захисту своєї свободи та незалежності ми маємо право використовувати всі доступні засоби й повинні робити це максимально ефективно, жорстко і, якщо треба, асиметрично», — резюмував Єгор Чернєв». ***(Кравцев Сергей. Нардеп розповів про сферу, в якій Україна «покладе Росію на лопатки» // Comments.ua (https://politics.comments.ua/ua/news/domestic-policy/nardep-rozpoviv-pro-sferu-v-yakiy-ukraina-poklade-rosiyu-na-lopatki-686071.html). 13.10.2021).***

***

«Шахраї почали масово торгувати підробленим додатком Дія у соцмережах. За допомогою ненадійної програми підлітки можуть купувати алкоголь сигарети в супермаркетах, а також показувати підроблені QR-коди з Covid-сертифікатами.

Зловмисники продають додаток в соцмережах за 120 грн. Інтерфейс програми повністю ідентичний сервісу Дія в смартфоні, але в ньому можна редагувати дані — фотографії, ім’я, прізвище та вік. В одному з розділів також є несправжній QR-код Covid-сертифікату, який візуально нагадує оригінал. Правда, якщо його спробувати сканувати — дані зображатимуться некоректно.

За словами міжнародного консультанта з кібербезпеки Михайла Чайкіна, боротися з такими додатками все ж таки можна.

– Створити такий застосунок може кожен, але можна боротися з можливістю використання інформації з державних реєстрів у підробленому додатку, – заявив Михайло.

Також є варіант відрізнити фейковий додаток від справжнього.

– Розпізнати підроблений сервіс можна тільки за допомогою сканування QR-коду. Наприклад, для покупки алкоголю або сигарет людина відкриває додаток і вибирає документ, після чого генерується унікальний QR-код. Якщо його просканувати – касир дізнається про підробку документа. Але в магазинах пристроїв для зчитування кодів не вистачає, і багато продавців нехтують перевіркою, – додав експерт.

В офіційному каналі Telegram міністра цифрової трансформації Михайла Федорова вже прокоментували новину про поширення підроблених додатків, і закликають українців не користуватися послугами шахраїв.

– Для тих, хто купує подібні сервіси, будьте обережні, можна потрапити під статтю "підробка документів", – повідомляється в каналі Федорова.

За словами радника віцепрем'єр-міністра України – Міністра цифрової трансформації Олесі Діденко, боротьбою з фейковими застосунками вже займається кібреполіція.

– Цим займається кіберполіція, яка розглядає кожен випадок окремо. Експерти вже залучені до пошуків шахраїв, які через застосунки крадуть дані користувачів. Цей випадок – не виняток, – запевняє радник.

У Мінцифрі також розповіли, як відрізнити цифрові документи в офіційній Дії від фейкової.

– Щоб підтвердити свою особу, натисніть на цифровий документ у Дії. Згенерується QR-код, який представники бізнесу можуть зчитати сканером, представники поліції — планшетом або будь-яка людина іншою Дією.Кожен може самостійно перевірити дійсність цифрового документа – у застосунку є зчитувач, яким можна просканувати QR-код іншого користувача Дії. Якщо документ фейковий, сканер або застосунок його не зчитають — відобразиться повідомлення про помилку. Фейковий документ не зчитується Дією, а лише сторонніми QR-сканерами й відкривається в браузері, — додала Олеся…». ***(Микола Олефіренко. Шахраї продають підроблені додатки Дія: для чого вони потрібні і як з ними боротися // Факти ICTV (https://life.fakty.com.ua/ua/tekhnolohii/shahrayi-prodayut-pidrobleni-dodatky-diya-dlya-chogo-vony-potribni-i-yak-z-nymy-borotysya/). 25.10.2021).***

***

«Сайт Київського інституту соціології зазнав кібератаки - з нього зникли всі матеріали. Гендиректор організації звертатиметься до правоохоронних органів…

Після публікації рейтингів КМІС, про що раніше повідомляли Букви, сайт організації зазнав кібератаки. Наразі на ньому недоступні жодні новини, релізи або дослідження.

Опубліковане напередодні цього соцопитування показало, що рейтинг політичної партії «Слуга народу» суттєво впав та вона вже поступається першим місцем «Європейській солідарності».

Генеральний директор КМІС Володимир Паніотто на своїй сторінці у Facebook підтвердив атаку на сайт та оголосив, що організація звертатиметься до кіберполіції з заявою про злочин.

Паніотто також наголосив, що цю атаку КМІС не пов'язує з публікацією рейтингів.

«Маю сказати, що у нас немає підстав пов'язувати атаку чи не пов'язувати саме з цими рейтингами. З нашої точки зору, в них практично не було нічого нового, вони статистично значуще не відрізнялися від травневих рейтингів. З іншого боку, напад більш ймовірно може бути пов'язаний все ж з політичними даними, а не іншими нашими даними (споживання трансжирів, культурні проблеми людей з інвалідністю тощо)», - сказав Паніотто.

Також він додав, що організація регулярно отримує погрози.

«Після публікації кожних рейтингів ми отримуємо листи з мовою ненависті і погрозами. Під час виборів ми проводили дослідження практично для всіх політичних сил, що потрапили до парламенту, зараз теж паралельно проводимо дослідження для політичних супротивників. Тому незадоволених може бути багато і ми не можемо це пов'язати з конкретною політичною силою», - наголосив гендиректор КМІСу…». ***(Сайт КМІС зазнав кібератаки після публікації останніх політичних рейтингів // Эксперт-Центр (http://expert.org.ua/smi-i-tehnologii/2021/sayt-kmis-zaznav-kiberataki-pislya-publikaciyi-ostannih-politichnih-reytingiv). 22.10.2021).***

***

«Державна служба спеціального зв’язку та захисту інформації» повідомляє, що протягом останніх семи днів системою захищеного доступу державних органів до мережі Інтернет заблоковано 59922 атаки різних видів, що на 26% більше ніж попереднього тижня. Переважна більшість – мережеві атаки прикладного рівня (97%).

Зафіксовано та заблоковано чотири DDoS-атаки.

Системою виявлення вразливостей і реагування на кіберінциденти та кібератаки на об’єктах моніторингу зафіксовано 76345 підозрілі події (на36% менше ніж попереднього тижня):

спроб отримання прав користувача – 8%;

спроб отримання прав адміністратора – 26%;

порушень корпоративної політики безпеки–29%;

виявлення мережевого ШПЗ – 17%;

застосування нестандартних протоколів – 10%;

підозрілого виконувального коду – 6%;

інші–4%.

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA у цей період зареєстровано та опрацьовано 2651 кіберінцидентів, приблизно нарівні попереднього тижня.

Переважна більшість опрацьованих інцидентів належить доменній зоні UACOM (близько 99%). Основна кількість інцидентів стосується розповсюдження шкідливого програмного забезпечення – 96%». ***(Кількість кібератак на державні***

інформаційні ресурси під час свят збільшилася на чверть// Компьютерное Обозрение (https://ko.com.ua/kilkist_kiberatak_na_derzhavni_informacijni_resursi_pid_chas_svyat_zbilshilasya_na_chvert_139093). 20.10.2021).

***

«С 2014 года и до настоящего времени Украина выдержала больше кибератак на госучреждения и объекты критической инфраструктуры, чем страны Европы в течение прошлого десятилетия, и за это время смогла создать эффективную систему для противодействия таким угрозам.

Об этом сегодня в Брюсселе в ходе семинара по противодействию новейшим кибернетическим и гибридным угрозам, состоявшегося под эгидой международного аналитического центра Beyond the Horizon при содействии Посольства Украины в Королевстве Бельгия, заявил Временный поверенный в делах Украины в Королевстве Бельгия и в Великом Герцогстве Люксембург Егор Пивоваров…

«Уже семь лет подряд Украина противостоит российской военной агрессии. Так называемая гибридная война, которая была начата Москвой против нашей страны, имеет много измерений, и кибернетические атаки - среди главных разрушительных элементов. Беспрецедентное количество кибератак было совершено против наших энергетических станций, предприятий, государственных учреждений, Национального банка, министерств и других объектов. Можно сказать, что количество таких атак, которые были совершены против Украины, превышает количество всех подобных нападений в каждой из стран ЕС в течение прошлого десятилетия», - сказал украинский дипломат.

Он отметил, что во времена пандемии, когда многие люди находятся в вынужденной изоляции, противник использует социальные сети, чтобы подорвать доверие к государственным институтам, дискредитировать кампанию вакцинации, распространять фальшивки о вакцинах и их эффективности, манипулировать статистикой, сеять сомнения и неопределенность. Созданы целые армии фальшивых пользователей соцсетей и «экспертов», распространяющих откровенную ложь. Понятно, что не только Россия применяет такие методы, но именно эта страна делает это настолько дерзко.

«Речь идет о попытках преднамеренного разрушения важных социальных и инфраструктурных объектов. Это не сценарий фильма-катастрофы, это происходит прямо сейчас, в Европе, в 21 веке... Мы стали полигоном для использования новых методов кибернетического оружия, но Украина не единственная страна, против которой они направлены. Их ощутили и в Европе, и в Америке. Эти методы позже будут использоваться с тем, чтобы поразить уже вашу жизнь, так, как они сейчас стараются делать это с нами», - сказал Пивоваров.

Он подчеркнул, что Служба безопасности Украины провела экспертное исследование относительно кибернетических атак, объективность которого подтверждена участием международных специалистов от ЕС и НАТО. Собранные доказательства однозначно указывают на общие черты таких нападений и на их единый источник происхождения.

«Собранные доказательства и примеры четко указывают, что это была не частная инициатива, а управляемая государством специальная кибернетическая операция, направленная на то, чтобы ослабить наши оборонительные способности и сделать уязвимой нашу национальную безопасность. Мы приняли этот вызов, как государство, и мобилизовали национальные ресурсы, чтобы дать достойный ответ на такие враждебные действия», - сказал украинский дипломат.

Он напомнил, что в 2016 году Украина приняла Стратегию кибернетической безопасности, и это был важный шаг на пути модернизации и цифрового развития Украины, повышения ее устойчивости к будущим кибернетическим угрозам.

«Моя страна с каждым годом становится все более устойчивой к таким атакам. Мы смогли создать стабильную систему кибернетической защиты, которая, безусловно, еще не является совершенной, но является надежной и достаточно гибкой, чтобы реагировать и предвидеть. Мы сотрудничаем с нашими европейскими и американскими партнерами на взаимовыгодных принципах, чтобы достичь лучшей устойчивости против российских кибератак», - отметил Пивоваров.

При этом он подчеркнул, что успех в борьбе с кибернетическими преступлениями может быть достигнут только тогда, когда цивилизованный мир создаст действительно эффективный механизм для привлечения государств, виновных в таких действиях, к правосудию. Должны быть созданы общие и равные для всех международные правила, которые станут предохранителем от превращения в оружие компьютерных технологий, главным назначением которых является развитие всего человечества…». ***(Украине удалось создать надежную систему противостояния кибератакам из России – дипломат // Укринформ (https://www.ukrinform.ru/rubric-polytics/3338882-ukraine-udalos-sozdat-nadeznuu-sistemu-protivostoania-kiberatakam-iz-rossii-diplomat.html). 25.10.2021).***

***

Боротьба з кіберзлочинністю в Україні

«Правоохранители разоблачили хакера, который создал сеть ботов, распространял вирусы и осуществлял DDoS - и спам-атаки.

Сотрудники Службы безопасности Украины вместе с другими правоохранительными органами разоблачили хакера, который создал и администрировал мощный ботнет - автоматизированную сеть из более чем 100 тысяч фейковых учетных записей. Через нее он осуществлял DDoS - и спам-атаки, выявлял уязвимости веб-сайтов и взламывал их, сообщает пресс-служба СБУ.

Как удалось установить киберспециалистам СБУ, злоумышленником оказался житель Ивано-Франковской области. Кроме кибератак и взлома сайтов, он занимался подбором паролей к ящикам электронной почты на удаленных платформах так называемым «брутфорсом».

Заказчиков находил на закрытых форумах и в чатах Telegram, а расчеты с «клиентами» осуществлял через запрещенные в Украине электронные платежные системы.

При этом, по данным следствия, прикарпатец является представителем российской электронной системы мгновенных расчетов Webmoney, на которую распространяется действие санкций СНБО. Он изготавливал и выдавал пользователям аттестаты подсанкционной платежной системы, которые используются для проведения трансакций.

В ходе обысков, проведенных по адресам регистрации и фактического проживания злоумышленника, изъято компьютерное оборудование с доказательствами противоправной деятельности.

Организатору ботнета готовится сообщение о подозрении по ч. 2 ст. 361-1 (создание с целью использования, распространения или сбыта вредоносных программных или технических средств, а также их распространение или сбыт) и ст. 363-1 (препятствование работе электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи путем массового распространения сообщений электросвязи) Уголовного кодекса Украины…». ***(Виктория Токарева. Распространял вирусы и совершал DDoS-атаки: правоохранители разоблачили хакера, создавшего сеть ботов// UNIAN.NET (https://www.unian.net/science/rasprostranyal-virusy-i-sovershal-ddos-ataki-pravoohraniteli-razoblachili-hakera-sozdavshego-set-botov-novosti-11573371.html). 11.10.2021).***

***

«В рамках международной спецоперации, проведенной Департаментом киберполиции Национальной полиции Украины с привлечением представителей Интерпола, Европола, а также правоохранительных органов Республики Франции и США разоблачили 25-летнего хакера, причастного к совершению вирусных атак более 100 иностранных компаний.

Об этом сообщила пресс-служба Киевской городской прокуратуры.

В ходе следствия установлено, что гражданин Украины распространял вредоносное программное обеспечение с целью дальнейшего вымогательства денежных средств у иностранных компаний за восстановление данных.

«Вирусное программное обеспечение попадало в компьютерные системы корпораций путем взлома программы для удаленной работы пользователя с компьютером, а также через спам-рассылку. После попадания в компьютерные системы вирус осуществлял шифрование данных, за восстановление доступа к которым с компаний требовались денежные средства», - говорится в сообщении.

По данным следствия, в результате кибератак пострадало более 100 иностранных компаний, среди которых известные мировые энергетическая и туристическая компании, а также разработчики техники, которым нанесен ущерб на сумму более 150 млн долларов США.

Идентифицировать украинского хакера удалось в ходе международной полицейской операции. Как установили правоохранители, мужчина имел сообщника, который помогал выводить деньги, добытые преступным путем.

В рамках следствия правоохранительными органами, привлеченными к спецоперации, проведены обыски на территории города Киева, Киевской и Хмельницкой областей по месту жительства хакера и близких к нему лиц, в ходе

которых изъяты денежные средства на общую сумму свыше 360 тыс. долларов США, компьютерная техника, терминалы мобильной связи, транспортные средства. Кроме того, на криптокошельках мужчины заблокировано 1,3 миллиона долларов США.

Следственные действия продолжаются.

Уголовное производство расследуется по ч. 2 ст. 361 (несанкционированное вмешательство в работу компьютеров, автоматизированных систем, компьютерных сетей или сетей электросвязи), ч. 3 ст. 209 (легализация (отмывание) имущества, полученного преступным путем) Уголовного кодекса Украины…». ***(Татьяна Герасименко. Вирусные атаки на сотню иностранных компаний: разоблачен украинский хакер // UNIAN.NET (https://www.unian.net/science/virusnye-ataki-na-sotnyu-inostrannyh-kompaniy-razoblachen-ukrainskiy-haker-novosti-11565976.html). 04.10.2021).***

***

«Кіберфахівці СБУ та спецоргани США провели спільну операцію із викриття українців, які діяли в мережі Darknet. Зловмисники займалися «відмиванням» грошей для міжнародних хакерів і за час своєї діяльності легалізували десятки мільйонів доларів.

Для виведення грошей з «тіні» зловмисники організували масштабну схему. Вони ховалися під різними нікнеймами в мережі Darknet, мали багатьох підставних осіб, а також працювали через різні фінансові сервіси.

Клієнтами викритих злочинців були хакери, які займалися кіберкрадіжками і хотіли вивести крадене у готівку. Наприклад, злодії, які «зламували» банківські рахунки компаній по всьому світу, забирали собі віртуальні гроші «жертви».

Більше того, ці особи самостійно виготовляли та продавали флеш-накопичувачі із вірусами, які зламували цифрові гаманці жертв та викрадали з них криптовалюту.

Їх вдалося викрити у Миколаєві, в рамках міжнародного співробітництва із органами США. Внаслідок обшуків у зловмисників правоохоронці вилучили:

- комп’ютерну техніку із доказами протиправної діяльності;
- шкідливі програмно-апаратні засоби;
- чорнові записи та готівку.

Наразі здійснюється аналіз вилученої інформації для притягнення до кримінальної відповідальності усіх відповідальних осіб, у тому числі іноземних замовників махінацій.

Заходи із викриття зловмисника проводилися співробітниками Департаменту кібербезпеки СБУ, Управління СБ України в Миколаївській області та слідчими ГСУ Нацполіції за процесуального керівництва Офісу Генерального прокурора». ***(Кіберфахівці СБУ та спецслужби США викрили злочинців, які «відмили» десятки мільйонів доларів з «Darknet» // Служба безпеки України (https://ssu.gov.ua/novyny/kiberfakhivtsi-sbu-ta-spetssluzhby-ssha-vykryly-zlochyntsiv-yaki-vidmyly-desiatky-milioniv-dolariv-z-darknet). 25.10.2021).***

***

«З початку 2021 року кіберфахівці СБУ блокували роботу 12 «ботоферм» потужністю понад 65 тисяч акаунтів. Через них поширювався антиукраїнський, антивакцинальний та інший деструктивний контент у соціальних мережах.

Про це повідомляє прес-служба СБУ.

Фахівці змогли локалізувати понад 1200 кібератак та кіберінцидентів на об'єкти критичної інфраструктури. Для захисту кібербезпеки держави, за матеріалами СБУ, розпочато 427 кримінальних проваджень, 62 зловмисники вже притягнуто докримінальної відповідальності.

Серед масштабних спецоперацій, проведених кібердепартаментом СБУ – блокування діяльності транснаціонального угруповання хакерів, які своїм шкідливим програмним забезпеченням Egregor та Maze «зламали» понад 150 компаній з Європи та США. Збиток від діяльності цих хакерів становить понад $80 млн.

Крім того, заблоковано масштабну злочинну схему оформлення дозвільних документів моряків. Через несанкціоноване втручання у роботу відповідного Державного реєстру щорічно злочинці незаконно отримували понад $150 млн.

СБУ активно протидіє поширенню фейків та проросійської пропаганди. Зокрема, за цей період розпочато 36 кримінальних проваджень за ст. 109 (дії, спрямовані нанасильницьку зміну або повалення конституційного ладу або на захоплення державної влади) таст. 110 (посягання на територіальну цілісність та недоторканність України) Кримінального кодексу України. Засуджено 23 особи.

Кіберфахівці Служби безпеки України викрили масштабну агентурну мережу, яка займалася розвідувально-підривною діяльністю на замовлення спецслужб РФ. Країна-агресор залучила українських громадян до створення та адміністрування низки політичних всеукраїнських та регіональних Telegram-каналів: «Легітимний», «Резидент», «Картель», «Пліткарка» та інші.

Також припинено деструктивну діяльність мережі інтернет-агентів, якою керували зРФ. Зловмисники діяли на території Дніпропетровської, Херсонської, Полтавської та Закарпатської областей. Вони підбурювали користувачів соцмереж до участі в акціях протесту та порушення суспільного спокою.

Заборонено в'їзд до нашої країни 83 іноземцям, причетним до пропаганди сепаратизму в інтернеті.

За матеріалами Департаменту кібербезпеки СБУ внесено пропозиції до Ради національної безпеки та оборони щодо введення санкцій щодо 187 фізичних та юридичних осіб. Крім того, за рішенням РНБО було обмежено роботу 500 веб-ресурсів за поширення деструктивної інформації про порушення конституційного ладу та територіальної цілісності України.

Заборонено діяльність 81 розробника програмного забезпечення та постачальника комп'ютерного обладнання з країни-агресора, які діяли на шкоду інтересам нашої держави.

Також на території України заблоковано роботу 3 електронних платіжних систем та 29 афілійованих компаній, які використовували для фінансування терористичної діяльності…»***(З початку року СБУ ліквідувала величезну «армію***

ботів» у соціальних мережах // UA.NEWS (https://ua.news/ua/s-nachala-goda-sbu-likvidirovala-ogromnuyu-armiyu-botov-v-sotsialnyh-setyah/). 27.10.2021).

***

«С момента выявления поддельного приложения до задержания его создателя прошло 3 дня. В липовой «Дії» можно было подделывать документы, например, паспорт.

В Запорожье задержали 21-летнего гражданина, который создал программу, полностью копирующую приложение "Дія". Об этом сообщает пресс-служба Нацполиции.

Как утверждают правоохранители, при помощи приложения пользователи могли изготавливать поддельные документы. Нарушителю теперь грозит до 6-ти лет тюремного заключения.

Кто оказался разработчиком фейковой "Дії"

Распространял приложение житель Запорожья через мессенджеры. Услуга была платной — 100 грн. В рекламе своего «продукта» он указывал, что несовершеннолетние смогут покупать алкоголь и сигареты. В фейковой «Дії» можно было менять возраст, добавлять любое фото и подделывать сертификат о вакцинации от коронавируса.

На данный момент правоохранители проводят мероприятия для блокировки каналов распространения поддельного приложения. Устанавливаются лица, которые купили лже-«Дію». Правоохранители будут оказывать правовую квалификацию действиям покупателей.

Также были проведены обыски в доме у задержанного. У него изъяли мобильные телефоны, компьютерную технику и банковские карты. Было открыто уголовное производство по части 2 статьи 361 Уголовного кодекса Украины — несанкционированное вмешательство в работу компьютеров, автоматизированных систем, компьютерных сетей или сетей электросвязи. Санкция статьи предусматривает до 6-ти лет лишения свободы.

На задержание вероятного разработчика липовой «Дії» отреагировал министр цифровой трансформации Михаил Федоров. Он предложил направить задержанного на исправительные работы.

«Предлагаю парня направить на исправительные работы в IT, без персональных данных и других сенсативных вещей. Вчера читал, что двум ребятам, которые воровали магнитолы, одесский судья назначил читать книги Марка Твена и Джека Лондона», — написал министр…» ***(Киберполиция задержала 21-летнего разработчика фейковой «Дії» (видео) // Фокус (https://focus.ua/digital/496365-kiberpoliciya-zaderzhala-21-letnego-razrabotchika-feykovoy-diji-video). 27.10.2021).***

***

«Протиправну діяльність 33-річного чоловіка викрили співробітники управління протидії кіберзлочинам у Дніпропетровській області спільно зі слідчими Дніпровського районного управління поліції та за сприянням працівників служби безпеки торговельної корпорації.

Схему збуту конфіденційної інформації налагодив колишній керівник аналітичного відділу мережі продуктових супермаркетів. За винагороду у понад 130 тисяч гривень діючі працівники корпорації передавали фігуранту інформацію, що містила комерційну таємницю. Зокрема, він незаконно отримував звіти щодо продажу товарів, відомості про заплановані акційні знижки, інформацію про відкриття нових магазинів.

Зібрані дані правопорушник збував компаніям-конкурентам. Таким чином мережа супермаркетів зазнала понад мільйон гривень збитків.

Правоохоронці провели обшуки та вилучили докази причетності до протиправної діяльності.

Чоловіка було затримано в порядку ст. 208 Кримінально процесуального кодексу України. Наразі правоохоронці встановлюють його спільників.

Зловмиснику оголошено про підозру за ч. 3 ст. 27, ч.ч. 2, 3 ст. 362 (Несанкціоновані дії з інформацією, яка оброблюється в комп'ютерах, автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї) Кримінального кодексу України.

Підозрюваному загрожує до шести років позбавлення волі. Вирішується питання щодо обрання запобіжного заходу.

Процесуальне керівництво здійснює Центральна окружна прокуратура Дніпра». ***(Кіберполіцейські Дніпропетровщини викрили чоловіка у збуті конфіденційних даних торговельної мережі // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpoliczejski-dnipropetrovshhini-vikrili-cholovika-u-zbuti-konfidenczijnix-danix-torgovelnoji-merezhi/). 28.10.2021).***

***

«Співробітники СБУ викрили київських підприємців, які розкрадали кошти, виділені на захист секретної інформації, яка циркулює у державних установах і силових відомствах України. За попередньою інформацією, зловмисники завдали державі збитків на 20 млн грн…

«Розкрадання коштів відбувалося за рахунок махінацій із вартістю робіт. Зловмисники завідомо завищували ціни на власні послуги, а неправомірно отримані гроші виводили через фіктивні підприємства. При цьому організатори оборудки – київська приватна компанія, яка пройшла сертифікацію Держспецзв’язку і має відповідну ліцензію», - повідомили в СБУ.

Як зазначається, головним завданням ділків, відповідно до контрактів, був технічний та криптографічний захист інформації, яка циркулювала у державних органах.

Протягом 2018-2019 років ця фірма обслуговувала такі відомства: Національна поліція України; Національна гвардія України; АТ «Укрзалізниця»; Міністерство молоді та спорту України; ДП «УКРАЕРОРУХ»; ДП «Укренерго»; Окружний адміністративний суд України.

Наразі двом фігурантам провадження - директорам фіктивних підприємств, - повідомлено про підозру за ч.2 ст.205-1 КК України за підроблення документів, які подаються для проведення державної реєстрації юридичної особи.

Під час обшуків виявлено та вилучено документи фінансово-господарської діяльності та комп'ютерну техніку. Крім того, під час обшуку задокументовано факти зберігання посадовими особами «фірми» інформації з грифом «таємно» на не зареєстрованих носіях інформації. Це суперечить нормативно-правовим документам у сфері охорони державної таємниці.

Наразі планується проведення експертизи щодо наявності у документах відомостей, що становлять державну таємницю, судово-економічної та комп'ютерно-технічної експертиз з метою підтвердження завданих державі збитків та прийняття за їх результатами відповідного процесуального рішення, повідомили в пресслужбі…». **(Київська фірма вкрала 20 мільйонів, виділених державою на кіберзахист секретної інформації – СБУ // Укрінформ (https://www.ukrinform.ua/rubric-society/3340720-kiivska-firma-vkrala-20-miljoniv-vidilenih-derzavou-na-kiberzahist-sekretnoi-informacii-sbu.html). 28.10.2021).**

***

Міжнародне співробітництво у галузі кібербезпеки

«Министр обороны Андрей Таран обратился к канцлеру Министерства обороны Эстонской Республики Кусти Салму с просьбой поддержать инициативу Украины о присоединении к Объединенному центру передовых технологий по кибероборoне НАТО.

…об этом сообщает пресс- служба Минобороны.

Отмечается, что во вторник, 5 октября, Таран обсудил с канцлером Министерства обороны Эстонии актуальные вопросы, представляющие взаимный интерес.

Таран выразил благодарность Салму за непоколебимую политическую поддержку Таллинном усилий Украины по защите суверенитета и восстановления территориальной целостности страны, практическую помощь Вооруженным силам Украины и стойкую позицию в отношении нашей страны в пределах Альянса.

«Политическая и дипломатическая поддержка Украины Эстонской Республикой, в частности стратегического евроатлантического курса нашего государства, является чрезвычайно важной. Рассчитываем на продолжение последовательной позиции наших друзей в разблокировании заседаний Комиссии Украина-НАТО на уровне министров обороны и получение Плана действий относительно членства в Альянсе», - отметил Таран.

Особое внимание было уделено вопросам двустороннего оборонного сотрудничества в сфере военного образования, военной подготовки, сотрудничества по кибербезопасности, а также лечения и реабилитации в Эстонии раненых украинских военнослужащих.

«Министр обороны Украины обратился к канцлеру Министерства обороны Эстонской Республики с просьбой поддержать инициативу Украины о присоединении к Объединенному центру передовых технологий по кибероборoне НАТО. Сейчас центр является одним из ключевых элементов системы Альянса по развитию возможностей в сфере кибернетической обороны. Он обеспечивает борьбу с кибератаками и киберзащиту информационных систем, а также обучение и подготовку специалистов по киберзащите НАТО», - говорится в сообщении…». ***(Таран просит Эстонию поддержать присоединение Украины к центру кибероборoны НАТО // Укринформ (https://www.ukrinform.ru/rubric-polytics/3327836-taran-prosit-estoniu-podderzat-prisoedinenie-ukrainy-k-centru-kiberoborony-nato.html). 05.10.2021).***

***

«Під час підбиття підсумків Олександр Гринчак особливу увагу звернув на взаємодію кіберполіції з іноземними колегами-правоохоронцями.

«Сьогодні кіберполіція не лише допомагає підрозділам кримінального блоку у розкритті та виявленні злочинів, вчинених з використанням інформаційних технологій та мережі Інтернет, підрозділ робить акцент на взаємодії з іноземними колегами, адже кіберзлочинність немає чітко окреслених кордонів. Результатами такої співпраці стало успішне проведення п’яти міжнародних поліцейських операцій з викриття хакерських угруповань. Наші закордонні колеги на високому рівні оцінили організацію та результати проведених операцій» - повідомив Олександр Гринчак.

Так, на початку року кіберполіція спільно з правоохоронними органами Німеччини, США, Великобританії та Нідерландів, викрила та заблокувала діяльність транснаціонального хакерського злочинного угруповання з розповсюдження найнебезпечнішого і найстійкішого вірусного програмного забезпечення – «EMOTET». В результаті діяльності хакерів іноземні банки та фінустанови зазнали 2,5 мільярда доларів збитків.

Також цього року кіберполіція викрила хакерське угруповання у розповсюдженні вірусу-шифрувальника “Clop” та нанесенні іноземним компаніям пів мільярда доларів збитків. Хакерське угруповання викрили в рамках міжнародної операції за сприяння та координації Інтерполу та спільно з працівниками правоохоронних органів США та Республіки Корея, співпраця з якими відбулася вперше.

За словами начальника Департаменту кіберполіції Олександра Гринчака, з початку цього року працівники кіберполіції ідентифікували понад 5 тисяч Інтернет-зловмисників.

«Кіберполіція веде наступальну боротьбу, кількість злочинів, вчинених у віртуальному просторі, лише зростає. Правопорушники щоразу вдосконалюють свої схеми або ж вигадують нові. Тому ми ще й робимо акцент на превентивній роботі з населенням. Адже знання основних правил кібергігієни мінімізує ризики постраждати від злочинних дій хакерів чи інтернет-шахраїв», - підкреслив Олександр Гринчак.

Також він повідомив, що упродовж 9-ти місяців поточного року працівники підрозділу надали кваліфіковану допомогу 48 тисячам громадян, які зверталися до кіберполіції». ***(З початку року кіберполіцейські ініціювали п'ять міжнародних операцій з викриття хакерських угруповань – Олександр Гринчак // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/z-pochatku-roku-kiberpoliczejski-inicziyuvaly-pyat-mizhnarodnyx-operaczij-z-vykryttya-xakerskyx-ugrupovan--oleksandr-grynchak-3694/). 12.10.2021).***

***

Світові тенденції в галузі кібербезпеки

«Эксперты по кибербезопасности рекомендуют интернет-пользователям не устанавливать в качестве паролей к учетным записям имена вымышленных супергероев - их очень просто взломать.

Об этом говорится в докладе компании Mozilla, разработавшей браузер Firefox.

На основе анализа базу данных взломанных паролей с сайта haveibeenpwned.com, аналитики обнаружили более 900 тысяч паролей с именами супергероев.

В топ-5 самых популярных вариантов входят:

«Супермен» (почти 370 тыс.);

«Бэтмен»(более 226 тыс.);

«Человек-паук» (160 тыс.);

«Росомаха» (53 тыс.);

«Железный человек» (44 тыс.).

Кроме того, тысячи аккаунтов по всему миру оказались защищены паролями в виде имен вымышленных персонажей, обладающих суперспособностями, например, «Джеймс Хоулетт» (Росомаха), «Кларк Кент» (Супермен), «Брюс Уэйн» (Бэтмен) и «Питер Паркер» (Человек-паук).

«Пароль подобен ключу от вашего дома. В онлайн-мире ваш пароль обеспечивает безопасность вашего дома с личной информацией, поэтому важно убедиться, что он надежен», — призывают киберэксперты…». ***(Станислав Кожемякин. Киберэксперты названы самые популярные взломанные пароли // UNIAN.NET (https://www.unian.net/science/kiberekspertу-nazvany-samye-populyarnye-vzlomannye-paroli-novosti-11566639.html). 04.10.2021).***

***

«Даже несмотря на то, что организации отметили увеличение количества нападений и взломов по сравнению с предыдущим годом, многие из них смогли лучше выявлять и реагировать на них - из-за текущих инвестиций в реагирование на инциденты и безопасность. Это основано на текущем опросе Dark Reading, в котором приняли участие 215 профессионалов в области ИТ и

кибербезопасности, которые распознали виды инцидентов, представляющих наибольший риск для тонких знаний группы.

ВотчетеDark Reading «Состояние реагирования на инциденты в 2021 году» показано, что профессионалы в области безопасности больше всего участвовали в нарушениях интеллектуальной собственности и коммерческих секретов и методов (36%), принятых путем несанкционированного использования целей уполномоченными клиентами (17%).Кроме того, 16% заявили, что сбои в работе внутренних ИТ-программ, целей или сетей представляют серьезную организационную опасность.

Выбирая лучший путь, респонденты, тем не менее, рассматривают заражение программ-вымогателей и вредоносных программ, а также нарушение данных о покупателях и сотрудниках как важные угрозы для группы, хотя и не так много, как в прошлом году. В 2021 году 48% респондентов указали вымогатели и вредоносное ПО как потенциальные угрозы, по сравнению с 58% в 2020 году, тогда как 44% в 2021 году указали на потерю знаний покупателей и сотрудников по сравнению с 59% в 2020 году. связаны с более высокой степенью уверенности в средствах группы для обнаружения потенциального компрометации так же быстро, как это произойдет, или в течение нескольких минут / часов после инцидента…». ***(Loss of Intellectual Property, Customer Data Pose Greatest Business Risks // The Hack Posts (https://thehackposts.com/loss-of-intellectual-property-customer-data-pose-greatest-business-risks/). 05.10.2021).***

***

«Дэвид Камминс, вице-президент Tenable по региону EMEA, исследует, как университеты подвергаются серии кибератак в 2021 году и что они могут сделать, чтобы защитить себя.

Пандемия сильно повлияла на сектор образования. Чтобы обеспечить продолжение основной учебной программы и экзаменов для студентов, бесценными стали такие системы, как облачное программное обеспечение, инструменты видеоконференцсвязи и игровое электронное обучение. Однако этот переход к полной зависимости от технологий означал, что поверхность кибератак расширилась, и все большее количество электронных учреждений стали уязвимыми из-за использования новых систем в течение учебного дня.

Национальный центр кибербезопасности (NCSC) подчеркнул угрозу атак с использованием программ-вымогателей на сектор образования Великобритании в августе / сентябре 2020 года. Поскольку большинство образовательных учреждений в настоящее время возвращается к очному обучению, этот сектор по-прежнему находится в поле зрения злоумышленников. В конце мая - начале июня NCSC снова предупредил, что расследует очередной рост атак программ-вымогателей на школы, колледжи и университеты в Великобритании.

Эту мысль подтверждает и Microsoft, которая из-за глобальной активности угроз твердо ставит сектор образования на первое место, утверждая, что это отрасль, наиболее пострадавшая от сообщений о встречах с корпоративными вредоносными программами за последние 30 дней.

Для академических учреждений виртуальные технологии являются очень важным фактором в учебный день, но сектор обязательно должен принять меры для устранения рисков.

К счастью, есть несколько простых и доступных шагов, которые образовательные учреждения могут предпринять для усиления мер безопасности и обеспечения надлежащей защиты сетей:

Определите общие точки отказа

Подавляющее большинство сегодняшних утечек данных не являются изощренными для опытного глаза. Фактически, большинство инцидентов, которых можно избежать, вызваны либо известными, но не исправленными уязвимостями, либо посещением вредоносного веб-сайта, зашифрованного с помощью вредоносного ПО.

Выявление и устранение распространенных уязвимостей, предпочитаемых преступниками, а также блокировка известных вредоносных сайтов и IP-адресов из сети поможет защитить данные и системы.

Принудительная многофакторная аутентификация для сотрудников и студентов

Обеспечение доступности средств удаленного обучения только для необходимых и соответствующих людей может быть достигнуто с помощью решений для многофакторной аутентификации. Пользователи должны предоставить дополнительную форму идентификации, а не полагаться на комбинацию имени пользователя и пароля для доступа к системам. Могут быть реализованы дополнительные уровни идентификации, такие как одноразовый пароль (OTP), отправленный через SMS, или сканирование отпечатка пальца или радужной оболочки глаза.

Оптимизация ограниченных ресурсов и поддержки

Совместные консультативный выданная NCSC, кибербезопасность и инфраструктура Агентство безопасности (CISA) и австралийская кибербезопасность центр (ACSC)подтвердила, а не творческие векторов угроз, плохие актеры, какправило, целевые известные уязвимости скомпрометировать незакрытых системы и нарушение защиты организации. Чтобы предотвратить это, ИТ-команды должны определить приоритеты известных недостатков, используя подход к управлению уязвимостями на основе рисков. Этот подход фокусируется на конкретных угрозах, которые представляют реальный, а не теоретический риск для организации, при этом значительно сокращая время, затрачиваемое на определение приоритетов угроз вручную. Исследования показали, что такой подход может повысить безопасность в 7,5 раз без дополнительных затрат.

Иметь целостный подход

С начала пандемии к школьным сетям получил доступ ряд неизвестных устройств, с которыми командам безопасности никогда не приходилось сталкиваться раньше. Для большинства школ понимание и отображение такого обширного набора активов может быть ужасно сложным. Обнаружение и управление неизвестными активами может быть практически невозможно без надлежащего использования инструментов. Еще один полезный ресурс, который в настоящее время пилотируется Министерством образования, - это инструмент

Cyber Secure. С помощью бесплатного и анонимного инструмента самооценки школы могут оценивать свои меры кибербезопасности по системе оценок от 0 до 5, чтобы помочь понять риски, с которыми они сталкиваются.

Выполнение этих начальных шагов к пониманию нового ландшафта атак должно быть приоритетом для любого образовательного учреждения, которое движется вперед. Усилия по улучшению кибергигиены в организационном масштабе помогут создать более насыщенное и безопасное образование для следующего поколения классов.

Поскольку школы возвращаются к обучению в помещениях, а некоторые продолжают использовать виртуальные системы, внедренные в разгар пандемии, эти простые меры безопасности помогут гарантировать, что учебные заведения сохранят доверие учащихся, родителей и учителей.» ***(Education sector suffers series of cyber attacks in 2021 // Open Access Government (https://www.openaccessgovernment.org/education-sector-suffers-series-of-cyber-attacks-in-2021/122465/). 15.10.2021).***

***

«Большинство организаций используют то, что можно назвать активным подходом к кибербезопасности. Они готовы к определенным действиям после того, как произойдет атака. Или они используют реактивный подход, предпринимая действия после завершения атаки. Проактивная стратегия кибербезопасности заключается в том, чтобы действовать до того, как произойдет какая-либо атака; это хорошая позиция готовности к кибербезопасности.

Ознакомьтесь с политиками, инструментами и практиками, составляющими упреждающие меры кибербезопасности.

Проактивный, а не реактивный и активный обзор

Создание и проверка инструментов, протоколов, политик и практик безопасности слишком часто - это процесс, который нужно запрограммировать и забыть. Но мир постоянно меняется. Проактивный подход состоит в том, чтобы постоянно анализировать все это с учетом возникающих угроз, новых инструментов и новых идей, часто обновляя все.То же самое и с тренировками. Вам следует как минимум раз в квартал активно пересматривать «учебную программу» для ознакомления с кибербезопасностью и соответствующего обучения сотрудников.

Этический взлом

Вместо того, чтобы ждать атаки, лучше взломать самостоятельно. Сертифицированные этические хакеры могут исследовать вашу защиту, выискивая уязвимости и слабые места. Эти исследователи атакующей безопасности используют те же методы и инструменты, что и злоумышленники. Упражнения красной / синей команды, тестирование на проникновение и другие симуляции позволяют вашим сотрудникам извлекать уроки из кибератак, не подвергаясь реальной атаке.

Автоматизировать разведку

Используйте инструменты, которые позволяют понять, что происходит в ваших сетях, и автоматически реагировать. Проактивный подход означает, что у

вас есть как можно больше исправлений, которые уже заблокированы и загружены.Интеллектуальное программное обеспечение круглосуточно и без выходных выявляет нарушения и странное поведение, готовое локализовать и исправить, когда что-то действительно происходит. Это нападение, а не защита.

Нулевое доверие

Используя активный подход, вы можете запирать двери, когда ваша система обнаруживает злоумышленников. Но с упреждающим подходом вы можете запереть двери до их прибытия.

Принцип нулевого доверия направлен на проверку и авторизацию каждого устройства, приложения и пользователя, пытающегося получить доступ к каждому ресурсу.

Для злоумышленников, даже если они могут украсть пароль, они все равно обнаружат, что двери заперты, потому что у них нет авторизованного устройства. Это упреждающее запирание дверей с помощью модели нулевого доверия еще более важно, поскольку многие удаленные сотрудники используют домашние офисы. Они используют оборудование в местах с неизвестной физической безопасностью и в сетях неизвестного качества.

Модель нулевого доверия является динамичной и требует от вас постоянного мониторинга, обучения и адаптации.

Превентивная и реактивная в мониторинге конечных точек

Проактивная безопасность означает проактивный мониторинг конечных точек. С распространением Интернета вещей, облачной инфраструктуры и устройств для удаленной работы это важно как никогда. Автоматизируйте мониторинг конечных точек, чтобы максимально повысить локальную безопасность каждого устройства.

Индикаторы поведения

Активная и реактивная кибербезопасность требует поиска индикаторов компрометации - признаков, указывающих на то, что произошло нарушение и было совершено киберпреступление. Но проактивная кибербезопасность ищет индикаторы поведения (IoB), совокупность действий пользователей.

Например, он может обнаружить, что кто-то загружает бизнес-данные на внешнее запоминающее устройство или загружает код в неизвестную облачную службу. IoB может быть изменением разрешений или переключением сети пользователя на настольном ПК с внутреннего Wi-Fi на точку доступа мобильного широкополосного доступа. Собрав сотни или тысячи из них, можно составить более четкую картину того, где организация уязвима с точки зрения поведения. Он также может вносить изменения с минимальными нарушениями. Например, вы можете подготовиться к решению об активном отключении подключения флэш-накопителя, заранее подготовив пользователей, которые используют флэш-накопители, к поиску более безопасных вариантов.Он также может изолировать определенные устройства или конечные точки, чтобы внимательно отслеживать, когда поведение сотрудников подвергает их риску.

Проактивный или ответный - это образ мышления

Проактивная кибербезопасность - это широкий, всеобъемлющий подход. Он включает в себя не только конкретные методы и практики, но и настрой на наступательную кибербезопасность.

В конце концов, зачем ждать, пока на вас нападут? Вместо этого вы можете действовать сейчас и предотвратить нападение». ***(Mike Elgan. What Is Proactive Cybersecurity? // IBM (https://securityintelligence.com/articles/what-is-proactive-cybersecurity/). 20.10.2021).***

***

«По мере увеличения масштабов и серьезности кибератак растет и глобальный спрос на профессионалов в области кибербезопасности - во всех сферах деятельности и во всех секторах. Предложение, похоже, не успевает, что приводит к острой нехватке талантов.

Но в этой нехватке талантов есть еще больший и более тревожный пробел: отсутствие разнообразия в кибербезопасности.

Улучшение условий работы для недопредставленных групп

Последние статистические данные о демографии в сфере кибербезопасности вызывают беспокойство: согласно последнему отчету центра Aspen Digital Tech Policy, недопредставленные группы, такие как черные (9%), латиноамериканские (4%) и азиатские (8%) профессионалы, составляют все более низкий процент индустрия. Например, женщины составляют 51% населения, но только 24% сотрудников, занимающихся кибербезопасностью.

С другой стороны, только в Соединенных Штатах существует почти 500000 открытых вакансий в сфере кибербезопасности, что свидетельствует о системном, но не непреодолимом разрыве. Если мы будем работать вместе, предпринимая индивидуальные и коллективные действия, чтобы улучшить текущую среду для недостаточно представленных групп, это может иметь долгосрочные положительные последствия в области кибербезопасности.

Специалисты по кибербезопасности работают сверхурочно. Во многих случаях они изнуряют себя, чтобы защитить инфраструктуру, ИТ-системы и учреждения. Почти все в кибербезопасности растянуты до тонкости. Как организациям, так и нациям нужны более квалифицированные люди для работы в области кибербезопасности.

Профессионалы должны действительно понимать угрозы, предлагая более надежные решения. Для этого отрасль должна исправить некоторые аспекты найма, удержания и развития лидерских качеств.

Выбор кандидатов с правильными основными качествами

Сосредоточение внимания на препятствиях на пути к вовлечению и успеху в отрасли, а не на явной дискриминации, может помочь уменьшить нехватку талантов. Лидеры кибербезопасности играют в этом важную роль. При отборе кандидатов они должны сосредоточиться на разнообразии и инклюзивности.

Вместо того, чтобы просто набирать новых разнообразных кандидатов в рабочую силу, они также должны предоставить этим профессионалам, которые уже работают, возможности и инструменты для достижения успеха и роста. Наконец,

менеджеры должны позволить разным кандидатам получить набор навыков, чтобы добиться успеха в качестве будущих лидеров в этой области.

При наборе опытных талантов следует учитывать любопытство, способность решать проблемы и критическое мышление. Кибербезопасность - это динамичная область, которая постоянно меняется, особенно когда речь идет об угрозах или потенциальных атаках. Чтобы добиться успеха в этой области, профессионалы не могут оставаться статичными в своих знаниях.

Вот почему любознательный ум и способность решать проблемы имеют решающее значение для следующего поколения киберпрофессионалов.

Люди, стремящиеся к кибербезопасности, считают, что даже получить первую работу слишком сложно. Работа начального уровня, на которую они претендуют, требует ряда квалификаций.

Что, если бы рекрутеры смотрели на основные черты характера, а затем обучались и вкладывались в людей? Это практика, которую используют многие военные по всему миру, в том числе армии Израиля и США.

Приоритет разнообразия, справедливости и инклюзивности

Вдобавок к этому лидеры должны позаботиться о людях, уже работающих в отрасли, особенно когда речь идет о будущих руководящих должностях. Это включает в себя все: от профессионального развития и союзничества до ухода за детьми и оплачиваемого отпуска по семейным обстоятельствам.

Вот где нужны такие усилия, как #ShareTheMicInCyber. Проект подчеркивает опыт профессионалов, уже работающих в отрасли. Инициативы, такие как CyberBase и #MakingSpace от института R Street, которые направлены на повышение разнообразия мероприятий по кибербезопасности, а также стипендиальный фонд Women in Security and Privacy, устраняющий финансовые препятствия для тренингов по кибербезопасности, выросли из #ShareTheMicInCyber. Это действенные и действенные способы, благодаря которым союзники сильно изменили ситуацию в этой сфере.

Организации, ставящие во главу угла разнообразие, равенство и инклюзивность, считают эти четыре конкретных шага полезными:

Сделайте ставку на возможности удержания и развития различных сотрудников. Удержание сотрудников имеет важное значение, если вы хотите добиться разнообразия на более высоких уровнях организации.

Относитесь ко всем сотрудникам как к личностям, дайте им возможность самовыражаться, создавайте безопасное пространство и признавайте их вклад.

Убедитесь, что ваш лидер активно поддерживает разнообразие, равенство и вовлеченность в организации.

Создавайте возможности для всех публиковать, писать и участвовать в публичных выступлениях.

Подготовка к будущим вызовам

Освещение большего количества путей к лидерству для большего числа сотрудников жизненно важно для удержания талантов. Но разнообразие должно быть представлено на всех уровнях организации. Все эти вопросы взаимосвязаны и связаны с национальной и международной безопасностью.

Следующее поколение лидеров в области кибербезопасности должно быть подготовлено.Настоящие лидеры должны сосредоточиться на создании возможностей для разнообразной группы сотрудников для профессионального развития, наставничества и создания сетей.

Отсутствие разнообразия закрывает нам глаза на бесчисленное множество способов, которыми субъекты могут напасть на нас, и лишает нас талантов и вовлеченности важных слоев населения мира. Отсутствие разных точек зрения и разнообразного представления мешает нам смотреть на проблемы сегодняшнего дня. Это истощает нашу энергию и способность предвидеть будущие угрозы.

По мере того как мы внедряем цифровизацию во все сферы нашей жизни, угрозы нашей безопасности и здоровью становятся все более масштабными и сложными. Эти угрозы необходимо решать в глобальном масштабе - творческими способами.

Разнообразие - жизненно важная часть нашего коллективного инструментария, который гарантирует более надежные, инновационные и гибкие идеи.

Трудно понять, с чего начать. Трудно признать свою привилегию и знать, что вы можете добиться большего... Это требует серьезного самоанализа. Но с точки зрения безопасности, бизнеса и морали это того стоит.

Разбейте проблему, определите свою платформу, используйте рычаги и действуйте». ***(Lauren Zabierek, Algirde Pipikaite. Why cybersecurity needs a more diverse and inclusive workforce // World Economic Forum (https://www.weforum.org/agenda/2021/10/why-cybersecurity-needs-a-more-diverse-and-inclusive-workforce/). 26.10.2021).***

***

«Во вторник Google объявил о создании новой команды по кибербезопасности, которая поможет реагировать на атаки на правительства и другие критические группы, а также о новой программе, направленной на усиление кибербезопасности предприятий.

Группа действий по кибербезопасности Google будет состоять из экспертов по кибербезопасности компании и будет предоставлять клиентам услуги реагирования на инциденты, консультационные услуги по планам безопасности и способы безопасного развертывания Google Cloud, что усложнит задачу этих клиентов. успешно атакован хакерами.

«Кибербезопасность стоит на первом месте в повестке дня каждого высшего руководства и совета директоров, учитывая растущую значимость эксплойтов в цепочке поставок программного обеспечения, программ-вымогателей и других атак», - заявил во вторник генеральный директор Google Cloud Томас Куриан.«Группа действий по кибербезопасности Google является частью нашего постоянного стремления быть лучшим партнером для наших корпоративных и государственных заказчиков на их пути преобразования безопасности».

Фил Венейблс, директор по информационной безопасности и вице-президент Google Cloud, заявил журналистам перед объявлением о новой команде, что они

надеются, что это будет «ведущая в мире группа консультантов по кибербезопасности».

«У этой группы есть особая миссия - поддержка безопасности и цифровой транспортировки для правительств и критически важных инфраструктур, предприятий и малых предприятий, и на самом деле видение этой группы состоит в том, чтобы направлять клиентов через цикл их преобразования безопасности», - сказал Венейблс.

Джен Истерли, директор Агентства по кибербезопасности и безопасности инфраструктуры (CISA), похвалила Google за действия, особенно после создания CISAСовместного сотрудничества в области киберзащиты (JCDC) для защиты страны от кибератак.Google Cloud является участником группы.

«Приятно видеть, что такая крупная компания, как Google Cloud, ориентируется на поддержку кибербезопасности всех организаций, больших и малых, с помощью своей группы действий по кибербезопасности, и в рамках JCDC и других инициатив мы надеемся на сотрудничество с ними и другими технологическими компаниями. в этом жизненно важном усилии», - сказал Истерли в заявлении во вторник.

Группа действий по кибербезопасности Google является частью более широкого спектра инициатив в области кибербезопасности, которые преследует Google, в том числе 10 миллиардов долларов, которые компания обязалась инвестировать в кибербезопасность в течение следующих пяти лет после встречи в Белом доме.

Эти усилия также включают программу повышения безопасности труда, объявленную Google во вторник. Программа сочетает в себе Google Workspace с предложениями по кибербезопасности от кибергрупп Palo Alto Networks и CrowdStrike, чтобы помочь организациям, более уязвимым для кибератак, таким как малые предприятия и другие группы, работающие удаленно.

«Как свидетельствуют ежедневные заголовки, количество угроз растет, а уязвимости в старых системах связи и совместной работы продолжают эксплуатироваться», - заявил во вторник Сунил Потти, вице-президент и генеральный менеджер Google Cloud Security.«Work Safer облегчает организациям принятие более жестких мер безопасности для защиты от фишинга, вредоносных программ, программ-вымогателей и других кибератак»…». ***(MAGGIE MILLER. Google creates cybersecurity team to respond to increased hacks // NEXSTAR MEDIA INC. (https://thehill.com/policy/cybersecurity/576280-google-creates-cybersecurity-team-to-respond-to-increased-hacks). 12.10.2021).***

***

«Учитывая текущие заголовки, можно подумать, что каждая организация должна постоянно находиться в состоянии кибервойны. Куда бы мы ни посмотрели, мы находимся в осаде. С одной стороны, это атаки программ-вымогателей, а с другой - взломы цепочки поставок, спонсируемые государством.

Решающим фактором на любом поле боя является так называемый «туман войны». Сэр Лонсдейл Огастес Хейл описал это как «состояние невежества, в

котором командиры часто оказываются в отношении реальной силы и положения не только своих врагов, но и своих друзей». Правильно - знание того, что делают ваши союзники, может быть так же важно, как и знание того, что делают ваши враги. Если применить это к полю битвы за информационную безопасность, то отсутствие видимости того, что нормально в вашей собственной сети, может помешать вашим усилиям так же, как и отсутствие информации об угрозах.

Действительно, видимость - важнейший элемент высокой безопасности. Я думаю о видимости как о данных, которые могут мне сказать:

- Что было в прошлом
- Что происходит сейчас
- Что может случиться в будущем

В мае этого года организации по всему миру проверяли свои сети, серверы и журналы Exchange, чтобы узнать, стали ли они жертвами команды HAFNIUM или десятков второстепенных участников. На основе того, что содержалось в этих журналах, каждая организация могла бы в идеале определить уровень вторжения, если таковой имеется, и соответствующие следующие шаги. Видение того, что злоумышленники делали в прошлом, давало жертвам знания, позволяющие принимать обоснованные бизнес-решения в отношении настоящего. Как говорится, знание - сила.

Видимость может исходить из сетевых журналов, захвата пакетов, телеметрии приложений или чего-либо еще, что может отправлять данные о том, что находится в среде или что в ней происходит. Хорошая видимость достигается за счет связывания всех этих источников данных вместе таким образом, что что и когда помещается в контекст того, кто и почему.

Переход от исторической видимости к видимости в реальном времени - логический шаг, который может помочь группам безопасности создавать триггеры, правила и предупреждения для автоматического принятия мер в зависимости от того, что происходит прямо сейчас. Но есть третий тип видимости, который может помочь совершенно по-другому.

Вы когда-нибудь слышали, чтобы кто-то сказал: «Меня беспокоит изменение системы безопасности, потому что я не знаю, может ли это что-то сломать»? Неуверенность в изменениях может убить инициативу по безопасности быстрее, чем вы можете сказать «вторник исправлений».Но что, если бы вызнали, что это безопасно, и могли бы это доказать?

Вот один пример: я сторонник блокирования трафика сервера в Интернет, разрешая определенные, требуемые направления. Это отличный способ сделать жизнь трудной для нападающих, но я получил свою долю от заинтересованных сторон буксировки, когда указывает на это, на основе - скажем прямо - страх перед неизвестным. Но, используя прозрачность сети, как историческую, так и в реальном времени, я могу показать, что в этом нет ничего страшного.

Мы тратим много времени и усилий, чтобы замечать нападающих - и на то есть веские причины! Но без видимости наших собственных организаций у нас остается слишком много неуверенности. Итак, как вы можете использовать большую видимость, чтобы противостоять туману войны?» ***(James Nelson. Countering the fog of war in cybersecurity // BNP Media***

(https://www.securitymagazine.com/articles/96319-countering-the-fog-of-war-in-cybersecurity). 18.10.2021).

***

«Национальный альянс кибербезопасности и CybSafe объявили о выпуске отчета, в котором было опрошено 2000 человек в США и Великобритании. В отчете были рассмотрены ключевые тенденции, отношение и поведение в области кибербезопасности в преддверии Месяца осведомленности о кибербезопасности в этом месяце.

«Ландшафт угроз кибербезопасности столь же сложен и разнообразен, как никогда», - сказала Лиза Плаггемьер, временный исполнительный директор Национального альянса по кибербезопасности.

«Ежедневные заголовки об утечках данных и атаках программ-вымогателей свидетельствуют об усугублении проблемы, но большинство людей не знают, какие простые шаги они могут предпринять, чтобы стать частью решения. Очень важно иметь более глубокое понимание как проблем, с которыми мы сталкиваемся, так и преобладающих взглядов и поведения среди населения».

«Кибербезопасность - это больше, чем просто инструменты, это люди», - сказал Оз Алаше, генеральный директор CybSafe.«Слишком часто в разговорах о кибербезопасности о людях забывают».

Киберпреступность считается более распространенной среди миллениалов и поколения Z

Согласно результатам исследования, миллениалы (44%) и поколение Z (51%) с большей вероятностью скажут, что они испытали киберугрозу, чем бэби-бумеры (21%).Кроме того, 25% миллениалов и 24% представителей поколения Z заявили, что их личности украли однажды, по сравнению с только 14% бэби-бумеров.Фактически, 79% бэби-бумеров заявили, что никогда не были жертвами киберпреступлений.

«Несмотря на миф о том, что пожилые люди с большей вероятностью будут уязвимы для киберпреступников и их тактики, наше исследование показало, что более молодые поколения с гораздо большей вероятностью осознают, что они стали жертвой киберпреступности», - сказал Плаггемьер.

«Это явное напоминание для технологической отрасли о том, что мы не можем воспринимать осведомленность о кибербезопасности как должное среди любой демографической группы и должны сосредоточиться на нюансах каждой отдельной группы. И, очевидно, нам необходимо переосмыслить представления о том, что молодые люди более технически подкованы и чаще используют передовые методы кибербезопасности, чем пожилые пользователи технологий».

Общественность не принимает передовые методы кибербезопасности

Согласно отчету, общественный отклик и внедрение общеизвестных передовых методов, включая надежные пароли, многофакторную аутентификацию (MFA) и другие, в лучшем случае невысокие.Выводы о передовых методах включают:

Плохая гигиена паролей: 46% респондентов заявили, что онииспользуют другой парольдля важных онлайн-учетных записей, а 20% заявили, что они

«никогда» или «редко» делают это.Кроме того, только 43% заявили, что создают длинный и уникальный пароль «всегда» или «очень часто».

МИД остается загадкой: 48% респондентов утверждают, что «никогда не слышали о МИД».

Задержка установки обновлений программного обеспечения: 31% респондентов сказали, что они либо «иногда», «редко», либо «никогда» не устанавливают обновления программного обеспечения.

«Существует явный разрыв между индустрией высоких технологий и общественностью, когда дело доходит до внедрения передовых методов кибербезопасности», - сказал Алаше. «Существует неопровержимое доказательство того, что простые передовые методы, такие как надежные пароли, MFA и регулярная установка обновлений, могут творить чудеса для повышения общей кибербезопасности.

«В конечном счете, не существует универсального подхода к кибербезопасности. Чтобы обратить вспять эту тенденцию и более значимо вовлекать людей в безопасное онлайн-поведение, мы должны занять более ориентированное на человека мнение и понять поведенческие последствия, которые приводят к этому разрыву».

Проблемы с отчетностью подрывают кибербезопасность

Согласно отчету, 34% людей лично стали жертвами кибербезопасности. Из этих людей 51% заявили, что они были жертвами более одного раза.Кроме того, 19% участников заявили, что стали жертвой кражи личных данных.Из тех, кто стал жертвой киберпреступности, 61% заявили, что не сообщали об инциденте.

Более того, только 22% участников заявили, что они «всегда» сообщали о попытках фишинга - одного из основных типов угроз, применяемых киберпреступниками. Интересно, что только 29% людей указали, что их не пугает кибербезопасность.

«Отрасль технологий полагается на отчетность как на один из ключевых столпов в выявлении и пресечении злоумышленников, но даже те, кто напрямую пострадал от киберпреступности, обычно не уведомляют соответствующие стороны о том, что инцидент произошел», - сказал Алаше.

«В повседневной жизни для людей - вторая натура - сообщать о преступлении, если они его видят; однако такое поведение не повторяется с киберпреступностью. Крайне важно, чтобы профессионалы в области кибербезопасности разобрались в причинах этого, поскольку повышение количества сообщений среди людей будет иметь решающее значение для высвобождения времени киберпрофессионалов, помогая им определять приоритеты угроз и корректировать свои стратегии».

Ограниченный доступ к кибертренингу

Согласно отчету, 64% респондентов не имеют доступа к обучению по кибербезопасности, в то время как 27% тех, у кого есть доступ, предпочитают не использовать его.

«Несмотря на продолжающийся рост невероятно изощренных атак кибербезопасности, подавляющее большинство работодателей и производителей

технологий не могут вооружить людей инструментами и знаниями, необходимыми для выявления, предотвращения и сообщения киберугроз», - сказал Плаггемьер.

«Успех в области кибербезопасности во многом зависит от действий обычных людей, и, если мы не сможем резко расширить нашу инфраструктуру обучения и образования, мы останемся чрезвычайно уязвимыми для злоумышленников».***(Cybersecurity best practices lagging, despite people being aware of the risks// Help Net Security (https://www.helpnetsecurity.com/2021/10/07/cybersecurity-best-practices-lagging/). 07.10.2021).***

***

«Разработка приложений - это творческий процесс, который также требует, чтобы кодировщики знали о проблемах безопасности. Обучение безопасному программированию имеет решающее значение, но то, как это обучение разрабатывается и проводится, может иметь огромное значение между обучением «ставя галочку» и обучением, которое дает результаты.

Ставки высоки. Компании, занимающиеся кибербезопасностью, и правоохранительные органы сообщают о 800%-ном всплеске кибератакс начала пандемии COVID-19. В то время как средняя стоимость взлома данных во всем мире составляет 4,24 миллиона долларов, средняя стоимость взлома в США составляет ошеломляющие 9,05 миллиона долларов. В 2020 году компаниям требовалось в среднем 280 дней на выявление и устранение утечки данных, что еще больше увеличивает общие затраты.

Согласно Forrester, веб-приложения были вектором атаки номер один. Уязвимости, связанные с внедрением, находятся на вершине рисков безопасности веб-приложений OWASP более 14 лет. Кроме того, все больше приложений требуют личных данных, и вводятся новые правила защиты этих данных.Учитывая, что затраты на исправление кода значительно выше, чем на создание кода в производственной среде, на разработчиков программного обеспечения оказывается огромная потребность в создании превосходного и безопасного кода. Тем не менее, только 20% вновь нанятых разработчиков прошли обучение безопасному программированию.

Разработчики сталкиваются с множеством проблем, в том числе с тем, как найти время для эффективного обучения пониманию и внедрению передовых практик. Опросы показывают, что половина разработчиков сообщают, что объем их кодовых баз за последние десять лет увеличился в 100 раз.Более 90% вынуждены развиваться быстрее. Действия, которые прерывают рабочий процесс, бесполезны в этой среде. Директор по информационным технологиям из списка One Fortune 500 сказал об этом так: «Разработчики рассматривают обучение безопасному программированию как налог на свою работу».Таким образом, когда проводится обучение безопасному программированию, разработчики должны рассматривать его как дополнительную ценность.

Форматы обучения имеют значение. Видеообучение недорогое и доступно в любое время, но может оказаться неэффективным. Как и любое видео, работающее в фоновом режиме, его можно легко проигнорировать. Он также не является

интерактивным, поэтому обучаемым не требуется демонстрировать понимание. Видеоуроки не адаптированы к потребностям конкретной компании. Точно так же онлайн-библиотеки или электронные книги не имеют интерактивности и руководства. Стажеры могут больше походить на браузеров, чем на учеников. Обычные практические онлайн-платформы доступны, но могут также не иметь возможности настройки для удовлетворения конкретных потребностей и вопросов разработчиков. Очное обучение может быть эффективным, но оно требует больших затрат времени и средств.Со временем в цене,

Контент тоже имеет значение. Эффективное обучение затрагивает как наступательные, так и защитные концепции. Стажеры должны научиться думать, как их противники, и уметь понимать, как их приложения могут быть атакованы.Обучение должно быть разделено на короткие, легко усваиваемые концепции, чтобы обучаемый мог выучить конкретный элемент за 20–30 минут. Обучение также должно быть контекстным, чтобы разработчики могли связать то, чему их учат, с работой, которую они делают каждый день.

Программы обучения безопасному программированию не созданы равными. Некоторые режимы обучения могут соответствовать стандартам соответствия регулирующим органам, но оставляют пробелы в понимании разработчиком того, как эффективно решать наиболее распространенные проблемы, которые могут привести к использованию уязвимостей в их коде. С увеличением числа кибератак, ростом затрат на утечку данных и значительными потерями времени при утечке данных недостаточно полагаться на трудоемкое обучение или обучение вне пределов досягаемости. Ключевым моментом является предоставление разработчикам настраиваемых интерактивных реальных сценариев, в которых они могут обучаться за расходуемые отрезки времени. То, как обучаются разработчики, может иметь значение между дорогостоящим взломом и безопасностью». ***(JARED ABLON. Now More Than Ever, Secure Coding Training Is Crucial for Web App Developers // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/now-more-than-ever-secure-coding-training-is-crucial-for-web-app-developers/). 18.10.2021).***

***

«Три главные цели большинства организаций - это безопасность, киберустойчивость и прибыльность. Фактически, в 2020 году McKinsey & Company отметила, что, когда организация объединяет свой бизнес в области киберустойчивости, в результате получается «более безопасное и прибыльное учреждение».Но как у предприятия могут быть наилучшие шансы на достижение этой ключевой тройки целей?

Ключевым моментом является то, что для истинной киберустойчивости требуется больше, чем просто обеспечение высокой доступности (HA), а также больше, чем просто обеспечение аварийного восстановления (DR).Оба необходимы, и именно здесь некоторые компании могут споткнуться, предполагая, что HA и DR - одно и то же. Это не так. Вкратце, это различие:

Высокая доступность означает непрерывную бесперебойную работу базы данных и связанных с ней сервисов, обеспечивающую безотказную работу до согласованного уровня обслуживания.

Аварийное восстановление означает, что организация может поддерживать или восстанавливать услуги после катастрофы или сбоя и восстанавливать свои данные и базы данных.

Слои проблем

Обеспечить высокую доступность и аварийное восстановление базы данных сложно, поскольку возникает множество проблем, связанных с отказоустойчивостью, безопасностью и масштабируемостью. Это верно для данных, хранящихся локально, а также в общедоступных облаках и удаленных хранилищах. Одна из проблем заключается в том, что компании должны обеспечивать отказоустойчивость баз данных не только между зонами доступности, но и внутри этих различных регионов. Проблемы безопасности, целостности и масштабируемости также являются частью головоломки, поскольку данные перемещаются между изолированными сетями и организациями, которым необходимо масштабировать несколько экземпляров базы данных, а не просто управлять ими.

Давайте рассмотрим проблему HA / DR, которая заключается в обеспечении удаленной защиты данных и надежном использовании всей мощности возможностей аварийного восстановления Microsoft SQL Server, а также локальной высокой доступности. Традиционно это серьезное препятствие заключалось в том, что при использовании SQL Server в Linux для обеспечения высокой доступности и аварийного восстановления компании сталкивались с выбором одного из двух неоптимальных вариантов. В одном из них использовалось решение на основе Pacemaker, для которого требовались виртуальные частные сети (VPN) для аварийного восстановления и отдельные кластеры для обеспечения высокой доступности. Другой требовал использования VPN для аварийного восстановления и последующего объединения экземпляров HA SQL Server с отдельным решением для репликации данных…

Существует более разумная альтернатива вышеупомянутому решению, ориентированному на VPN, и оно работает поверх программного обеспечения кластеризации SQL Server: Smart Availability, которое предлагает в три раза большую производительность SQL Server AG и повышает RPO с помощью микротоннелей. Его также легко реализовать, и он упрощает автоматическое сквозное управление отказом.

Этот тип решения обеспечивает необходимую предприятиям киберустойчивость за счет:

Стандартизированные HA и DR

Настройка одного кластера

Небольшое время простоя

Переносимость рабочей нагрузки

Вечнозеленая инфраструктура

Экономия затрат

Высокая рентабельность инвестиций

Это не единственные преимущества программного обеспечения кластеризации Smart Availability; он также предлагает защиту данных через безопасную сетевую связь на нескольких сайтах и в облаках, а также надежную сетевую безопасность за счет устранения боковой поверхности сетевых атак VPN.Это программное обеспечение дополнительно исключает репликацию серверов, что означает отсутствие необходимости использовать VPN, лицензии SQL Server и несколько технологий кластеризации.

Это правда, что другие системы управления корпоративными данными обеспечивают кластеризацию высокой доступности, но программное обеспечение Smart Availability гораздо более эффективно в облаке и между центрами обработки данных, предлагая возможности HA и DR для обеспечения киберустойчивости. Программное обеспечение очень эффективно работает с Microsoft SQL Server и помогает компаниям запускать HA, распределенные кластеры SQL Server в Linux, а также Windows. Устраняя как сложность, так и проблемы с производительностью традиционных решений VPN, кластеризации и репликации, программное обеспечение обеспечения доступности становится явным победителем». ***(DON BOXLEY JR. Cyber Resilience Paired with Business Functions Equals Greater Security // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/cyber-resilience-paired-with-business-functions-equals-greater-security/). 20.10.2021).***

***

«Последние полтора года подтолкнули предприятия и клиентов, которых они обслуживают, к радикальным изменениям в использовании технологий. Пандемия ускорила цифровую трансформацию 68% глобальных компаний, чтобы не отставать от потребителей, которые быстро переходили в Интернет. Теперь обслуживание клиентов стало еще удобнее, чем когда-либо, но доверие, которое получили бренды, ненадежно из-за возросших рисков кибербезопасности.

Несмотря на то, что быстрый переход на цифровые каналы сделал обслуживание клиентов более удобным, он также заставил компании управлять большим количеством технологических интеграций, большим количеством удаленных сотрудников, выполняющих вход с большего количества конечных точек, и большим количеством клиентов, совершающих покупки по-новому. Из-за этих изменений и других сбоев, связанных с пандемией, глобальные атаки программ-вымогателей увеличились на 62% с 2019 по 2020 год.

Программы-вымогатели не просто блокируют доступ жертв к их данным.Злоумышленники также могут украсть и продать данные, что приведет к краже личных данных, захвату учетных записей, финансовым потерям и юридическим осложнениям для клиентов. Такой ужасный опыт работы с клиентами может стоить бренду его доходов, репутации и способности продолжать свою деятельность. Примите во внимание, что 84% онлайн-покупателей в опросе ClearSale, проведенном в марте 2021 года в пяти странах, согласились с тем, что они больше не будут вести бизнес с веб-сайтом, который позволяет мошеннику использовать их карту.

Компании, которые инвестируют в свою кибербезопасность и постоянно обновляют ее, могут предотвратить перебои в работе с клиентами, защитить репутацию своего бренда и сохранить доверие и лояльность своих клиентов. Этот процесс включает в себя ключевые шаги по защите данных клиентов.

Уточните свои стратегии и методы сбора данных

Злоумышленники-вымогатели знают ценность данных клиентов, поэтому они так усердно работают, чтобы украсть их, и почему так много из них продается в темной сети. Чтобы защитить своих клиентов от раскрытия данных и защитить свой бизнес от ответственности, просмотрите собранные вами данные о клиентах.

Вы запрашиваете только ту информацию, которая вам нужна для их аутентификации и обеспечения хорошего опыта? Есть ли поля данных, которые вы могли бы прекратить собирать без ущерба для контроля за мошенничеством и CX? Если это так, вы можете прекратить запрашивать эти данные в дальнейшем и безопасно очистить существующие данные.

Что касается данных, которые вы должны собирать, это ваши разрешения, политики использования и хранения с соответствующими правилами защиты данных, такими как GDPR для клиентов из ЕС, CCPA для клиентов из Калифорнии, а также национальные и местные правила в других частях мира, где вы занимаетесь бизнесом? В противном случае приведение вашей практики в соответствие с требованиями защитит ваших клиентов и поможет вашей компании избежать дорогостоящих штрафов за несоблюдение в случае нарушения.

Пересмотрите свои методы шифрования

Данные клиентов, которые вы храните, должны быть зашифрованы, когда они вводят их на вашем веб-сайте или в приложении, а также когда данные хранятся на сервере. Это особенно важно, когда данные передаются на платежный шлюз, процессор, службу предотвращения мошенничества или другого надежного партнера.

Проверьте безопасность своего облачного хранилища, чтобы убедиться, что вы не храните данные клиентов в виде открытого текста на неправильно настроенных облачных серверах. Этот сценарий привел к взломам в последние годы в Facebook, Accenture, Verizon и других компаниях.

Также разумно посмотреть, как ваша организация отслеживает трафик на свои серверы и с них, чтобы предотвратить кражу данных.Мониторинг трафика данных может позволить вашей группе безопасности быстро отреагировать на неожиданное перемещение данных из вашей компании в неизвестный пункт назначения.

Держите программное обеспечение исправленным и обновленным

Рекомендация исправлений и обновлений может показаться самым основным советом по кибербезопасности, но крупные организации не решались на этот шаг еще до того, как пандемия заставила компании принимать больше программных решений. В 2019 году 60% нарушений были вызваны непропатченным программным обеспечением, и это были не эксплойты нулевого дня, а известные уязвимости, для которых были доступны исправления. Согласно опросу Ponemon Institute, среднее время исправления критических уязвимостей составляло 16 дней.

Исправления и обновления требуют баланса между безопасностью и накопителем, чтобы свести к минимуму сбои, а также время и персонал, необходимые для выполнения работы. Два подхода, которые могут помочь компаниям не отставать от требований к установке исправлений, - это автоматизация обновлений, когда это возможно, и выбор поставщиков программного обеспечения, которые доставляют обновления, не требуя действий со стороны вашей ИТ-группы.

Усильте защиту от вредоносных программ

Защита от вредоносных программ имеет решающее значение для предотвращения взломов. Убедитесь, что брандмауэры веб-приложений ваших сайтов соответствуют данным, и разверните непрерывное сканирование сайтов для обнаружения и удаления вредоносных программных кодов, которые могут привести к атакам со сбором данных, которые собирают информацию о клиентах, когда они вводят ее в формы оформления заказа.

Также по-новому взгляните на свою тактику защиты электронной почты. Хотя каждая компания должна продвигать культуру безопасности, все труднее отличить изощренные атаки с целью взлома электронной почты от реальных сообщений. Лучший превентивный подход - убедиться, что эти электронные письма никогда не достигают своих целей.

Изучите свой план реагирования на утечку данных

Если ваша компания нарушит правила, ваш ответ может определить степень ущерба, нанесенного вашим отношениям с клиентами, вашему бренду и репутации инвесторов, а также вашей финансовой ответственности. Как можно быстрее сообщайте о нарушениях в правоохранительные и соответствующие регулирующие органы. Отслеживайте изменения в законах, чтобы точно знать требования к отчетности для вашего бизнеса.

Открыто общайтесь со своими клиентами о том, что вы знаете и чего не знаете, и о шагах, которые вы предпринимаете для их защиты. Разработайте план до взлома, чтобы предлагать услуги мониторинга затронутым клиентам, и убедитесь, что CX работает отлично. Семьдесят восемь процентов клиентов говорят, что они «простят компании ее ошибку, получив отличное обслуживание».

Найдите время, чтобы оценить свою новую технологическую среду и предпринять шаги, чтобы сделать ее максимально безопасной. Доверие клиентов ценно, его трудно заработать и легко потерять. Лучший способ сохранить это сейчас - обеспечить безопасность данных ваших клиентов». ***(RAFAEL LOURENCO. Cybersecurity Improvements May Be the Best Customer Experience Tool You're Not Using // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/cybersecurity-improvements-may-be-the-best-customer-experience-tool-youre-not-using/). 14.10.2021).***

***

«Ежемесячный бюллетень Координационного центра кибербезопасности сектора здравоохранения (HC3) HHS информирует сектор здравоохранения о главных киберугрозах и уязвимостях в сфере здравоохранения, на которые следует обратить внимание. Группа сообщила, что уязвимости BrakTooth, группа

Conti Ransomware и вредоносное ПО Medusa / TangleBot по-прежнему представляют серьезную угрозу для организаций здравоохранения.

Семейство уязвимостей BrakTooth влияет на устройства с поддержкой Bluetooth и было впервые обнаружено ASSET Research Group в августе. Уязвимости позволяют злоумышленникам инициировать атаки типа «отказ в обслуживании» (DoS) на ноутбуки, смартфоны и другие устройства Bluetooth.

Предварительные результаты показали, что уязвимости BrakTooth могут повлиять на более 1400 списков продуктов. Уязвимость представляет собой серьезную угрозу для сектора здравоохранения из-за характера DoS-атак, которые могут привести к сбою прошивки устройства и отключению Bluetooth-соединения. HC3 рекомендовал медицинским организациям обратиться за помощью к организациям по обмену информацией и анализу (ISAO).

Программа-вымогатель Conti представляет собой известную угрозу в секторе здравоохранения. В феврале Conti опубликовал две свалки медицинских данных в темной сети и с тех пор совершил атаки на несколько медицинских учреждений и 400 кибератак в США и за рубежом. Агентство кибербезопасности и инфраструктуры (CISA), ФБР и Агентство национальной безопасности (NSA)выпустили консультативное предупреждение организациям о возможностях группы.

Вредоносные программы Medusa / TangleBot продолжают представлять угрозу и для медицинских организаций. Хакеры распространяют вредоносное ПО через SMS и, как известно, нацелены на пользователей Android, отправляя сообщения, связанные с COVID-19, с вредоносными ссылками. При нажатии ссылки развертывают вредоносное ПО и начинают сбор данных.Вредоносная программа может получить доступ к Интернету, GPS и журналам вызовов своей жертвы.

«Это вызывает беспокойство, если мобильное рабочее устройство кого-то из работников здравоохранения скомпрометировано, потому что после установки вредоносного ПО на устройство его может быть сложно обнаружить и удалить», - поясняется в бюллетене.

«В настоящее время предупреждающие сообщения от Android кажутся лучшим вариантом для защиты мобильных устройств от заражения. HC3 рекомендует информировать пользователей корпоративных устройств Android об этой угрозе и чтобы все переходили по ссылкам или загружали только заслуживающие доверия приложения (приложения) ».

HC3 также призвал отрасль здравоохранения усилить услуги виртуальных частных сетей (VPN), поскольку VPNS часто используются в качестве точек входа в защищенные сети. Сектор здравоохранения полагается на технологии VPN для телемедицины и доступа пациентов к медицинским картам.NSA и CISA выпустили совместный информационный лист, чтобы помочь организациям управлять рисками, связанными с VPN.

Кроме того, новая ошибка в реализации Active Directory в Microsoft Azure создает риски для отрасли здравоохранения, поскольку она позволяет выполнять однофакторный перебор экземпляра Active Directory без необходимости проверки подлинности. В настоящее время нет исправления для этой уязвимости.

«Ожидается, что эта уязвимость повлияет на сектор здравоохранения из-за того, что технология Microsoft Active Directory широко распространена и, как таковая, широко используется», - предупредил HC3.

«Природа этой уязвимости позволяет достичь компромисса с минимальной возможностью обнаружения, а отсутствие патча усложняет задачу, оставляя администраторов и защитников сети с минимальной видимостью действий злоумышленника».

HC3 выявила дополнительные уязвимости Microsoft, Adobe, Cisco, Apple и Google, некоторые из которых с тех пор были исправлены.Поскольку кибератаки продолжаются, как никогда важно, чтобы медицинские организации сохраняли бдительность в отношении основных киберугроз в этом секторе. ***(Jill McKeon. Top Healthcare Cyber Threats, Vulnerabilities to Watch For// TechTarget, Inc. (https://healthitsecurity.com/news/top-healthcare-cyber-threats-vulnerabilities-to-watch-for). 25.10.2021).***

***

…Высококлассный высокотехнологичный характер Формулы 1 делает ее привлекательной целью для киберпреступников и искушенных хакеров всех мастей.

«Профиль этой организации, популярность спорта и тот факт, что мы добились значительных успехов за последние несколько лет, на самом деле служат небольшой мишенью для этого вида деятельности», - объясняет Майкл Тейлор, ИТ-директор компании Mercedes-AMG Petronas Формула-1.

Большинство киберугроз, с которыми сталкивается команда F1, знакомы организациям по всему миру, например, фишинговые атаки, пытающиеся украсть имена пользователей, пароли и другую конфиденциальную информацию, или постоянная угроза программ-вымогателей. Но в Формуле 1 вы также должны учитывать проблему обеспечения удаленной рабочей силы, которая может быть в трех странах за столько же недель из-за напряженного графика в напряженном сезоне из 22 гонок.

А затем добавьте еще одну угрозу, исходящую от самых изощренных сетевых злоумышленников, которые могут интересоваться секретами высокопроизводительной гоночной команды.

«В этом гибридном мире большая часть технологий исходит из Формулы-1, а затем проникает в автомобили, на которых мы ездим, поэтому существует огромное количество новейших технологий, которые, очевидно, нуждаются в защите и, безусловно, могут быть цель для субъектов национального государства», - говорит Джордж Курц, генеральный директор CrowdStrike, партнера Mercedes по кибербезопасности, который предоставляет команде технологии, помогающие защитить свои сети, а также информацию о меняющемся характере киберугроз.

Сюда входит досье перед каждым гоночным уик-эндом, в котором аналитики безопасности CrowdStrike подробно описывают потенциальные киберугрозы, с которыми члены команды могут столкнуться в стране, где расположена гоночная трасса, и способы защиты от этих угроз.

«Это всегда сенсация, которая всегда помогает поднять некоторые неудобные истины и некоторые вопросы», - говорит Тейлор.

Обеспечение того, чтобы кибербезопасность команды Формулы 1 была достаточно сильной для защиты от всех этих угроз, начинается с защиты конечных точек - ноутбуков, планшетов и других устройств, которые сотрудники используют ежедневно.

«Конечные точки для нас - это наша самая большая зона риска, потому что на другом конце у них есть человек, и большая часть риска по своей природе принадлежит людям, которые делают то, что они, вероятно, не должны делать или не собирались делать намеренно», - Тейлор объясняет.

«Конечная точка - это область, над которой у нас есть контроль, но не полный контроль, и это действительно самая главная цель для нас с точки зрения снижения вероятности риска».

Mercedes может полностью заблокировать машины со строгим контролем над тем, какие действия могут выполнять пользователи; но ограничение активности пользователей, как это было в Формуле 1, где время имеет существенное значение, а стратегические решения за доли секунды и данные, которые их информируют, могут сделать или прервать гоночный уик-энд, может поставить команду в невыгодное положение.

«Мы очень креативны с точки зрения решения проблем и проектирования, и исторические меры безопасности могут сдерживать инновации или потенциально могут ограничивать инновации», - говорит Тейлор.

Это означает, что жесткое ограничение доступа к данным или затруднение работы инженеров на пит-лейн с аналитиками на заводе - это не выход. Вместо этого необходим баланс между обеспечением безопасности, а также обеспечением того, чтобы персонал мог эффективно выполнять свою работу, не причиняя вреда Льюису Хэмилтону или его товарищу по команде Валттери Боттасу во время гоночных уик-эндов.

«Это всегда баланс риска и вознаграждения, и он пытается предоставить эту гибкую платформу, позволяющую сотрудничать, но при этом понимая потенциальные риски и затем устраняя их», - говорит Тейлор.

Приложения кибербезопасности, такие как межсетевые экраны, сегментация сети, предоставление доступа к данным на основе служебной необходимости и многофакторная аутентификация, играют роль в обеспечении безопасности команды, но глобальный характер Формулы 1 означает, что персонал: и компьютерные сети - не оставайтесь на одном месте надолго, пока вас не унесут и не перенесут на другую трассу в календаре.

Вот почему многие приложения, которые помогают управлять процедурами безопасности, являются облачными, что позволяет Mercedes обеспечивать защиту конечных точек от новейших угроз, независимо от того, где они находятся.

«Независимо от того, на заводе ли мы относимся к нашей защитной среде, или в Австралии, это по-прежнему та же постоянная защита конечных точек, что и у нас; тот факт, что она вызывает дом в облачном местоположении где-нибудь в мире, значительно упрощает сложность и проблему для нас в организационном плане», - объясняет Тейлор.

Все десять команд Формулы 1 сталкиваются с одинаковыми проблемами, связанными с защитой своих сетей от утечки данных и кибератак, независимо от того, где они находятся, и при этом стараются работать максимально эффективно в быстро меняющейся среде.

Киберпреступники уже давно эксплуатируемые лихорадочный характер бизнеса, а также огромное число писем, которые присылают в день в качестве отправной точки для кибер -атака- и это ничем не отличается для Формулы -1.

Например, в ноябре прошлого года Формула 1 была в Имоле на Гран-при Эмилии-Романьи, 13-й гонке в сезоне чемпионата мира Формулы-1 2020 года. Это было в конце года для гонки F1, после того, как начало сезона было отложено с марта на июль из-за воздействия пандемии COVID-19, и гонки были интенсивнымии быстрыми во время укороченного календаря; Всего за несколько дней до этого команды были в Португалии на предыдущем Гран-при.

Именно в этот момент некоторые хакеры сразу же отправились за большим призом, пытаясь атаковать Зака Брауна, генерального директора гоночной команды McLaren Formula 1.

Они создали изощренное фишинговое письмо, похожее на деловые письма, которые Браун ожидал бы получить. Но Браун так и не увидел этого, потому что защита кибербезопасности, которую McLaren применяет к почтовым ящикам всех своих сотрудников, означала, что он сразу перешел к нежелательной почте, а возможность щелкнуть ссылку была отключена - несмотря на продолжающиеся усилия злоумышленников.

«Что касается объема атак, они определенно стали умнее. Они нацелены на людей с помощью фишинговых и целевых фишинговых атак» - это очень целенаправленно, очень умно, - говорит Крис Хикс, ИТ-директор группы McLaren Group. «Это игра в кошки-мышки; злоумышленники будут реагировать на ваши изменения, а затем мы реагируем по очереди - но я чувствую, что мы всегда на шаг впереди».

McLaren отразил эту конкретную атаку, используя технологию, предоставленную Darktrace, официальным партнером команды по кибербезопасности - ее логотип заметно выделялся на ливре автомобилей, которыми управляют Ландо Норрис и Даниэль Риккардо.

Природа Формулы 1, в которой члены команды могут находиться в разных частях мира в течение нескольких недель подряд, означает, что блокировка доступа к электронной почте только потому, что они отправляются с IP-адреса в незнакомом месте, не сработает.

Но программное обеспечение безопасности электронной почты McLaren анализирует информацию о предыдущей активности и использует ее, чтобы определить, является ли действие законным, а это означает, что важные сообщения, доставленные из незнакомых часовых поясов или мест, не блокируются. Между тем, сообщения, подобные тому, которое киберпреступники пытались отправить генеральному директору McLaren, отфильтровываются, поскольку они признаются необычными или вредоносными…

«Доступность данных в реальном времени и совместная работа в реальном времени, где бы вы ни находились, абсолютно критически важны - любой в Формуле 1 скажет вам, что каждая миллисекунда на счету», - добавляет он.

Огромный объем данных, передаваемых в течение гоночного уик-энда, потенциально составляет сотни тысяч электронных писем, отправляемых внутри McLaren, а также между McLaren и его партнерами.

«В гоночный уик-энд можно измерить, сколько еще атак приходит на бизнес, когда по телевизору показывают « Формулу-1», - говорит Дэйв Палмер, директор по продуктам Darktrace.

«За гоночную неделю может быть 250 000 писем, а во время гоночных выходных количество злонамеренных писем возрастает примерно до 3,5%, что очень много - в 3,5% входящей электронной почты что-то не так, с этим нужно действовать. на машине ".

Если хотя бы одно вредоносное фишинговое письмо не будет идентифицировано и получено, это может иметь разрушительные последствия - это может не только повлиять на планы гонки, но также есть вероятность того, что фишинговое письмо будет использовано в качестве шлюза для более широкой атаки на сеть.

«Это то, с чем мы всегда сталкивались, потому что во многих областях интеллектуальная собственность не будет секретной очень долго - примерно через шесть месяцев она станет достоянием общественности, просто из-за характера Формулы 1. Но в реальном времени мы мы хотим держать его при себе, и часто это делается из-за финансовой выгоды или по разным причинам, по которым злоумышленники могут попытаться скомпрометировать нас, поэтому крайне важно, чтобы мы защищали этот IP-адрес », - говорит Хикс из McLaren.

McLaren не просто полагается на технологии для обеспечения безопасности персонала - ключевым элементом защиты сети от кибератак является регулярное обучение персонала, включая руководителей, по вопросам кибербезопасности.

«Информационные кампании, которые мы проводим, абсолютно важны, и обычно они идут сверху вниз. Обычно в первую очередь вы ориентируетесь на генеральных директоров или их помощников; люди наверху», - говорит Хикс.

Williams Racing - одна из самых успешных команд в сетке Формулы 1, и она тоже оказалась объектом кибератак, пытающихся запустить фишинговые атаки на зал заседаний.

Высококлассный характер Формулы 1 означает, что легко узнать, кто управляет командами - они часто прямо здесь, по телевизору, - и киберпреступники попытаются использовать это для социальной инженерии.

«Мы знаем, что постоянно являемся мишенью, есть даже несколько целевых фишинговых атак, направленных на преследование генерального или финансового директора», - говорит Грэм Хакленд, ИТ-директор Williams Racing F1.

«Они не блокируют вам доступ к вашей учетной записи, они просто сидят в вашей учетной записи и наблюдают. Мы получили ответ на электронное письмо от поставщика, в котором говорилось: «Мы изменили наш банковский счет, вы можете обновить свои записи »- и этот ответ был отправлен хакером, а не поставщиком », - поясняет Хакленд.

Злоумышленники также зарегистрировали ложные адреса электронной почты Williams, пытаясь совершить атаки против команды - например, они попытаются зарегистрировать URL-адрес, в котором строчные l заменены на заглавную L, что, если только кто-то действительно не проверяет адрес электронной почты., выглядело бы аутентично.

«Он выглядит так же, как наш адрес электронной почты, и поэтому я не виню никого из наших сотрудников, попавших в ловушку этих вещей, потому что это было очень, очень изощренно - теперь в фишинговых письмах гораздо больше социальной инженерии. Они изучают огромное количество информации», - говорит Хакленд.

Уильямс был продан новым владельцам, американской частной инвестиционной компании Dorilton Capital, в течение 2020 года - и с новыми руководителями и новым персоналом вокруг них было жизненно важно, чтобы эти люди знали о потенциальных угрозах безопасности, с которыми они столкнутся как высокопоставленные сотрудники. команда Формулы 1.

«У нас появился новый генеральный директор, поэтому мы провели образовательную кампанию с его личным помощником, чтобы напомнить ей, что она станет целью, и мы действительно наблюдаем рост количества спам-писем, отправляемых ей», - объясняет Хакленд.Все сотрудники Williams проходя то бучение фишингу, чтобы понять, как киберпреступники могут попытаться проникнуть в сеть через электронную почту.

Но огромное количество кибератак означает, что не всегда удавалось защитить сеть от атак – и несколько лет назад Уильямс оказался жертвой атаки вымогателя.

Атака в 2014 году началась в пятницу утром и была быстро обнаружена командой кибербезопасности. Большая часть сети была защищена от атаки. Но если бы атака началась несколькими часами позже, вероятно, никто бы этого не заметил до следующей недели.

«Если бы это произошло в 18:00, он мог бы потратить все выходные на шифрование всех наших данных, а когда мы придем в понедельник, у нас были бы огромные проблемы. Это было удачно, это было утро пятницы, и мы заметили такое поведение довольно неплохо. в самом начале процесса», - объясняет Хакленд.

Атака программы-вымогателя попала в сеть после того, как сотрудник случайно посетил взломанный веб-сайт.

«Они загрузили технические спецификации для своей стиральной машины. Они не сделали ничего плохого. Они пошли на проверенный веб-сайт, загрузили файл и не подозревали, что эта программа-вымогатель работает в фоновом режиме», - говорит Хакленд.

Во время инцидента в 2014 году процедуры кибербезопасности не были такими зрелыми, как сегодня, и в этом случае затронутые файлы не могли быть восстановлены. Но это послужило тревожным сигналом для обеспечения максимальной защиты сетей и сотрудников от кибератак.

Теперь Williams Racing извлекла выгоду из партнерства с компанией Acronis, занимающейся кибербезопасностью, в течение нескольких лет, помогая

обеспечивать безопасность конечных точек и персонала, а также водителей Джорджа Рассела и Николаса Латифи, независимо от того, находятся ли они в штаб-квартире в Гроуве, Оксфордшир, или в гоночные трассы по всему миру.

Партнерство означает, что Williams использует Acronis для защиты конечных точек, а также резервного копирования для обеспечения безопасности данных, независимо от того, где находится пользователь, работает ли он удаленно, на заводе или на гоночной трассе.

«Команды автоспорта, даже находящиеся на вершине отрасли, сталкиваются с серьезными проблемами, связанными с постоянно растущими объемами данных - управлением, архивированием, совместным использованием и защитой от кибератак», - говорит Ронан МакКуртин, вице-президент по Европе, Турции и Израилю. Acronis.

Благодаря большему количеству гонок, чем когда-либо прежде, команды Формулы 1 работают на пределе возможностей как на трассе, так и за ее пределами. Высокий уровень спорта и передовые технологии, лежащие в его основе, означают, что все команды Формулы 1 являются соблазнительной мишенью для киберпреступников и хакеров.

К сожалению, как и команды Формулы 1, за которыми они гонятся, злоумышленники всегда ищут способы улучшить свою работу. Но, в отличие от гонки F1, в гонке кибервооружений нет финиша». ***(Danny Palmer. This is how Formula 1 teams fight off cyberattacks // ZDNet (https://www.zdnet.com/article/this-is-how-formula-1-teams-fight-off-cyberattacks/). 14.10.2021).***

***

«…два Положения, принятые ЕЭК ООН (органом Организации Объединенных Наций) по кибербезопасности и обновлениям программного обеспечения в автомобильном секторе, могут повлиять на ваши продукты и услуги, даже если ваш сектор совершенно другой.

Эти правила содержат уроки, не зависящие от сектора, о том, как подходить к требованиям информационной безопасности в правилах защиты данных и аналогичном законодательстве, и могут стать основой для новых законов о кибербезопасности в будущем.

Вот некоторые выводы, от понимания необходимости и объема системы управления кибербезопасностью до подробных списков угроз и мер по их смягчению. И что может быть лучше для того, чтобы включить их в повестку дня вашей организации, чем Европейский месяц кибербезопасности (и даже Неделя кибербезопасности в Люксембурге)?

Какие правила?

Эти правила исходят от Всемирного форума для согласования правил в области транспортных средств, WP.29 (не путать с WP29 по защите данных, Рабочей группой по статье 29).WP.29 является частью ЕЭК ООН, Европейской экономической комиссии Организации Объединенных Наций (члены которой находятся далеко за пределами Европы), и он определяет различные требования, которым должны соответствовать транспортные средства, оборудование и детали.

Поскольку автомобили превратились в компьютеры на колесах, кибербезопасность стала ключевой проблемой, с множеством примеров взлома автомобилей на протяжении многих лет (от убийства джипа на шоссе до кражи даже недавних автомобилей Tesla), а на ежегодной конференции хакеров DEF CON Car Hacking Village с 2015 года.

Помимо необходимости устранения уязвимостей, эти компьютеры на колесах должны развиваться постепенно, с новыми или усовершенствованными функциями и исправлениями ошибок.

Это привело к созданию двух правил ЕЭК ООН:

Правило 155(Система управления кибербезопасностью и кибербезопасностью) с требованиями, касающимися системы управления кибербезопасностью («CSMS»), которая должна быть введена в действие несколькими видами производителей транспортных средств, и

Правило 156(Система обновления программного обеспечения и управления обновлениями программного обеспечения) с требованиями, касающимися разработки, выпуска и обслуживания обновлений программного обеспечения для еще более широкого диапазона транспортных средств.

Целевая группа, работающая над Правилом 155, в частности, частично совпадала с отраслевой командой, работающей над ISO / SAE 21434: 2021. Таким образом, этот стандарт по обеспечению кибербезопасности дорожных транспортных средств может служить хорошим справочным материалом для обеспечения технического соответствия, что подтверждается в документе отолковании правил 155, одобренном WP.29.

Требования Правила 155 станут обязательными для новых типов транспортных средств с июля 2022 года как в Европейском союзе, так и в Японии, в результате чего многие проекты соответствия все еще продолжаются (если они начаты). Так что, если ваша компания работает в этом секторе, возможно, еще не поздно начать, но уже давно пора.

Уроки из правила 155 (кибербезопасность)

Правило 155 содержит много соображений, которые могут быть полезны при рассмотрении соблюдения других требований законодательства с точки зрения информационной безопасности. Во-первых, он определяет CSMS как «систематический подход, основанный на оценке рисков, определяющий организационные процессы, обязанности и управление для обработки рисков, связанных с киберугрозами для транспортных средств, и защиты их от кибератак». Замените «транспортные средства» на «активы», «личные данные» или «информацию», и система CSMS должна стать краеугольным камнем подхода вашей компании к кибербезопасности. Правило 155 делает CSMS центральным элементом соответствия: без CSMS производитель транспортных средств не может получить специальный сертификат, что, в свою очередь, означает, что он не может размещать свою продукцию на рынке. Та же идея присутствует в зачаточной форме в Директиве NIS (Network & Information Security) и ее национальных реализациях,

Урок: наличие хорошего подхода к кибербезопасности может иметь решающее значение для качества продуктов или услуг, а иногда даже для правильного размещения их на рынке. Компании должны разработать глобальную

стратегию кибербезопасности и задокументировать ее. Наша статья о том, как объяснить правовые аспекты кибербезопасности Совету директоров, может вам пригодиться.

Далее, просто иметь CSMS в какой-то момент времени недостаточно - производитель транспортного средства должен продемонстрировать разрешающему органу, что CSMS применяется к трем этапам жизненного цикла транспортного средства: разработка, производство и постпроизводство (т.е. Между окончанием производства и по окончании срока службы). Кроме того, сертификаты соответствия CSMS действительны не более трех лет, и перед продлением требуется новая оценка. Так же, как защита данных должна приниматься во внимание от этапа проектирования до конца обработки, кибербезопасность - это непрерывный процесс, требующий проверки.

Урок: убедитесь, что подход вашей компании к кибербезопасности применяется ко всему жизненному циклу продукта или услуги, и что существуют процессы, позволяющие(пере) оценивать общий уровень риска, а также конкретные угрозы даже после конкретного продукта или услуги. перестает предоставляться. Учитывая, что новые нормативные требования могут повлиять на уровень риска, юристы (штатные или внешние) также должны участвовать в таких проверках.

В Правиле 155 требования CSMS применяются к производителю транспортных средств, а не непосредственно к его поставщикам, но производители транспортных средств должны «продемонстрировать, как их [CSMS] будет управлять зависимостями, которые могут существовать с поставщиками по контракту, поставщиками услуг или под организациями производителя», и должны «выявлять и управлять рисками, связанными с поставщиком для одобренного типа транспортного средства».Это правило немного более детально, чем обязательство «должной осмотрительности», содержащееся в ст.28 (1) GDPR в отношении выбора обработчиков, но общий принцип аналогичен: принципал часто может нести ответственность за действия поставщика услуг. Это приводит к наложению обязательств по обеспечению безопасности на поставщиков посредством контракта.

Урок: даже если ваша компания не участвует в создании определенного компонента или предоставлении определенной услуги, она должна проверить (в разумных пределах), что ее поставщик или субподрядчик действует ответственно в отношении информационной безопасности. Включите такие проверки в процесс адаптации поставщика или рассмотрите сценарий переговоров по контракту.

Также существуют требования по выявлению и снижению рисков. CSMS должна охватывать, в частности, процессы выявления рисков, с32 примерами угроз, перечисленных в приложении к Правилу 155, и должны быть процессы для оценки, категоризации и управления этими рисками, а также для «обеспечения того, чтобы оценка рисков оставалась актуальной». Кроме того, в Правиле 155 перечислено около 70 примеров смягчающих мер., каждая из которых связана с определенной угрозой. Эти подробные списки угроз и мер по их снижению резко контрастируют с глобальным требованием большинства других законов иметь «соответствующие технические и организационные меры для обеспечения уровня

безопасности, соответствующего риску» (как в ст. 32 GDPR, но см. Также ст. 14 Директива NIS, статья 95 PSD2, статья 4 Директивы о конфиденциальности и т. Д.).

Урок: убедитесь, что соблюдение требований к кибербезопасности не остается на усмотрение ИТ - решающее значение имеет междисциплинарный подход (юридический, ИТ, бизнес, коммуникация и т. Д.), Чтобы обеспечить выявление как можно большего количества рисков и мер по их снижению, а в случае мер по смягчению - положи на место. Детальный подход в Правиле 155 сегодня необычен, но может быть планом для завтрашних законов, и эти списки должны служить источником вдохновения для внутреннего выявления рисков и усилий по их снижению.

Что касается реагирования на инциденты и уязвимости, Правило 155 сначала выглядит менее строгим, чем правила защиты данных в отношении утечек личных данных или другие правила в отношении инцидентов безопасности. Например, что касается сроков, это требует устранения угроз и уязвимостей «в разумные сроки». Однако власти, вероятно, будут использовать подробный список угроз и связанных с ними мер по смягчению при оценке качества и эффективности усилий производителя по реагированию на инциденты: если возникает одна из перечисленных угроз и предлагаемая мера по смягчению не реализована, она, вероятно, будет использована против производителя.

Урок: после подготовки оценки рисков с идентификацией как угроз, так и мер по смягчению, убедитесь, что согласованность с планом реагирования на инциденты, чтобы компания могла показать, что ее оценка рисков является хорошей отправной точкой. При необходимости убедитесь, что любые недостатки в оценке рисков, обнаруженные во время инцидента, используются как возможность для улучшения. Кроме того, в случае инцидента убедитесь, что запущенные процессы должным образом соблюдаются, чтобы ограничить правовой риск, который может возникнуть в результате самого реагирования.

Уроки из правила 156 (обновления программного обеспечения)

Правило 156 касается обновлений программного обеспечения в целом, но менее детально, чем Правило 155.

Он требует от производителей наличия различных процессов и документации, в частности, в отношении влияния обновлений на (i) безопасную эксплуатацию транспортного средства (т.е. продукта) и (ii) рыночные утверждения, необходимость уведомлений для пользователей относительно обновлений по их запросу и, наконец, безопасность процесса развертывания обновлений. Некоторые из них могут быть очень важны, если ваша компания предоставляет программное обеспечение для внутренних или внешних заказчиков, независимо от сектора.

По первому пункту Правило 156 по существу требует, чтобы производители определяли влияние обновления программного обеспечения до его развертывания. Например, если обновление изменяет систему транспортного средства, оно может повлиять на разрешение, предоставленное в отношении этой системы; Аналогичным образом, если обновление затрагивает любую другую систему, необходимую для безопасной и непрерывной работы транспортного средства, для производителя крайне важно принять это решение до того, как обновление будет развернуто.Более того, как указано ниже, пользователи должны быть

проинформированы об изменениях, поэтому определение влияния также помогает обеспечить прозрачность.

Урок: встроите оценки в процесс обновления, так как даже в других секторах неспособность предвидеть влияние обновления может облегчить иски о возмещении ущерба, относящегося к прямым последствиям обновления.

Что касается уведомлений об обновлении программного обеспечения, Правило 156 гласит, что должен существовать процесс, «посредством которого пользователь транспортного средства может быть проинформирован об обновлениях», и что эта информация должна включать (a) цель обновления, (б) любые изменения, реализованные обновление функций [транспортного средства], (c) ожидаемое время завершения выполнения обновления (другими словами: время установки), (d) любые функции [транспортного средства],которые могут быть недоступны во время выполнения обновления и (e) любые инструкции, которые могут помочь пользователю [транспортного средства] безопасно выполнить обновление.

Урок: прозрачность- ключ к успеху. Операционные группы должны обращать внимание на необходимость управлять ожиданиями пользователей и избегать ситуаций, которые могут привести к жалобе или ответственности, и прозрачность может здесь сильно помочь.

Наконец, Правило 156 требует, чтобы производители обеспечивали безопасность процессов обновления (i) для (разумного) предотвращения манипуляций до начала процесса обновления и (ii) (разумно) предотвращения их компрометации, включая разработку системы доставки обновлений. Кроме того, крайне важно обеспечить, чтобы «[t] оные процессы, используемые для проверки и подтверждения функциональности программного обеспечения, и код программного обеспечения, используемого в транспортном средстве, были подходящими». Другими словами, злоумышленники не должны участвовать в процессе разработки и развертывания обновлений программного обеспечения.

Урок: безопасность конкретного программного пакета - это еще не все, безопасность механизма обновления не менее важна. Некорректная защита обновлений может иметь серьезные юридические последствия, поэтому убедитесь, что процессы защищены от таких рисков.

В целом, Правило 156 имеет меньшее значение для отдельных секторов, но оно показывает моменты внимания, которые могут появиться в будущем законодательстве или даже в прецедентном праве, касающемся ответственности.

Общий урок? Поскольку законы становятся все более техническими, диалог между юридическими и техническими группами больше не является просто передовой практикой; это становится необходимостью. Если они не говорят на одном языке, обязательно обратитесь за помощью!» ***(Why all companies should care about the UN's cybersecurity & software update regulations – lessons for all sectors // Nauta Dutilh (https://www.e-nautadutilh.com/95/4612/landing-pages/why-all-companies-should-care-about-the-un-s-cybersecurity-and-software-update-regulations---lessons-for-all-sectors.asp?sid=7862f755-9271-49cd-91b0-a0dbcc646545). 26.10.2021).***

***

«Кибербезопасность - главная забота организаций всех форм и размеров. Будь то глобальная организация или малый бизнес, каждая из них неизбежно будет собирать и хранить данные о потребителях, которые хакеры могут попытаться украсть. Хотя важные события, такие как запуск продуктов, слияния и поглощения, а также новые партнерские отношения с поставщиками, являются основными возможностями для атак, риск все еще существует в повседневной деятельности. Подумайте о данных, хранящихся в отделах кадров для потенциальных, прошлых и нынешних сотрудников. Или другие данные, относящиеся к повседневным операциям для многих предприятий, такие как GPS-слежение, информация о медицинских пациентах и финансовые транзакции. Дело в том, что каждая организация ежедневно взаимодействует с данными и, вероятно, использует электронную систему для хранения этой информации. Из-за этого, кибербезопасности или наймите штатного юриста, практикующего в этой области. Отношения можно масштабировать в соответствии с размером организации и конкретными потребностями в безопасности, чтобы оставаться в рамках бюджета, при этом улучшая методы обеспечения безопасности для защиты конфиденциальных данных.

Вот несколько важных причин, по которым каждой организации следует подумать о найме кибер-поверенного:

Конфиденциальность между адвокатом и клиентом. Основой взаимоотношений организации с адвокатами любого типа является доверие - как в отношении содержания рекомендаций, так и гарантий конфиденциальности. При решении вопросов кибербезопасности возможность воспользоваться юридической экспертизой дает несколько преимуществ. Во-первых, в случае нарушения консультация по быстрому набору очень поможет смягчить последствия. Это позволяет организации быстро собирать советы об обязательствах по уведомлению и других нормативных требованиях. Проактивность и установление этих взаимоотношений до инцидента оптимизирует усилия по устранению последствий и ограничит риск выпадений, поскольку протоколы реагирования уже будут определены и протестированы. Скорее всего, ваш советник по кибербезопасности нанял технических экспертов для помощи в таких вопросах, как реализация программы безопасности и реагирование на нарушения. Это означает, что не только совет вашего поверенного будет конфиденциальным, но также есть аргумент, что любые директивы стороннего технического эксперта также могут быть скрыты под этой привилегией. В случае судебного разбирательства, возникшего в результате инцидента, это основная защита.

Хотя организация может захотеть заявить о своих правах для защиты или уменьшения ответственности, рассмотрение с другой точки зрения раскрытие информации может быть полезным во время судебных разбирательств или нормативной проверки. Прозрачность в отношении процедур безопасности и развернутых обновлений может помочь продемонстрировать соответствие, и любой технический консультант, которого использовал поверенный, может свидетельствовать, чтобы продемонстрировать, что организация использует стандартные отраслевые практики.

Расширенные юридические знания и отраслевые связи: большинство кибер-поверенных обладают разнообразным опытом и навыками в таких областях, как судебные разбирательства, реагирование на инциденты, управление технологиями и их внедрение, бизнес-операции, внутренняя оценка рисков и рисков поставщиков, контракты, слияния, страхование., конфиденциальность и правительство. При выборе кибер-поверенного важно учитывать его опыт и расставлять приоритеты, какие навыки будут наиболее полезны для достижения ваших целей. Например, организация, сталкивающаяся с регулирующими расследованиями, могла бы получить пользу от адвоката, обладающего знаниями в области государственного управления, слияний и / или конфиденциальности. Если целью является создание комплексной программы реагирования на инциденты, ценные навыки будут включать оценку рисков, планирование реагирования на инциденты и / или управление технологиями. В целом, внедрение надежных методов обеспечения безопасности будет способствовать соблюдению нормативных требований и уменьшать риски, связанные с кибератаками.

Кроме того, кибер-поверенный также внесут свой вклад в общение, что будет полезно для организации. Это включает в себя связи с регулирующими органами, агентствами, экспертами по технологиям, поставщиками и т. Д.Возможность использовать эти ресурсы будет полезна при принятии решений по безопасности, таких как переговоры по соглашению о технологии или поставщиках, создание внутренних структур соответствия или формулировка плана готовности к судебным разбирательствам. Кибер-поверенный также может предложить определенный уровень объективности, чтобы предоставить беспристрастную оценку методов обеспечения безопасности или реагирования на инциденты в организации.

Наличие последовательного консультанта по вопросам кибербезопасности - будь то на месте или со сторонним консультантом - поможет гарантировать, что инфраструктура, политики и методы организации способствуют защите данных. Это важный этап до инцидента на этапе планирования и после этапа реагирования на инцидент для борьбы с угрозами и ускорения усилий по устранению последствий. Некоторые небольшие области, на которые следует обратить внимание на начальном этапе, включают политику конфиденциальности веб-сайтов, тестирование на проникновение, отображение данных, оценку соответствия и обучение сотрудников. При консультировании со сторонним юристом важно четко сформулировать, почему организация хочет привлечь их, и обсудить преимущества установления постоянных отношений.

Немного важной информации. Краткое описание включает в себя организационную структуру, источники конфиденциальных данных, текущие практики и политики безопасности, партнерские отношения с поставщиками, данные прошлых проверок безопасности (если таковые были), нормативные обязательства, договорные обязательства и методологию оценки рисков. Затем можно поговорить о том, где существуют пробелы и как их закрыть. Роль кибер-поверенного при желании может быть постоянной, не только для помощи в таких вещах, как реагирование на нарушения или нормативные расследования, но и для постоянного информирования о киберрисках по мере появления новых технологий

или угроз с годами…» ***(Why no Organization Should be without a Cyber Attorney // Epiq. (https://www.epiqglobal.com/en-us/resource-center/articles/no-organization-should-be-without-cyber-attorney). 20.10.2021).***

***

«Октябрь - месяц осведомленности о кибербезопасности - глобальная инициатива, направленная на повышение осведомленности об опасностях киберпреступности и привлечение внимания к решениям, которые могут помочь каждому защитить свои данные.

Ожидается, что к концу 2021 года стоимость киберпреступностиво всем мире достигнет 6 триллионов долларов. К 2025 году эта цифра, по прогнозам, составит 10,5 трлн долларов. Пандемия COVID-19 и последующий переход к удаленной работе повысили уязвимость миллионов людей и организаций перед кибератаками.

Тема этого месяца - «Сделай свой вклад», #BeCyberSmart. Целью этой кампании является обеспечение безопасности в Интернете и обучение сотрудников, клиентов и пользователей вопросам конфиденциальности в Интернете. Центральные темы и темы в центре внимания в этом году включают:

Понимание и внедрение основных мер кибербезопасности, которые слишком часто игнорируются, несмотря на то, что они оказывают существенное влияние на киберзащиту, включая замену трудно запоминаемых паролей надежными парольными фразами, использование многофакторной аутентификации и современных методов аутентификации, выполнение обновлений программного обеспечения и резервное копирование данных.

Распознавание попытки фишинга, исходящей из электронной почты, текстовых сообщений или чатов

Практика безопасного поведения в Интернете, безопасного просмотра и избегания опасных сайтов

Расстановка приоритетов и разработка стратегии кибербезопасности в бизнес-среде, особенно когда речь идет о конфиденциальной информации о клиентах.

BIO-key International Inc. (NASDAQ: BKYI)- провайдер управления идентификацией и доступом (IAM) со встроенной биометрией спривязкой к идентификационной информации, который стремится помочь отдельным лицам, предприятиям и крупным организациям внедрить простые инструменты кибербезопасности.

Как ведущий поставщик IAM, BIO-key предлагает решения, позволяющие защитить и подтвердить свою личность при получении доступа к цифровым приложениям, данным и устройствам.

Уникальная платформа BIO-key, PortalGuard, предлагает широкий спектр гибких опций, включая более 16 методов многофакторной аутентификации, самостоятельный сброс пароля, единый вход, биометрические данные и даже индивидуальные решения. Каждое решение предназначено для обеспечения беспрепятственного взаимодействия с пользователем и обеспечения первоклассной безопасности. PortalGuard - единственная платформа IAM, предлагающая биометрию с привязкой к идентификатору, которая является единственным

фактором, который действительно подтверждает личность человека и того, кто стоит за транзакцией, а не только его устройство или токен…» ***(Jacinta Sherris. What to Know About Digital Protection this Cybersecurity Awareness Month // benzinga (https://www.benzinga.com/markets/penny-stocks/21/10/23550749/what-to-know-about-digital-protection-this-cybersecurity-awareness-month?utm_campaign=partner_feed&utm_source=SmartNews&utm_medium=partner_feed&utm_content=site). 26.10.2021).***

***

«Многие люди не понимают, что степень гуманитарных наук открывает двери для самых разных профессий. Это включает карьеру в сфере кибербезопасности. А с учетом нехватки навыков и количества доступных рабочих мест явно есть спрос. Кто-то должен подойти, чтобы заполнить эти рабочие места. Итак, почему бы не тому, кто имеет большой опыт в так называемых soft skills?

Навыки кибербезопасности за пределами высоких технологий

Конечно, работа в сфере кибербезопасности требует технических навыков. Возможно, вам потребуется знать, как кодировать на разных языках, как создавать сетевые архитектуры, понимать аналитику и так далее. Также в верхней части списка находятся такие навыки, как решение проблем, общение, внимание к деталям и естественное любопытство.

Как отметил Leverage.Edub своем блоге, существует острая потребность в людях, обладающих знаниями и опытом, выходящими за рамки высоких технологий. «Потенциальные роли в области кибербезопасности настолько широки, что даже области, не связанные с техническими знаниями, не защищены от опасностей кибератак, таких как психология, управление проектами, маркетинг и связи с общественностью», - говорится в сообщении.

Почти каждая работа - и в данном случае я имею в виду индивидуальные должностные обязанности по сравнению с общей карьерой - имеет уникальные аспекты, которые новые сотрудники изучают по ходу работы. Они опираются на то, чему учатся, и переходят к следующей позиции, где они делают то же самое. Любой тип формального обучения дает основу, но наиболее полный способ овладеть навыками - это работа. Так что же мешает людям с гуманитарным образованием попасть на эти должности?

Менеджменту и персоналу необходимо мыслить нестандартно

Уже давно существует стандартный список навыков в области кибербезопасности, который сотрудники и руководство используют для новых сотрудников. Честно говоря, персонал отдела кадров ищет технические навыки и ученые степени. Менеджеры должны знать, что работа выходит за рамки этих стандартных потребностей. Тем не менее, им нужен человек, который может приступить к работе готовым к работе.

Команды кибербезопасности и так перегружены работой, и ни у кого нет времени беспокоиться об обучении неквалифицированного кандидата. Таким образом, многие менеджеры требуют от пяти до десяти лет опыта и набора сертификатов. Это отлично подходит для специализированной должности или для

кого-то, кто хочет стать начальником службы информационной безопасности. Это не так уж и хорошо для должности начального уровня.

Команда по найму должна определить, чем будет заниматься новый сотрудник и чему его можно научить в процессе работы. Если работа требует навыков межличностного общения, эффективного и действенного общения, как устного, так и письменного, и обеспечивает низкоуровневую техническую поддержку, это может быть правильная должность для кого-то без традиционного образования в STEM.

Киберосведомленность: мыслить как лицо, создающее угрозу

Многие роли в этой отрасли являются реактивными. Они включают в себя попытку выяснить, как злоумышленник проник в систему, чтобы смягчить инцидент и предотвратить его повторение. Но сегодня угрозы национальных государств становятся все более заметными, а угрозы критически важной инфраструктуре рассматриваются как кибервойны. Необходимы навыки кибербезопасности, которые могут быть проактивными. Защитникам необходимо выяснить, почему и где злоумышленник сделает следующий ход.

Например, люди, имеющие опыт работы в области психологии и социологии, понимают человеческую психику. Они могут найти закономерности в поведении злоумышленников. Специалисты в области политологии и истории знают о конфликтах и причинах, по которым угрозы одного региона отличаются от других.

А если есть инцидент, который нужно объяснить общественности? Писатель или специалист по маркетингу с обучением в области кибербезопасности будет идеальным человеком для вашей команды по исправлению ситуации. В конце концов, они могут представить техническую информацию простым языком.

Перспективы работы в сфере кибербезопасности для специальностей гуманитарных наук

Технические навыки по-прежнему важны. Сотрудник по кибербезопасности на любом уровне должен знать, как обращаться с компьютером или сетью. Недостаток навыков в области кибербезопасности оставил много открытых дверей, но человеку, неимеющему навыков в области информационных технологий или киберпространства, придется доказать, что он готов принять вызов.

Полезно иметь некоторую курсовую работу или неформальное обучение, чтобы добавить их в резюме. Возможно, возьмите уроки кодирования на стороне или поработайте над ИТ-сертификатами. Это показывает, что вы знаете основы и хотите изучать новые задачи. Полезно продемонстрировать передовые методы обеспечения безопасности и ознакомиться с отраслью, которая стоит за заголовками. Таким образом вы покажете, что знаете, где находятся проблемные места.

Когда начать

Две конкретные области хороши для людей с гуманитарным образованием, чтобы развить свои навыки кибербезопасности. Это обучение по вопросам кибербезопасности и работа в службе поддержки. Тренинг осведомленности - задача, которую недооценивают. Кому-то нужно составить образовательные программы, даже если это нужно для еженедельного электронного письма с Phish Test.Служба поддержки - это уже должность начального уровня. Это требует

некоторых исследований, некоторых базовых диагностических навыков и умения обращаться с разочарованными людьми.

В целом, команда по найму должна иметь четко определенное представление о проблеме, которую они пытаются решить. Вы должны уметь определять, где ваша команда терпит неудачу, где слабые и сильные стороны вашей защиты и реальные навыки, необходимые для решения проблем. Если вы хотите, чтобы кто-то перенастроил вашу облачную архитектуру, вам нужен кто-то с сильными ИТ-навыками и опытом работы в облачных вычислениях. Если вы хотите, чтобы кто-то решал проблемы с вниманием к деталям, вы можете найти идеального сотрудника со степенью бакалавра гуманитарных наук». ***(Sue Poremba. Your Liberal Arts Degree Gives You the Skills for a Cybersecurity Career // IBM (https://securityintelligence.com/articles/liberal-arts-degree-skills-cybersecurity-career/). 26.10.2021).***

***

«Согласно новым результатам исследования 2021 (ISC)^2 Cybersecurity Workforce Study, проведенного (ISC)I, некоммерческой ассоциацией сертифицированных профессионалов в области кибербезопасности, с 2020 года в отрасль США присоединились более 260 000 профессионаловв области кибербезопасности. В исследовании отслеживается глобальная оценка персонала в области кибербезопасности и нехватка кадров в области кибербезопасности ежегодно с 2019 года.

(ISC)I собраны данные от 4753 специалистов в области кибербезопасности и ИТ / ИКТ, каждый из которых посвящает не менее 25% своего времени задачам кибербезопасности, работая с малыми, средними и крупными организациями в Северной Америке, Европе, Латинской Америке и Азии. Тихоокеанский регион для точной оценки численности нынешнего персонала в области кибербезопасности и проблем, с которыми он сталкивается в условиях меняющегося ландшафта угроз.

Исследование показывает снижение глобальной нехватки рабочей силы второй год подряд с 3,12 миллиона до 2,72 миллиона профессионалов в области кибербезопасности. Одним из существенных факторов, повлиявших на оценку нехватки кадров в этом году, является то, что с 2020 года 700000 новых участников присоединились к этой области во всем мире, что способствовало резкому увеличению доступного предложения, которое сейчас составляет 4,19 миллиона человек.

Даже при 700 000 новых участников спрос продолжает опережать предложение талантов. Чтобы эффективно защищать критически важные активы организаций, глобальный персонал, занимающийся вопросами кибербезопасности, должен вырасти на 65%.

Как организации преодолевают разрыв

Исследование этого года позволяет по-новому взглянуть на то, как организации преодолевают нехватку собственных кадров. Участники исследования поделились запланированными в их организациях инвестициями в таланты и технологии, в том числе:

Больше обучения (36%); обеспечение более гибких условий труда (33%); и инвестирование в инициативы по разнообразию, справедливости и инклюзивности (DEI) (29%)

Использование поставщиков облачных услуг (38%); развертывание интеллекта и автоматизации для ручных задач (37%); и вовлечение сотрудников службы кибербезопасности ранее в отношения с третьими сторонами (32%)

Исследование выявило последствия, которых можно избежать, если сотрудники отдела кибербезопасности слишком растянуты. Участники сказали, что столкнулись с неправильно настроенными системами (32%); не хватает времени для правильной оценки и управления рисками (30%); медленно исправляемые критические системы (29%); и поспешное развертывание (27%).

Участники также высказали свое мнение о том, каких специализированных навыков и ролей не хватает их командам, в соответствии с ролями, изложенными в Национальной инициативе правительства США по образованию в области кибербезопасности (NICE). Они назвали такие категории, как «Надежное обеспечение» (48%); Анализировать (47%); и «Защищать» и «Защищать» (47%) как главные области, в которых нуждаются, но данные также показывают острую потребность в помощи для всех ролей.

Длительное воздействие пандемии

Процент профессионалов в области кибербезопасности, работающих удаленно в той или иной степени из-за пандемии, остается неизменным и составляет 85%; однако 37% сообщают, что теперь они должны приходить в офис время от времени по сравнению с 31% в 2020 году. В дополнение к преимуществам удаленной работы в качестве меры общественного здравоохранения, организации указали на повышение гибкости рабочего места (53%); ускорение инноваций и цифровой трансформации (37%); и более тесное сотрудничество (34%), поскольку пандемия изменила их организации к лучшему.

Проблемы безопасности, связанные с удаленной рабочей силой, включали быстрое развертывание новых инструментов для совместной работы (31%); недостаточная осведомленность о безопасности среди удаленных сотрудников (30%); и растущее беспокойство о физической безопасности распределенных активов (29%)». ***(Closing the cybersecurity workforce gap //BNP Media (https://www.securitymagazine.com/articles/96385-closing-the-cybersecurity-workforce-gap). 26.10.2021).***

***

«100 лучших веб-сайтов обычно не соблюдают передовые методы безопасности транспортного уровня (TLS) и по-прежнему поддерживают устаревшие протоколы, говорится в новом отчете.

Отчет TLS Telemetry Report за 2021 год, составленный фирмой по кибербезопасности F5 Labs, анализирует, насколько успешно самые загруженные веб-сайты в Интернете внедряют передовые методы HTTPS и TLSс использованием данных сканирования самых популярных веб-сайтов.

«По мере того, как старые протоколы оказываются небезопасными и появляются новые стандарты, как никогда важно поддерживать конфигурации

HTTPS в актуальном состоянии... Как показывает этот отчет, проблема заключается не столько в отсутствии новых шифров и функций безопасности, сколько в скорость удаления старых и уязвимых протоколов», - говорится в отчете.

Комментируя важность этой информации, F5 говорит, что веб-сайты, которые обычно не соблюдают передовые методы TLS, также обычно являются старыми и любят уязвимые веб-серверы.

Два шага вперед...

Дэвид Варбертон, главный евангелист по исследованиям угроз (EMEA) в F5 Networks, пишет, что отчет показывает, что, хотя шифрование в Интернете улучшилось в нескольких отношениях по сравнению с прошлым годом, стагнация или даже регресс во многих других областях сводят на нет некоторые достижения.

В отчете отмечается несколько положительных моментов, таких как широкое распространение TLS 1.3, который, наконец, стал предпочтительным протоколом шифрования на большинстве веб-серверов из одного миллиона веб-сайтов.

Кроме того, максимальный срок службы недавно выпущенных сертификатов SSLтакже значительно снизился в сентябре 2020 года: с трех лет до 398 дней.

... и один шаг назад

С другой стороны, отчет показал, что 100 лучших сайтов с большей вероятностью будут поддерживать старые протоколы SSL 3, TLS 1.0 и TLS 1.1, чем серверы с гораздо меньшим трафиком.

Что еще более тревожно, было обнаружено, что 22% веб-серверов работали под Apache 2.0, который был выпущен в 2002 году и последний раз исправлен в 2013 году.

В отчете также отмечается, что количество фишинговых сайтов, которые использовали HTTPS с действующими сертификатами, чтобы выглядеть более легитимными, выросло с 70% в 2019 году до почти 83%.

«Совершенно очевидно, что в 2022 году мы сталкиваемся с двумя важными реалиями. Первая заключается в том, что желание перехватить, обойти и ослабить шифрование никогда не было таким большим... Другая заключается в том, что самые большие недостатки связаны не с новейшими функциями, с которыми мы сталкиваемся. принять, но старые мы не хотим отключать», - заключает Уорбертон». ***(Mayank Sharma. Many of the world's top websites still support older, deprecated security protocols // Future US, Inc (https://www.techradar.com/news/many-of-the-worlds-top-websites-still-support-older-deprecated-security-protocols). 22.10.2021).***

***

«Еще в 90-х мы все строили массивные брандмауэры вокруг наших систем и тратили наши повседневные ресурсы на поиск дыр, которые можно было бы исправить. Теоретически непроницаемая стена вокруг всего, что у вас есть, - отличная идея, потому что она защищает даже то, о чем вы забыли.

Однако, если стена - ваша единственная защита, она должна быть на 100 процентов идеальной в 100 процентов времени. И если у вас когда-либо был дом, вы знаете, что со временем на всех стенах образуются трещины.Не говоря уже о том, что сегодняшний корпоративный периметр включает в себя облако,

мобильные и удаленные ресурсы, а также могут быть скрытые активы, о которых вы не знаете.

Совершенство не должно быть предпосылкой хорошей кибербезопасности. Я бы сказал, вам не нужно знать обо всем, что у вас есть, чтобы защитить это. Активы можно сгруппировать и классифицировать таким образом, чтобы процедура безопасности учитывала недостатки периметра и видимости.

Подумайте обо всех способах создания мер безопасности, влияющих на целые группы вещей:

Если ваши исходящие правила запрещены по умолчанию, вы все равно можете поймать взломанное устройство, даже если вы не знаете, как оно туда попало.

Если все ваши разработчики обучены создавать образы по умолчанию, ваши инструкции по усилению защиты и ведению журнала могут быть соблюдены, даже если они развертываются с использованием неправильного токена Amazon Web Services (AWS).

Если вся ваша компания получает напоминания о фишинге, это может побудить пользователя предпринять превентивные меры, даже если отдел кадров забыл провести для них индивидуальный тренинг по безопасности для новых сотрудников.

У нас есть всевозможные защиты, которые работают даже при наличии неизвестных или ошибок.

Нанесите на карту свои внутренние пути

Ваша система чрезвычайно сложна. Так что, если я мыслю как злоумышленник, попытка понять всю поверхность атаки не является началом. Мне не нужно знать все ваши активы или все о вашей стратегии безопасности. Я должен думать о том, какая цель самая заманчивая - о пути к успеху - как о точке входа для взлома поверхности атаки.

Вот как вы должны думать о защите своей системы: найдите пути, которые существуют между вашей поверхностью атаки и вашими конфиденциальными активами, и уничтожьте их. Если пути приведут вас к критически важной функции, поставьте своего противника в узкое место и закопайте его в отказоустойчивые устройства и предупреждения. Таким образом, когда злоумышленники воспользуются этим путем, вы узнаете задолго до того, как они смогут извлечь данные.

Не существует волшебной формулы для классификации ваших активов и способов их защиты. Существует бесконечное количество способов их категоризации, и правильный полностью зависит от контекста вашей организации. BRandorimы пытаемся обучить себя и других группировать активы в функциональные кластеры: мы смотрим, какие из них представляют собой «путь» для злоумышленника, а затем определяем, сколько политик мы должны создать вокруг них, чтобы убедиться, что нам нравится «освещение».

Как мне классифицировать активы для киберзащиты?

Один из способов разделить это - распределить активы по категориям на основе того, что нужно для связи с Интернетом, а что нет. Скорее всего, подавляющее большинство ваших интернет-ресурсов - это компоненты

приложений или устройств типа «программное обеспечение как услуга» (SaaS), которые вы не используете или не должны использовать. Если у вас есть устройство, которое обеспечивает передачу файлов и VPN, и вы используете только VPN, отключите функцию передачи файлов.

Вы можете отключить эти функции и забыть о них. Если сотрудник приходит к вам и говорит, что он нужен им для работы, просто включите его снова (по умолчанию - запретить, кто-нибудь?).

Затем идет следующая категория: вещи, которые видны извне и необходимы для работы компании, например, ваш корпоративный веб-сайт или протокол удаленного доступа. Это, без сомнения, одни из самых заметных путей между вашей поверхностью атаки и драгоценностями вашей короны. Они предназначены для того, чтобы быть - как еще ваши сотрудники могли бы получить доступ к чему-либо? Эти активы должны быть защищены с большим количеством мониторинга и предупреждений, и вокруг них должна быть DMZ (демилитаризованная зона).

Знайте, что важно, и забудьте обо всем остальном

Вы, вероятно, уже установили DMZ в своей сети - куда вы помещаете активы, которые должны быть доступны в Интернете и тщательно отслеживаться. Ваш корпоративный веб-сайт находится на сервере, полностью изолированном от вашего основного бизнеса. Каждый раз, когда у вас также есть VPN или какой-либо инструмент удаленного доступа, он попадает в вашу демилитаризованную зону, где у вас есть жесткая сегментация и мониторинг.

Все, что находится в DMZ, намеренно реализуется с минимальными привилегиями, и, находясь в DMZ (или даже глубже в вашей сети), любая служба наследует сегментацию, а также некоторую видимость или мониторинг. Есть несколько небольших путей, но я подчеркиваю, что они небольшие, потому что вам необходимо тщательно следить за ними. Каждый уровень, расположенный глубже в вашей среде, должен унаследовать больше средств защиты и требовать большего количества сбоев для возникновения нарушения.

Сегментирование и усиление ограничивают возможности вашего оппонента. Ограничение нормальной активности между активами, где это возможно (например, между DMZ и вашей базовой сетью), создает возможности для обнаружения.

Команда безопасности здесь выступает в роли советника и создает политики, чтобы попытаться унаследовать защиту. BRandori, когда разработчики экспериментируют с кодом, я хочу, чтобы они «кодировали безопасно», но я также хочу, чтобы незаконченная работа или работа над прототипом унаследовала некоторые защиты, даже если будут сделаны ошибки. Итак, мы управляем несколькими простыми дополнительными уровнями: все развертывается без прямого доступа в Интернет. Разработчики могут выполнять свою работу, но даже если они случайно отключат аутентификацию в создаваемом приложении, приложение все равно «защищено» уровнем единого входа (SSO).

Всегда будут неизвестные и невидимые активы

Если вы получили сканирование Qualys, и оно сообщает о 3 миллионах уязвимостей на вашей поверхности атаки, вы ничего не сможете с этим поделать, потому что вы не можете отправить 3 миллиона исправлений. Но если вы знаете,

какие уязвимости в сегментах имеют значение и унаследовали недостаточную защиту, вы можете определить приоритеты для устранения.

Если сервер приложений, которому разрешено проходить через вашу демилитаризованную зону, не исправлен, вам нужно сначала исправить это. У вас есть внутренний сервер приложений, доступный только ограниченным внутренним пользователям? Может, пока не обращай на это внимания. Если есть место для паники по поводу неизвестных уязвимостей, то, скорее всего, это сервер приложений, проходящий через вашу демилитаризованную зону, а не ваш внутренний.

Мы все также знаем, что теневые ИТ - это серьезная проблема (примерно 40 процентов ИТ-расходов), и в идеале вы должны использовать платформу управления поверхностью атаки, чтобы помочь вам найти сюрпризы в своей сети. Но когда вы планируете свою позицию безопасности, вы должны предположить, что эта теневая проблема будет продолжать существовать, и убедиться, что эти один или два сюрприза не станут заголовком Associated Press.

Кто-то всегда будет «что-то подключать к Интернету». Если ваша демилитаризованная зона требует контроля доступа к сети (NAC), по умолчанию запрещает доступ к внутренней сети и генерирует предупреждения для вашего поставщика услуг управляемой безопасности (MSSP) или ИТ-команды, то для «подключения чего-либо к Интернету» требуется гораздо больше, чем один сбой. создать значительный риск нарушения.

Итог: вы должны проектировать свои системы безопасности с предположением, что злоумышленник может взломать любой актив и завладеть его элементами управления, его привилегиями и его функциями. Вы можете защитить актив, даже если вы о нем не знаете, практикуя глубокоэшелонированную защиту - зная, что важно, и внедряя множество разрозненных элементов управления без единой точки отказа». ***(David “moose” Wolpoff. Defending Assets You Don’t Know About, Against Cyberattacks // Threatpost (https://threatpost.com/defending-unknown-assets-cyberattacks/175730/). 25.10.2021).***

***

«Неумолимое перемещение данных и приложений в облако, которое началось несколько лет назад и ускорилось во время пандемии, не показывает никаких признаков замедления. Обоснование этой трансформации обусловлено желанием передать на аутсорсинг некритичные функции (создание и обслуживание центров обработки данных, запуск и исправление стандартных пакетов программного обеспечения) и добиться гибкости бизнеса (масштабирование, возможность быстро сместить фокус в свете рыночных условий).

Часть этой миграции приходится на общедоступные облака, такие как Amazon Web Services (AWS) и Microsoft Azure.Эти платформы выдвинули на первый план понятие «модели совместной ответственности», связанное с безопасностью и совместимостью всего решения. В этой статье я рассматриваю модель совместной ответственности общедоступного облака с точки зрения некоторых недавних уязвимостей безопасности, обнаруженных в платформах общедоступного облака, и их последствий для пользователей.

Вот беглый взгляд на вывод: поставщики облачных услуг не обязательно хороши в укреплении программных образов, которые они предоставляют компаниям.

Модель совместной ответственности

Как картинка лучше тысячи слов, так вот инфографика для модели совместной ответственности AWS; авоти для Microsoft Azure. Обе модели пытаются сообщить, что «мы заботимся об основах, а вы заботитесь о том, что находится под вашим контролем». Другими словами, AWS гарантирует, что доступ к корзинам S3 возможен только в соответствии с политикой, регулирующей их использование, и ответственность за установку политики, соответствующей хранящимся в них данным, лежит на клиенте. При предоставлении услуг «платформа как услуга» (PaaS) в Azure ответственность Microsoft заключается в том, чтобы ОС, используемая для предоставления услуги, была исправлена и усилена.

Теперь давайте рассмотрим, как эти модели работают в реальной жизни, рассмотрев три ошибки безопасности и то, как они повлияли на клиентов, которые мы можем охарактеризовать как хорошие, плохие и уродливые.

Хорошо…

Уязвимости с выходом из контейнера позволяют эксплойту выйти за пределы контейнера, в который ранее проник злоумышленник. Это похоже на создание злоумышленником эксплойта для выхода из виртуальной машины (ВМ) и проникновения в гипервизор, тем самым получая доступ к содержимому базовой ОС и других виртуальных машин, работающих под тем же гипервизором.

Примером может служить CVE-2019-5736, ошибка в RunC, проекте строительных блоков для контейнерных технологий, используемых многими предприятиями, а также поставщиками общедоступного облака. В 2019 году он исправил уязвимость, которая позволяла выполнять код на корневом уровне, выходить из контейнера и получать доступ к файловой системе хоста.

Хотя об этой проблеме было сообщено более двух лет назад, она является иллюстрацией случая, когда модель совместной ответственности работала на пользу клиентам общедоступного облака. Уязвимость и связанный с ней эксплойт были раскрыты 11 февраля 2019 г., когда все основные поставщики облачных услуг исправили уязвимость. Организации, которые запускали контейнеры в своих центрах обработки данных, были вынуждены изо всех сил исправлять свои образы ОС контейнеров.

Плохо…

Совсем недавно, в августе, Microsoft обнародовала сообщение об уязвимости в Azure Cosmos DB, масштабируемой базе данных NoSQL, предоставляемой по модели PaaS. Уязвимость была в функции Jupyter Notebook в Cosmos DB и, таким образом, затрагивала только клиентов, у которых была включена эта функция. К сожалению, функция Jupyter Notebook была автоматически включена для всех Cosmos DB, созданных после февраля этого года, что даже подвергло клиентов, которые не использовали эту функцию, потенциальной атаке.

Служба Cosmos DB фактически является мультитенантной. Таким образом, данные от нескольких клиентов объединяются в одном экземпляре службы. Доступ

к конкретным данным ограничен простыми программными конструкциями, которые в данном случае были подорваны. Это означает, что злоумышленник может зарегистрировать учетную запись Azure, запустить экземпляр Cosmos DB и использовать его для доступа к данным из экземпляров всех других клиентов.

Это пример уязвимости, которая встречается только в облаке, поскольку она существует в специальной службе Azure PaaS.И это подчеркивает тот факт, что то, что компания активно не использует определенную функцию (Jupyter Notebooks), не означает, что она не подвержена уязвимостям в этой функции.

...и уродливо

В сентябре Microsoft раскрыла серию уязвимостей, связанных с агентом Open Management Infrastructure (OMI), включенным в определенные образы виртуальных машин Linux, которые он поставляет клиентам.

Агент OMI включается в образы виртуальных машин, предоставляемые клиентам, в зависимости от того, какие службы Azure клиент намеревается использовать. Однако Microsoft не задокументировала присутствие агента, даже несмотря на то, что агент работает с максимально возможным уровнем привилегий.В некоторых случаях (при включенных определенных службах Azure) он принимает подключения через HTTPS через Интернет.

Группа из четырех уязвимостей, получившая общее название «OMIGOD», включала одну критическую с рейтингом 9,8 из 10 возможных по шкале серьезности ошибки CVSS; он позволяет удаленное выполнение кода.

Это случай, когда отсутствие прозрачности в цепочке поставок другого типа (стандартные образы виртуальных машин, предоставляемые поставщиком облачных услуг) открывает виртуальные машины, развернутые клиентом, для чрезвычайно серьезной атаки. Как будто для подтверждения этого утверждения, атаки на эту уязвимость начались почти сразу после раскрытия уязвимости, и устранение / исправление должны были быть скоординированным делом - Microsoft исправляла образы Linux, которые она поставляет, а клиентам необходимо исправлять уже работающие версии старых образов.

Выводы

Находиться в общедоступных облаках хорошо, когда обнаруживается масштабная уязвимость, такая как побег из контейнера. Поставщики облачных услуг, как правило, отлично справляются с решением таких проблем в большом масштабе, и их устранение часто требует небольшой работы со стороны их клиентов. Однако существуют значительные риски безопасности при выполнении рабочих нагрузок в общедоступном облаке.

Нет гарантии, что услуги, предоставляемые в модели PaaS, будут реализованы надежно и безопасно. У злоумышленников также есть большой стимул тратить энергию, пытаясь взломать такие службы, поскольку обнаруженная уязвимость легко используется для большого набора целей.

Более того, стимулы поставщика облачных услуг (устранение барьеров, мешающих более широкому использованию) и пользователя (включение минимального набора функций) не совпадают. Таким образом, даже клиенты Cosmos DB, которые никогда не использовали или не собирались использовать

функцию Jupyter Notebook, были подвержены потенциальной атаке из-за этого диссонанса в целях.

Хотя может показаться, что им легко доверить правильную модель совместной ответственности, в последнее время есть явные примеры, когда доверие было неуместным. Относитесь ко всему программному обеспечению, которое вы получаете от поставщиков облачных услуг, со здоровой долей скептицизма - сканируйте их и учитывайте каждый открытый порт и все имеющиеся программные пакеты». ***(Oliver Tavakoli. Public Clouds & Shared Responsibility: Lessons from Vulnerability Disclosure // Threatpost (https://threatpost.com/public-clouds-shared-responsibility-vulnerability/175778/). 26.10.2021).***

***

«В эпоху удаленной работы, когда гибридные команды работают вне офисов, домов и кафе, используя множество устройств, возникают проблемы с точки зрения понимания того, кто несет ответственность за обеспечение надлежащей кибергигиены во всем пространстве без периметра. Достаточно сказать, что кибербезопасность стала головной болью для многих организаций. Согласно отчёту IBM «Стоимость утечки данных за 2021 год», это также связано с большими затратами.

Помимо денежно-кредитных соображений, компании, столкнувшиеся с нарушениями, также рискуют подорвать свою репутацию и попасть в заголовки газет по неправильным причинам. Хорошая новость заключается в том, что, применяя проактивный подход к кибербезопасности, понимая роли безопасности и подотчетность, инвестируя в правильные инструменты и следуя передовым практикам, вы можете укрепить позицию своей организации в области безопасности и защитить свои системы, данные и бренд на этом пути.

Кто отвечает за кибербезопасность?

Исторически сложилось так, что руководство в значительной степени отвечало за кибербезопасность и почти всегда рассматривало безопасность как центр затрат. В эпоху эскалации кибератак все меняется.

Сегодня безопасность – это ответственность каждого. Если вы стремитесь защитить себя от угроз, вам будет трудно достичь своих целей, если каждый сотрудник не поймет, что безопасность - это общая ответственность.

В то же время специалистам-практикам в области безопасности важно понимать стоящие на кону бизнес-потребности и расставлять приоритеты по готовности и устранению последствий, а также уметь эффективно отражать риски, связанные с атакой. Когда вы заявляете, что все имеет высокий приоритет, ничто не является приоритетом.

Последствия плохой кибергигиены?

Сегодня компании уже заинтересованы в применении хорошей кибербезопасности. Ставя во главу угла кибербезопасность, они могут снизить вероятность проникновения в системы, тем самым защищая от связанных с этим последствий нарушений, таких как судебные штрафы, отток клиентов и более низкая цена акций.

Однако с ростом числа нарушений и ухудшением их воздействия стоит задуматься о том, можем ли мы, как общество, сделать больше, чтобы побудить организации серьезно относиться к кибергигиене.

Ранее в этом году администрация Байдена издала распоряжение о совершенствовании политики страны в области кибербезопасности на федеральном уровне. Несмотря на то, что в отношении предприятий было выпущено мало руководящих указаний, похоже, что это написано на стене, и организациям в конечном итоге придется нести большую ответственность, когда дело доходит до защиты своих систем и сетей.

Несмотря на то, что плохие методы обеспечения безопасности должны иметь последствия, не так-то просто понять, какими могут быть эти наказания. Например, компании, нарушающие Европейские общие правила защиты данных (GDPR), могут быть оштрафованы на сумму до 20 миллионов евро или 4 процентов годового мирового оборота, в зависимости от того, какая сумма больше. К сожалению, небольшие компании ощутят на себе влияние этих штрафов гораздо сильнее, чем такие гиганты, как Google и Facebook, которые могут даже не заметить вмятины на своем пресловутом кошельке.

Кроме того, наложение штрафов на компании за ненадлежащие меры безопасности может действительно навредить стартапам. В конце концов, большинство стартапов вряд ли могут позволить себе платить себе, не говоря уже о найме полностью функционирующей команды безопасности. Ситуация усложняется тем, что от некоторых угроз, с которыми сталкиваются организации - например, постоянных атак со стороны национальных государств - практически невозможно защититься. Разве разумно просить небольшую команду защищаться от подобных угроз?

Как ни крути, это сложный вопрос, на который нет простых ответов.

Как встроить подотчетность в вашу инфраструктуру безопасности

Хотя нормативно-правовые акты, безусловно, могут помочь поднять планку гигиены кибербезопасности, ни то, ни другое не удержит продвинутых злоумышленников навсегда. Компаниям необходимо применять проактивный подход к кибербезопасности, встраивая подотчетность в свою инфраструктуру безопасности и используя правильные инструменты и структуры.

Для этого начните с установки твердой базовой линии и начните с основ. Такие вещи, как установка исправлений, управление учетными данными, нулевое доверие и доступ с минимальными привилегиями, могут иметь большое значение для защиты вашей организации. Когда вы понимаете основы, у ИТ-отдела появляется больше времени, чтобы сосредоточиться на критических функциях, потому что нужно решать меньше обращений в службу поддержки, а сеть становится более предсказуемой, что часто приводит к менее напряженной работе.

В дополнение к использованию правильных инструментов и автоматизации повторяющихся ИТ-задач, где это возможно, организациям также следует использовать структуры, например, из Национального института стандартов и технологий (NIST), которые предоставляют отличные дорожные карты и рекомендации по структурированию вашей программы безопасности. Точно так же

им следует изучить передовой опыт Центра интернет-безопасности (CIS) как хорошую отправную точку, чтобы сразу приступить к работе.

Для достижения наилучших результатов компаниям необходимо определить чемпионов по безопасности внутри организации, особенно если еще нет специальной группы безопасности. Когда дело доходит до создания подотчетности, защитники безопасности могут стать умножителем силы, поскольку они обычно понимают свою роль и процессы своей команды лучше, чем кто-либо другой. Они могут быстро выявлять слабые места и управлять внедрением необходимых средств контроля и процессов, необходимых для исправления ситуации.

Улучшите свою гигиену кибербезопасности, пока не стало слишком поздно

Хотя в 2020 году количество взломов могло снизиться, хакерами было украдено колоссальные 37 миллиардов записей, что на 141 процент больше по сравнению с предыдущим годом. Если вашей организации удалось избежать взлома, вам повезло. Но если вы продолжите испытывать свою удачу, это лишь вопрос времени, когда злоумышленники завладеют вашими конфиденциальными данными - и вы будете вынуждены терпеть последствия.

Чем раньше вы начнете оптимизировать подход вашей организации к кибербезопасности, тем быстрее вы обретете душевное спокойствие, зная, что ваши сети защищены. Вместо того, чтобы изо всех сил реагировать на нарушение, когда уже слишком поздно, или беспокоиться о безопасности, вы сможете уделять значительно больше времени сосредоточению внимания на своей миссии и более стратегических и важных инициативах». ***(Chris Hass. Time to Build Accountability Back into Cybersecurity // Threatpost (https://threatpost.com/accountability-cybersecurity/175571/). 18.10.2021).***

***

«Для представителей отрасли неудивительно, что многие программы кибербезопасности пострадали из-за потери доходов во время пандемии. От режущего инструмента и бюджета кормов до сокращения штата - это было в лучшем случае непросто.

В недавнем опросе SANS 2021«Охота на угрозы в неопределенные времена» нам было показано, что пандемия повлияла на 11 процентов организаций, при этом 12 процентов опрошенных организаций полностью прекратили свои программы охоты. В связи с ростом числа партнерских программ-вымогателей и постоянным преследованием организаций, подвергающихся атакам компрометации корпоративной электронной почты (BEC), сейчас ужасное время, чтобы застрять в условиях сокращающегося бюджета.

В свете этого мы собираемся рассмотреть некоторые общие предложения и контрольные списки, как сделать 80 процентов того, что вам нужно делать на фронте киберинтеллекта, всего за 20 процентов от типичных затрат для корпоративной программы.

Оберните в ресурсы с открытым исходным кодом

К счастью, по мере того, как поставщики средств безопасности совершенствовали возможности корпоративных продуктов, росла и зрелость общественных проектов. Соедините эти бесплатные и открытые технологии с

выделенным временем аналитика или исследователя, и у вас будет жизнеспособная альтернатива для низкобюджетной команды.

В этом случае необходимо сделать упор на жизнеспособность, и важно отметить, что вы должны довести до сведения своего руководства тот факт, что управление собственными инструментами связано с ценой человеческих часов.

Многие из бесплатных инструментов и инструментов с открытым исходным кодом не так просты в работе или плохо интегрируются, и поэтому требуют выделенного времени более опытного члена вашей команды для создания части этого операционного клея. Тем не менее, можно многому научиться, а наборы навыков вырастут, если не передать информацию о вашем интеллекте членам вашей команды на серебряном блюде.

Имея это в виду, есть несколько рекомендаций, которые следует соблюдать, если вам нужно работать с ограниченным бюджетом.

Найдите подтверждение со стороны руководства, что недостаток ресурсов не идеален. Убедитесь, что высшее руководство осведомлено о том, что корпоративные инструменты обеспечивают более эффективный анализ и что вам нужно будет потратить человеческие часы, чтобы компенсировать то, что некоторые продукты безопасности «программное обеспечение как услуга» (SaaS) и «песочницы» для вредоносных программ предоставляют из коробка. Отображение показателей вашего успеха и наличие надежных данных о том, как их можно улучшить, - лучший способ обеспечить больший бюджет.

Планирование важнее, чем когда-либо. Перейдите к началу жизненного цикла разведки и изучите свои цели, а затем определите необходимые инструменты и источники данных для достижения ваших целей.

Будьте лучшим источником информации для себя. Использование внешних источников и прогнозной оценки - это фантастика, если у вас есть деньги, которые можно потратить на предположения, чтобы сэкономить время ваших людей при принятии решений. Однако, когда вы работаете без этих корпоративных каналов, вам нужны данные о видимости и угрозах с ваших собственных конечных точек для передачи в инструменты, которые вы используете внутри компании. Вот где команда просто не может сэкономить на SIEM. Даже если это так же просто, как пересылка «системного журнала» на одну управляющую виртуальную машину (ВМ), вам нужен способ приема информации с ваших конечных точек.

После того, как вы полностью определили свой бюджет и потребности в инструментах, пора принимать решения о людских ресурсах и возможностях управления этими инструментами.

Согласование человеческих ресурсов и навыков

Группы по анализу угроз часто состоят из людей разного происхождения. Требуемые навыки включают в себя основы работы с сетями, которые могут возникнуть в результате работы системного администратора, методологию исследования и написания статей журналиста, навыки автоматизации программиста и навыки обратной инженерии аналитика вредоносных программ. Редко когда в вашей команде есть кто-то, кто выполняет все вышеперечисленное, поэтому принимайте во внимание сильные стороны каждого члена команды при принятии решения, кто управляет тем, что имеет решающее значение.

Сложнее всего работать со всем этим - это управление вашими знаниями, обычно называемое платформами анализа угроз (TIP). В некоторой степени вы можете обойтись без электронных таблиц, но в конечном итоге у вашей команды будет слишком много данных для управления и потребуется специальный инструмент.

Инструменты с открытым исходным кодом, такие как MISP, The Hive или OpenCTI, имеют множество движущихся частей, причем обычно уровень приложения обслуживается и поддерживается базой данных, часто в сочетании с хранилищем документов. Для приложений такого типа вам понадобится член команды, обладающий опытом управления инфраструктурой и эксплуатации, поскольку, скорее всего, потребуется настроить значения конфигурации и размер компьютеров, соответствующих вашей рабочей нагрузке.

Если в вашей команде нет кого-то с таким набором навыков, вы можете попробовать присоединиться к экземпляру MISP сообщества или к одной из других открытых платформ обмена угрозами с бесплатным уровнем. В некоторые из них даже будет включен следующий важный элемент обогащения.

Более легким в эксплуатации будут ваши возможности обогащения. Обогащение индикаторов - одно из тех мест, где инструменты с открытым исходным кодом действительно сияют, поскольку такие инструменты, как IntelOwl и Cortex, становятся все более зрелыми; и компании теперь производят свои собственные плагины, позволяющие обогащать.

Оба этих инструмента легко работают через Docker и не требуют многого в плане базы данных производственного уровня. Это связано с тем, что после того, как ваши обогащения были перенесены в хранилище знаний, нет особых причин для сохранения самой работы по обогащению. Если эта служба выходит из строя и восстанавливает пропущенные вакансии месяц назад, это не сильно повлияет на вашу команду.

Эти приложения - хорошее место для тех, кто хочет получить опыт программирования и легкой инфраструктуры из-за их относительной простоты в настройке. Более сложная часть будет соединять эти обогащенные части в ваш СОВЕТ. Есть несколько способов сделать это, в зависимости от инструмента, в котором оба вышеупомянутых инструмента автоматически вводят обогащение в несколько советов с открытым исходным кодом.

После того, как вы разделили эти два основных набора инструментов между своей командой, вам нужно помнить о нескольких вещах, управляя собственной инфраструктурой:

Постарайтесь, чтобы инструмент принадлежал только одному аналитику и двум резервным копиям с некоторыми знаниями инструмента. Помните, что вам нужны люди, которые по-прежнему смогут выявлять угрозы, а управление инфраструктурой может быстро превратиться в постоянную работу.

При создании дополнительных склеивающих задач, которые не входят в сферу этих проектов с открытым исходным кодом, используйте готовое решение на 75 процентов, прежде чем писать его собственными силами. Часто вы найдете достаточно хорошее решение, которое позволит вам перенастроить рабочий процесс и сэкономить время на разработку.

Автоматизируйте и документируйте. Оба являются ключевыми. Напишите автоматизацию для развертывания с помощью инструментов управления инфраструктурой, таких как Terraform, и инструментов управления конфигурацией, таких как Ansible. Таким образом, поддержание инфраструктуры требует повторяемых шагов. Просто отключив процесс, вы сэкономите много времени.

Вернемся к классике. Этого недостаточно, но в наши дни «coreutils» доступны в каждой системе. Множество причудливых инструментов, которые извлекают индикаторы взлома (IoC), анализируют журналы и данные изменений, можно заменить рабочими процессами «awk / sed», «sort» и «uniq». С 1970-х годов люди быстро обрабатывают данные в командной строке. Терабайты данных можно проанализировать за считанные минуты с помощью крошечных одноразовых программ на языке C. Квалифицированные администраторы UNIX знали, что они делали тогда, и если ваша команда изучит этот бесплатный инструмент швейцарской армии, это значительно ускорит их обработку данных.

Когда дело доходит до управления вашей инфраструктурой внутри компании, существует ряд различных инструментов, которые могут помочь вашей команде максимально приблизиться к продуктам корпоративного уровня. Хотя это предприятие потребует определенного количества человеческих часов, отнимая у аналитиков время, которое может занимать исследование угроз, этот компромисс с затратами может быть тем, что вашей группе необходимо для продолжения эффективности в условиях ограниченного бюджета». ***(Chad Anderson. A Guide to Doing Cyberintelligence on a Restricted Budget // Threatpost (https://threatpost.com/guide-cyberintelligence-restricted-budget/175574/). 19.10.2021).***

***

«Исторически защита удаленного доступа в основном осуществлялась с помощью VPN. Однако, поскольку предприятия начали понимать принципы нулевого доверия, согласно которым ни один пользователь не может получить доступ к какому-либо источнику данных без предварительной аутентификации, виртуальных частных сетей оказывается недостаточно.

Спрос на безопасный удаленный доступ к локальным ресурсам неуклонно растет в течение многих лет. Однако, как известно, эта потребность была ускорена переходом на удаленную работу в условиях пандемии. Хотя предприятия переместили больше данных в облако, стремясь реализовать различные инициативы по цифровой трансформации и обеспечить удаленную работу, потребность в локальных ресурсах сохраняется, и сотрудникам по-прежнему необходим безопасный удаленный доступ к этим данным.

Поскольку компании стремятся реализовать решение доступа к сети с нулевым доверием (ZTNA), необходимо учитывать важные соображения, чтобы избежать распространенных ошибок в таких областях, как производительность, защита от потери данных (DLP), расширенная защита от угроз (ATP), видимость и отчетность.

Как избежать ловушек с нулевым доверием

При сравнении вариантов ZTNA организациям следует задать следующие четыре ключевых вопроса, чтобы убедиться, что их подход способен удовлетворить их потребности в безопасности:

1. Может ли он соответствовать сегодняшней гибридной рабочей среде?

Когда дело доходит до выбора правильного решения ZTNA, решающее значение имеет производительность. Рабочее место прошло долгий путь с первых дней пандемии, когда многие организации вложили значительные средства в масштабирование своих возможностей VPN для обеспечения удаленной работы. Степень расширения этой технологии, вероятно, больше не нужна сейчас, когда многие рабочие места перешли на гибридную среду.

Виртуальные частные сети на основе локальных устройств возлагают бремя подготовки и масштабирования на организацию-потребителя. Чтобы ограничить риск, который вызывает, компаниям следует искать решение ZTNA, которое позволяет инфраструктуре, необходимой для работы, размещаться у поставщика решения в общедоступном облаке.

Поиск общедоступного облачного решения - это начало, но это не единственный компонент производительности, который следует учитывать. Команды безопасности также должны тщательно проверять решение, чтобы убедиться, что его скорость реагирования и надежность соответствуют потребностям бизнеса. Для этого организациям следует сравнить его со своей типичной пользовательской базой (которая должна включать пользователей из разных мест по всему миру) и проверить возможные дополнительные задержки. Правильное решение сможет адаптироваться к пиковым нагрузкам независимо от местонахождения каждого пользователя и будет иметь подтвержденный отчет о стабильной высокой доступности.

2. Сможет ли он выявлять и предотвращать нежелательное воздействие в реальном времени?

Организации нуждаются в решении, которое делает больше, чем просто предупреждает их после того, как инцидент уже произошел. Вместо этого он должен обеспечивать принудительное исполнение в реальном времени, чтобы избежать потери данных. Предотвращение раскрытия конфиденциальной информации было одной из многих проблем, с которыми группы безопасности столкнулись на фоне перехода к удаленной рабочей среде и, как следствие, резкого увеличения использования неуправляемых персональных устройств.

Вот почему при выборе решения ZTNA важно учитывать способность технологии успешно применять политики DLP для загрузки и выгрузки (при необходимости) локальных ресурсов.

Чтобы упростить правила нулевого доверия во всей ИТ-инфраструктуре организации, группам безопасности важно обеспечить детальность решения и возможность настройки в зависимости от таких факторов, как местоположение, тип пользователя и другие элементы идентификации.

3. ATP: можно ли остановить вредоносное ПО в реальном времени?

АТФ - еще один важный компонент раствора ZTNA. Вредоносное ПО может быть легко загружено в документы без ведома сотрудника; и он может распространяться на другие устройства и пользователей через загрузки. Как только

это произойдет, и если подходящая технология отсутствует, злоумышленники могут перемещаться по организации горизонтально. Вот почему важно, чтобы решение ZTNA препятствовало загрузке, загрузке и распространению вредоносных программ в режиме реального времени.

Сейчас ATP особенно актуален из-за его способности защищать удаленных сотрудников с помощью личных, неуправляемых устройств, на которые компания не может установить программное обеспечение безопасности. Для этих лиц выгодно, чтобы решение ZTNA могло останавливать загрузку и загрузку вредоносных программ без необходимости установки программного обеспечения на устройства пользователей.

4. Может ли это помочь в соблюдении нормативных требований?

Наконец, организациям следует искать решение ZTNA, которое обеспечивает видимость и контроль в реальном времени, чтобы помочь им продемонстрировать соответствие нормативным требованиям. Возможности создания отчетов должны включать подробные журналы, в которых указываются все действия с файлами, пользователями и приложениями (включая тип устройства, IP-адрес, местоположение и время доступа) как для управляемых, так и для неуправляемых устройств.

Выбор решения, которое обеспечивает простую интеграцию SIEM и экспортируемые журналы, также расширит видимость дополнительных частей сети внутри компании.

Один аспект всеобъемлющей платформы

Стратегические инвестиции в ZTNA означают, что выбранная технология является частью комплексной платформы, такой как безопасный доступ к услугам (SASE). SASE - это концепция кибербезопасности, впервые описанная Gartner в 2019 году, которая объединяет то, что традиционно было разрозненными сетевыми и облачными сервисами. Эта платформа может защитить любое взаимодействие между устройствами, приложениями, веб-сайтами, локальными ресурсами и инфраструктурой с использованием различных технологий безопасности на единой облачной платформ.» ***(Anurag Kahol. 4 Key Questions for Zero-Trust Success // Threatpost(https://threatpost.com/key-questions-zero-trust-success/175392/). 07.10.2021).***

***

«Как профессионал в области информационной безопасности, готовы ли вы ответить государственному прокурору в случае киберинцидента?

Около половины (47 процентов) организаций, опрошенных в рамках отчета Kroll The State of Incident Response 2021, заявили, что их командам не хватает ясности в отношении того, когда обращаться к юристу в случае потенциального инцидента. Потенциальное влияние текущих и возникающих киберинцидентов настолько велико, что кибербезопасность больше не может оставаться исключительно в рамках группы информационной безопасности организации. Многоуровневый характер реагирования на инциденты требует участия ресурсов всей организации, особенно юридических.

Мы рассмотрим пять ключевых подходов, которые помогут командам информационной безопасности и юристов работать вместе в партнерстве, но сначала давайте рассмотрим некоторые общие передовые практики.

По крайней мере, две из пяти организаций в настоящее время плохо оснащены для выполнения всех юридических требований по урегулированию инцидентов, в то время как у 43 процентов отсутствует четко определенный процесс взаимодействия с регулирующими органами. Во многих организациях команды юристов остаются значительным слепым пятном в программах информационной безопасности. Крайне важно, чтобы они обеспечили согласованность этих двух ключевых групп до того, как произойдет инцидент.

Обмен знаниями о конфиденциальности и защите данных

Каждая организация, которая хранит в цифровом виде личную и / или конфиденциальную информацию, обязана принимать меры по обеспечению конфиденциальности и защиты данных. Это предполагает участие как юристов, так и специалистов по информационной безопасности, чтобы обеспечить сотрудничество для эффективной поддержки стандартов и средств контроля, необходимых для выполнения этих требований.

Некоторые правила конфиденциальности, такие как CCPA, HIPAA, CMMC и GDPR, предусматривают конкретные обязательные меры, которые должны быть приняты, когда организации хранят личную информацию клиентов в электронном виде.

Упражнения по сопоставлению данных имеют решающее значение для выявления и каталогизации защищенной личной информации в сети организации. Этот процесс также следует использовать для устранения любых уязвимостей, необходимых для соответствия применимым требованиям соответствия. Этот процесс требует перекрестной координации между юридической и информационной безопасностью, а также должен включать в себя разработку программы обеспечения конфиденциальности данных для создания дорожной карты для процесса соблюдения конфиденциальности.

Создание и реализация киберполитики и стратегий

Понятно, что после инцидента организации часто уделяют приоритетное внимание финансовым проблемам. В конце концов, киберинциденты могут привести к значительным финансовым потерям, будь то в результате краж, затрат на судебно-медицинское расследование, восстановления и восстановления сетей или уплаты «выкупа» или штрафов. Не говоря уже о разрушительном воздействии на бренд и репутацию, а также о потенциальной потере бизнеса в будущем.

Тем не менее, организации должны обеспечить, чтобы правовые вопросы занимали одно из первых мест в их списке приоритетов кибербезопасности - не только после инцидента / нарушения, но и на протяжении всего процесса создания и пересмотра внутренних политик, стратегий и реализаций безопасности. Это особенно важно при соблюдении новых нормативных или законодательных требований к конфиденциальности.

Юридическое образование по базовой кибербезопасности для оптимизации программ

Эффективное реагирование на инциденты проистекает из взаимной позиции по обмену знаниями. Для группы информационной безопасности важно получить юридическую консультацию по разработке программы обеспечения конфиденциальности данных, в то время как команда юристов также должна быть обучена базовой кибербезопасности. Тогда юристы будут лучше разбираться в нюансах внедрения новых политик или технологий для реализации этих программ.

Необходимость симбиотических отношений между информационной безопасностью и правовыми системами никогда не бывает более острой, чем при внедрении новых технологий. Например, использование устройств IoT, которые хранят защищенную медицинскую информацию (PHI), например те, которые используются в медицине и здравоохранении, должно быть указано и рассмотрено в политике информационной безопасности организации и в том, как это применяется к таким нормативным актам, как HIPAA. Тщательная координация со стороны юристов позволит infosec применять соответствующие элементы управления и конфигурации с «минимальными привилегиями», чтобы доступ к конфиденциальным данным предоставлялся только тем, кто действительно в этом нуждается.

Во время пандемии COVID-19 многие организации стали полагаться на программное обеспечение для видеоконференцсвязи, чтобы общаться с коллегами, клиентами и клиентами. Эти платформы часто используются для обсуждения конфиденциальной, а иногда и защищенной информации, поэтому компрометация может иметь серьезные негативные последствия. Команды Infosec должны координировать свои действия с юридическим отделом, чтобы понять, какие меры безопасности следует внедрить для защиты конфиденциальных данных от доступа посторонних лиц.

В то время как группа информационной безопасности может предлагать и внедрять конкретные технологические решения, следует проконсультироваться с юридическим лицом, чтобы дать рекомендации о том, что применимые нормативные акты определяют как «разумные» меры по соблюдению обязательных минимальных стандартов для защиты этих данных.

В партнерстве: основные действия, которые необходимо предпринять в ответ на инциденты

Сегодняшний ландшафт киберугроз требует перекрестной координации информационных служб и юридических групп для эффективного реагирования и восстановления после инцидента с технической точки зрения, а также с точки зрения соблюдения нормативных требований. Жизненный цикл обычно состоит из следующих этапов:

Определите характер нарушения и необходимые меры по устранению неисправностей

Когда организация выявляет потенциальное вторжение или компрометацию в своей ИТ-сети, информационная служба должна координировать свои действия с юридическим отделом, чтобы предоставлять постоянные обновления о статусе судебно-медицинской экспертизы. Юридический отдел будет нести ответственность за определение того, произошло ли нарушение обязательных данных, подлежащих отчетности, и за необходимые меры по исправлению

положения. Тот факт, что ИТ-команда смогла определить основную причину киберинцидента, локализовать и устранить проблему, не отменяет необходимости в юридическом заключении о том, было ли о «событии» сообщать.

Определите тип раскрываемых данных и любые обязательства по раскрытию информации

Организации должны иметь обновленный план реагирования на инциденты, в котором содержатся инструкции по привлечению юридических лиц и описывается партнерство с информационной безопасностью в области эффективного сохранения доказательств. Согласовав конкретные детали киберинцидента, информационная безопасность и юридический отдел смогут совместно определить тип данных, к которым открыт доступ или доступ к ним, источник компрометации и наличие каких-либо обязательных обязательств по раскрытию информации.

Определить уведомление и ответ

Infosec должна постоянно информировать юристов о масштабах и типах каждого события судебно-медицинской экспертизы, чтобы они могли определить наиболее эффективные меры реагирования. Затем юридический отдел должен сформировать этот ответ на основе законов о конфиденциальности данных и политики конфиденциальности данных, определяемых типом произошедшего нарушения.

Обеспечение соответствия всем применимым законам и нормам

Сложность раскрытия информации о взломе данных и киберинцидентах усугубляется, когда организации работают в нескольких юрисдикциях, каждая с разными требованиями к раскрытию информации и сроками. Это означает обеспечение соблюдения региональных, национальных и межведомственных законов и постановлений. Затем цепочка поставок должна осуществляться юридическими лицами при поддержке infosec.

Подготовьтесь к судебным разбирательствам и предоставьте отчеты

Юридический отдел должен подготовиться к возможным судебным разбирательствам и предоставить рекомендации по возможным гражданским, уголовным или нормативным штрафам, пока Infosec проводит расследование или восстанавливает сеть. Infosec также потребуется обновить правовые нормы о первопричине инцидента и о том, было ли боковое движение в сети, которое могло потенциально раскрыть защищенную информацию, которая потребовала бы обязательного отчета.

Эти этапы слишком часто проводятся разрозненно, хотя для того, чтобы они были эффективными, их необходимо тщательно координировать. Для этого организациям следует разработать четкую стратегию до немедленного реагирования на инциденты.

Заключение

Несмотря на растущее давление, создаваемое нарушениями, юридические последствия инцидентов остаются для многих организаций слепым пятном.Только наладив сотрудничество между своими информационными службами и юридическими отделами, организации могут избежать потенциальных ловушек при реагировании на инциденты.Это позволит им создать прозрачный и оптимизированный маршрут, по которому сотрудники смогут быстро отвечать и

более эффективно реагировать, когда атака идет и время имеет решающее значение». ***(Matt Dunn. Incident Response: 5 Principles to Boost the Infosec/Legal Relationship // Threatpost (https://threatpost.com/incident-response-infosec-legal-relationship/175461/). 11.10.2021).***

***

«Корпорация Майкрософт объявила сегодня о новой программе безопасности для некоммерческих организаций, чтобы обеспечить им защиту от атак со стороны государства, которые все чаще нацелены на них в последние годы.

Компания запустила программу в ответ на быстро развивающуюся индустрию киберпреступности, которая затронула все отрасли по всему миру и некоммерческие организации, в частности, из-за их уязвимости из-за отсутствия адекватных ресурсов для создания подходящей защиты.

После взлома некоммерческие организации обычно предоставляют злоумышленникам доступ к информации, принадлежащей волонтерам, донорам и другим участникам их программ.

«Отчет Microsoft по цифровой защите за 2021 год подтверждает, что за последний год масштабы и изощренность киберпреступности возросли, благодаря кризисам и использованию уязвимых целей», - сказал вице-президент Microsoft по технологиям социального воздействия Джастин Спелхаг.

«В отчете подчеркивается, что в прошлом году неправительственные организации и аналитические центры были вторым сектором, наиболее целевым для киберпреступников, на их долю приходился 31% всех уведомлений об атаках национальных государств на домены организаций, обнаруженных Microsoft».

В рамках новой программы безопасности для некоммерческих организаций Microsoft:

обеспечивать упреждающий мониторинг и уведомление в случае атаки на государство через программу AccountGuard

оценивать риски организации и инфраструктуры, чтобы помочь организациям повысить уровень безопасности в зависимости от среды,

а также оптимизировать обучение ИТ-специалистов и конечных пользователей по вопросам безопасности.

Зарегистрированные организации будут получать уведомления, когда их учетные записи Microsoft 365 или личные учетные записи сотрудников и членов правления Outlook и Hotmail становятся целью или взломаны хакерами, поддерживаемыми государством.

Цель Редмонда - поддержать 10 000 некоммерческих организаций до конца первого года и до 50 000 организаций по всему миру через три года.

«Эти организации являются привлекательными целями для субъектов национального государства, потому что они часто хранят конфиденциальные данные», -добавил Спелхауг.

«Кроме того, согласно Руководству по кибербезопасности для некоммерческих организаций от 2021 года, хотя киберпреступники пытаются получить доступ к правительственным и некоммерческим базам данных каждые 39

секунд, до 70% благотворительных сетей не имеют комплексной оценки уязвимости для определения риска». ***(Sergiu Gatlan. Microsoft now defends nonprofits against nation-state attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/microsoft/microsoft-now-defends-nonprofits-against-nation-state-attacks/). 21.10.2021).***

***

«Сети кибербезопасности, гиперавтоматизация, вычисления, повышающие уровень конфиденциальности, — все эти технологии станут популярными уже в 2022 году и значительно повлияют на развитие Индустрии 4.0.

Аналитическая компания Gartner опубликовала список технологий, которые станут трендовыми в 2022 году. Фокус выбрал самые интересные из них.

Сеть кибербезопасности

Cybersecurity Mesh, или Сеть кибербезопасности, — это интеграция структуры безопасности для защиты всех активов, независимо от местонахождения. К 2024 году организации и бизнесы, внедряющие такие сети для обеспечения защиты всей своей экосистемы, смогут сократить финансовые потери в следствие кибератак в среднем на 90%.

Вычисления, повышающие конфиденциальность

Методы Privacy-Enhancing Computation (PEC), которые защищают личную и конфиденциальную информацию на уровне данных, программного или аппаратного обеспечения, обеспечивают безопасный обмен, объединение и анализ данных без ущерба для конфиденциальности.

«ИТ-директора должны не только заниматься совершенствованием международного законодательства о конфиденциальности и защите данных, но и избегать таких рисков, как потеря доверия со стороны клиентов в результате инцидентов, связанных с нарушением конфиденциальности. К 2025 году 60% крупных организаций будут использовать один или несколько методов вычислений, повышающих уровень конфиденциальности», — говорится в документе.

Гиперавтоматизация

Исследование Gartner показывает, что те предприятия, которые сосредоточены на гиперавтоматизации, имеют три ключевые приоритета:

повышение качества работы,

ускорение бизнес-процессов,

повышение гибкости принятия решений.

Аналитики полагают, что данная технология безусловно станет трендовой в ближайшие годы.

Интеллект в принятии решений

Decision Intelligence, или Интеллект в принятии решений — это технология, призванная ускорять и делать более эффективным процесс принятия решений. Делается это благодаря системе decision-making. Полученные результаты анализируются, оцениваются, улучшаются. К 2024 году более 30% всех крупных

бизнесов и организаций будут применять эту технологию, чтобы повысить свою конкурентоспособность.

Генеративный искусственный интеллект

Generative Artificial Intelligence (генеративный ИИ) аналитики называют «одним из наиболее заметных и мощных методов искусственного интеллекта». При помощи машинного обучения такой ИИ изучает контент или объекты, и на основе полученных данных создает совершенно новые, оригинальные и реалистичные объекты/контент.

Генеративный ИИ может использоваться для создания софта, применяться при разработке лекарств или в сфере целевого маркетинга. К сожалению, он также может использоваться для мошенничества, политической дезинформации, подделки личности и многого другого. К 2025 году Gartner ожидает, что на генеративный ИИ будет приходиться 10% всех производимых данных, по сравнению с менее чем 1% сегодня.

Фабрики данных

Количество разрозненных хранилищ данных и приложений резко выросло за последнее десятилетие, в то время как количество квалифицированного персонала либо осталось неизменным, либо даже сократилось. Так называемые Data Fabric (фабрики данных) — гибкая, устойчивая интеграция данных между платформами и бизнес-пользователями — появились для упрощения инфраструктуры интеграции данных и создания масштабируемой архитектуры данных.

Настоящая ценность фабрик данных заключается в их способности улучшать использование данных с помощью встроенной аналитики, сокращая усилия по управлению данными до 70%.

Облачные платформы

Чтобы по-настоящему диджитализироваться, предприятиям необходимо перейти на облачные платформы, считают аналитики. Также благодаря облачным платформам (ОП) люди смогут получать цифровые услуги, находясь в любой точке мира. В Gartner полагают, что через 4 года на ОП будет базироваться до 95% новых цифровых инициатив. Сейчас мы имеем показатель в 40%.

Автономные системы

По мере роста предприятий автоматизация как таковая не будет масштабироваться, говорят эксперты. Но ситуацию смогут изменить так называемые автономные системы — самоуправляемые и самообучающиеся физические (роботические) или программные системы. В отличие от автоматизированных систем, автономные системы могут динамически изменять свои собственные алгоритмы без внешнего обновления программного обеспечения, что позволяет им быстро адаптироваться к новым условиям так, как это могут делать люди.

Составные приложения

Сегодня существует острая потребность в адаптируемости бизнеса, поэтому он нуждается в технологической архитектуре, которая поддерживает быстрое, безопасное и эффективное изменение приложений. Архитектура составных приложений обеспечивает высокую адаптивность, и те, кто ею пользуется, смогут

опередить конкурентов, сумев очень быстро внедрить новые функции. Аналитики говорят, что данная технология способна повысить адаптивность на 80%.

ИИ инжиниринг

К 2025 году 10% предприятий, внедряющих передовые методы разработки ИИ, будут приносить как минимум в 3 раза больше прибыли именно благодаря ИИ, чем 90% предприятий, которые откажутся от внедрения ИИ-систем. Но как бы там ни было, решения на искусственного интеллекта будет все более востребованными, а значит, востребованными будут и разработчики». ***(Аналитики Gartner назвали 10 технологий, которые изменят наше будущее // Фокус (https://focus.ua/digital/496313-analitiki-gartner-nazvali-10-tehnologiy-kotorye-izmenyat-nashe-budushchee). 26.10.2021).***

***

«Исследование компании Trend Micro, что глобальные организации используют в среднем 29 решений для мониторинга безопасности. Это усложняет работу центров управления кибербезопасностью (SOC) по приоритизации предупреждений и эффективному управлению рисками. Более того, специалисты, работающие в организациях сболее чем10тыс. сотрудников, имеют дело в среднем с 45 инструментами для мониторинга.

Глобальное независимое исследование Security Operations On The Backfoot: How poor tooling is taking its toll on security analysts («Трудности кибербезопасности: Как неправильный подбор инструментов затрудняет работу специалистов») (PDF, EN) основано на интервью с 2303 лицами, ответственными за принятие решений в области ИТ-безопасности в 21 стране. В их число входят руководители, которые управляют командами SOC (85%), и те, кто управляет SecOps из внутренней группы ИТ-безопасности (15%). Все респонденты представляли компании с более чем 250 сотрудниками.

Половина (51%) респондентов заявили, что они фактически не используют многие из имеющихся в наличии инструментов по таким причинам:

отсутствие интеграции (42%);

нехватка квалифицированных специалистов (39%);

сложности в управлении инструментами (38%);

устаревание инструментов (37%);

отсутствие доверия к ним (20%).

Потенциальный урон в результате подобных проблем может быть высок: респонденты заявили, что в среднем их организации могут потерять свыше 235 тыс.долл., если из-за какого-либо инцидента будет нарушен регламент GDPR.

«Чрезмерное количество инструментов– все более распространенное явление в глобальных организациях любого размера. Тем не менее, когда дело доходит до обнаружения инцидентов и реагирования, расходы, иногда неподтвержденные, продолжают расти»,– объясняет Бхарат Мистри (Bharat Mistry), технический директор Trend Micro в Великобритании.

Исследование также показало, что 92% респондентов рассматривали возможность аутсорсинга обнаружения и реагирования с использованием управляемых услуг. Подобные решения обычно помогают возместить нехватку

внутренних ресурсов и обеспечить компанию единой унифицированной платформой для улучшения реагирования на инциденты.

«Несмотря нато, что организации вынуждены платить за лицензирование и обслуживание, команды SOC все чаще подвергаются стрессу, пытаясь управлять несколькими решениями одновременно. Отсутствие возможности приоритизировать предупреждения может привести к потере данных. Неудивительно, что многие организации предпочитают схему «центр управления безопасностью как услуга» (SOC-as-a-Service)»,– добавляет Бхарат Мистри». ***(Организации используют десятки инструментов кибербезопасности, что снижает эффективность управления рисками //Компьютерное Обозрение (https://ko.com.ua/organizacii_ispolzuyut_desyatki_instrumentov_kiberbezopasnosti_chto_snizhaet_jeffektivnost_upravleniya_riskami_139034). 13.10.2021).***

***

«Почти в трети компаний (31%) возникают вопросы, как защищать корпоративные данные на личных устройствах сотрудников, 29% испытывают трудности с обеспечением безопасности в связи с тем, что на одного сотрудника приходится несколько рабочих устройств, 27% называют проблемой недостаток цифровой грамотности среди сотрудников. Каждая четвертая компания сталкивается с тем, что сотрудники не соблюдают правила информационной безопасности при ведении переписки по электронной почте, а каждая пятая (22%) — с тем, что они не всегда используют собственный отдельный логин и пароль для входа в системы. Для 19% компаний одна из основных проблем в области ИБ — обеспечить соответствие своих IT-систем законодательным требованиям.

Опрос показал, что представители небольших компаний нуждаются в советах по кибербезопасности. Так, 42% хотели бы понимать, как бороться с утечками, 29% — как избежать атак программ-вымогателей и что делать, если они произошли, 26% — как обеспечивать безопасность облачных сервисов.

В то же время более четверти (27%) опрошенных не уверены в том, что существует реальный риск пострадать от кибератаки или столкнуться с потерей либо кражей ценных данных. Однако, по данным другого исследования, для МСБ-компаний России, столкнувшихся с утечками данных, общий годовой ущерб от такого рода происшествий составляет $32 тыс США.

«У каждой организации независимо от ее размера и отрасли есть ценная для злоумышленников информация, например, интеллектуальная собственность, финансовые или персональные данные. Нередко маленькие компании являются частью цепочки поставок, и злоумышленники стремятся использовать доступ к их сетям в рамках многоэтапных операций по проникновению в сети более крупных организаций. Но бизнесу угрожают не только целевые атаки, очень часто заражение происходит из-за массовых рассылок вредоносного ПО, нацеленных на случайных жертв. А поскольку обычно небольшие компании защищены хуже, чем корпорации, это делает их легкодоступной мишенью», — отмечает Андрей Данкевич, эксперт «Лаборатории Касперского» по киберзащите малого и среднего бизнеса…». ***(«Лаборатория Касперского» выяснила, с какими проблемами***

кибербезопасности сталкивается малый и средний бизнес в России // CNews (https://www.cnews.ru/news/line/2021-10-21_laboratoriya_kasperskogo). 21.10.2021).

***

«Москва и Вашингтон внесли на рассмотрение Генеральной Ассамблеи ООН совместную резолюцию об ответственном поведении государств в киберпространстве.

Как сообщает «Коммерсантъ», это событие стало неожиданным с учётом длительного соперничества двух держав, продвигавших в ООН конкурирующие переговорные механизмы по кибербезопасности. Тем не менее, Москва и Вашингтон рассчитывают, что объединение усилий позволит сделать процесс внедрения добровольных правил ответственного поведения государств в сети более эффективным. При этом из резолюции следует, что в будущем речь может пойти и об обязательных нормах.

Голосование по документу «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности и поощрение ответственного поведения государств в сфере использования информационно-коммуникационных технологий» запланировано в Первом комитете Генассамблеи на ноябрь, после чего, уже в декабре, его вынесут на общее голосование. Выработка ответственных правил поведения государств в информационном пространстве на площадке ООН происходила в рамках двух механизмов.

Это американская Группа правительственных экспертов (включает 25 стран) ироссийская Рабочая группа открытого состава (открыта для всех государств). Год назад Россия и США внесли на рассмотрение Генассамблеи ООН две конкурирующие резолюции, и, хотя в итоге обе они были приняты, это создавало пространство для соперничества и закулисных интриг, а также оказывало негативное влияние на эффективность обоих механизмов.

Эксперты называют разработку двумя странами совместной резолюции настоящим «дипломатическим прорывом». Во многом это стало возможным благодаря достигнутым в июне договоренностям президентов РФ и США Владимира Путина и Джо Байдена о возобновлении взаимодействия в сфере кибербезопасности. Из документа следует, что работа продолжится в российском формате.

В резолюции подчёркивается, что все государства заинтересованы в поощрении использования информационно-коммуникационных технологий в мирных целях, а также в предотвращении конфликтов, возникающих в результате их использования. В то же время в ней сказано, что ряд государств занимаются наращиванием потенциала для военных целей, а использование этих технологий в будущих конфликтах становится все более вероятным.

Особую обеспокоенность у составителей документа вызывают возможные злонамеренные действия с использованием информационно-коммуникационных технологий, направленные против объектов критически важной инфраструктуры. В России «критически важными» (на основании принятого в 2017 году федерального закона) считаются 13 секторов, включая банковскую сферу, предприятия оборонной промышленности, объекты транспорта, здравоохранения и другие».

(Александр Пономарёв. Россия и США разработали совместную резолюцию по кибербезопасности // Популярная Механика (https://www.popmech.ru/technologies/news-761143-rossiya-i-ssha-razrabotali-sovmestnuyu-rezolyuciyu-po-kiberbezopasnosti/). 18.10.2021).

***

«ИТ-компания КРОК совместно с Phisman провели исследование по киберосознанности и ее эффективности в борьбе с фишинговыми атаками и методами социальной инженерии. Выводы сделаны на основе данных 287 организаций Enterprise-сегмента, среднего и малого бизнеса.

Мошенники постоянно придумывают новые схемы, используя методы социальной инженерии, с помощью которых заставляют сотрудников совершить выгодные злоумышленнику действия. Наиболее популярный инструмент среди киберпреступников – фишинг, который заключается в отправке специально подготовленных писем (сообщений), которые содержат либо вредоносные файлы, маскирующиеся под вполне безопасные, либо ссылки на фейковые сайты, созданные злоумышленниками.

«Бумажные меры по информированию сотрудников компаний, как правило, не эффективны. Согласно статистике 80% сотрудников реагируют на фишинговые письма, а порядка 25% открывают подозрительные ссылки, либо запускают вредоносный файл. Бороться с киберпреступлениями можно с помощью киберосознанности сотрудников, которую развивают специальные системы повышения осведомленности Security Awareness, помогающие формировать осознанное поведение в интернете», – отмечает генеральный директор компании Phisman Алексей Горелкин.

Среди компаний, использующих данные системы 91% респондентов отмечают, что используют киберосозаннность для снижения рисков кибербезопасности, связанных с поведением пользователей, 64% – для изменения поведения сотрудников в интернете, 61% - для выполнения нормативных актов, а 55% для соблюдения внутренних политик.

«Основные направления, на которые стоит обращать внимание при формировании навыков киберосознаности: безопасность электронной почты/фишинг, управление паролями, конфиденциальность данных, веб-безопасность и офисная безопасность. Навыки пользователей необходимо закреплять практически, проводя регулярные киберобучения и тестирования для закрепления навыков у старых пользователей и их выработки у новых», – подчеркивает эксперт по информационной безопасности IT-компании КРОК Анастасия Федорова.

Чтобы снизить риск кибератак, компании должны постоянно совершенствовать системы информационной безопасности, а также правильно мотивировать и обучать работников, чтобы снизить число непреднамеренных инцидентов с их стороны». ***(80% сотрудников попадаются на фишинг // ООО «ИКС-МЕДИА» (https://www.iksmedia.ru/news/5859139-80-sotrudnikov-popadayutsya-na-fish.html). 28.10.2021).***

***

«Комитет Сената по внутренней безопасности и делам правительства в среду одобрил закон, требующий от многих компаний сообщать как о серьезных нарушениях кибербезопасности, так и о платежах, связанных с атаками программ-вымогателей.

Комитет одобрил Закон об отчетности о киберинцидентах, официально представленный на прошлой неделе председателем комитета…

Законопроект потребует от владельцев и операторов критически важных инфраструктурных групп сообщать о киберинцидентах в Агентство по кибербезопасности и безопасности инфраструктуры (CISA) в течение 72 часов. Это также потребует от критически важных инфраструктурных групп, некоммерческих организаций и большинства средних и крупных предприятий в течение 24 часов сообщать о платежах, связанных с атаками программ-вымогателей.

Этот закон является одним из нескольких попыток укрепить протоколы кибербезопасности после ряда крупных атак как на правительство, так и на частный сектор в последние месяцы, включая атаки программ-вымогателей на Colonial Pipeline, производителя мяса JBS USA и ИТ-группу Kaseya…

Хотя большинство членов комитета поддержали идею введения обязательной отчетности о нарушениях для критических групп, во время разметки в среду разгорелись дебаты вокруг коротких сроков и требования о том, чтобы частные малые предприятия сообщали о платежах программ-вымогателей для восстановления доступа к своим сетям.

Скотт предложил поправку, которая была отклонена комитетом, которая сузила бы фокус законопроекта до требования, чтобы группы критически важной инфраструктуры сообщали о платежах, связанных с программами-вымогателями.

«Я поддерживаю намерение этого законопроекта, но я действительно считаю, что еще один обременительный правительственный мандат на наши малые предприятия не является ответом», - сказал Скотт.

Сенатор Джеймс Ланкфорд выразил озабоченность по поводу того, что в сроках законопроекта есть «дыры»…

В то время как общий законопроект был принят, Питерс и Портман пообещали в ближайшие недели принять во внимание отзывы обеих сторон о том, как его улучшить, прежде чем они поставят перед собой цель позже включить его в сенатский вариант Закона о полномочиях на национальную оборону 2022 года (NDAA)…

В прошлом месяце Палата представителей приняла свою версию NDAA 2022 года, включая двухпартийный закон от лидеров Комитета внутренней безопасности Палаты представителей, который запрещает CISA требовать от организаций сообщать о киберинцидентах раньше, чем через 72 часа после их возникновения.

Комитет по внутренней безопасности Сената в среду также одобрил отдельный законодательный акт, также спонсируемый Питерсом и Портманом, чтобы обновить Федеральный закон о модернизации информационной

безопасности и предпринять шаги по уточнению требований к отчетности для федеральных агентств в случае их успешной атаки хакерами.

В то время как комиссия по предыдущему законодательству разделилась, второй законопроект был единогласно одобрен голосовым голосованием». ***(MAGGIE MILLER. Bill requiring companies report cyber incidents moves forward in the Senate // The Hill (https://thehill.com/policy/cybersecurity/575627-bill-requiring-organization-to-report-cyber-incidents-moves-forward-in). 06.10.2021).***

***

«Конгресс работает над направлением ресурсов на укрепление инфраструктуры кибербезопасности государственных и местных органов власти после того, как пандемия COVID-19 вынудила муниципалитеты перенести многие важные операции на стареющие и уязвимые онлайн-источники.

В двухпартийный законопроект об инфраструктуре, принятый Сенатом в августе, включен 1 миллиард долларов для укрепления государственной кибербезопасности после года, в течение которого хакеры в полной мере использовали преимущества систем таргетинга. Чиновники говорят, что уроки были извлечены.

«Кибербезопасность была вопросом №1 и приоритетом для государственных руководителей по информационным технологиям. Это не изменилось, но, безусловно, пандемия усугубила многое с точки зрения финансирования, с точки зрения ресурсов и того, как обеспечить поддержание корпоративного уровня кибербезопасности, делая это виртуально», - Мэтт Пинкус, директор правительственных дел в Национальной ассоциации государственных директоров по информационным технологиям, сообщил The Hill.

Государства и местные органы власти уже сталкивались с киберугрозами еще до пандемии, особенно когда дело касалось атак программ-вымогателей. В 2019 году серия скоординированных атак поразила почти два десятка городских властей Техаса, а атаки на крупные города в том же году, включая Балтимор, Атланту и Новый Орлеан, нанесли ущерб на миллионы долларов и ослабили городские службы.

В начале 2020 года, когда разразилась пандемия, штаты и населенные пункты, уже подверженные таким атакам, были вынуждены перевести свои услуги в онлайн с уведомлением всего за несколько дней, что вынудило многих изначально отдавать предпочтение резидентным услугам, а не кибербезопасности, что сделало системы открытыми для уязвимостей.

Среди них рост числа случаев мошенничества в связи с безработицей и другими пособиями по пандемии, а также рост числа атак программ-вымогателей. Пинкус сказал The Hill, что 60% руководителей информационных служб штата заявили, что вымогатели - это их «нет».1 проблема кибербезопасности».

«Конечно, это никуда не делось, и, во всяком случае, COVID стал хорошим тестом для многих государств с точки зрения их позиции в киберпространстве», - сказал Пинкус.

Майкл Уотсон, главный специалист по информационной безопасности Агентства информационных технологий штата Вирджиния, заявил на прошлой неделе, что его офис находится в «фазе очистки» после того, как в начале пандемии бросился на цифровые услуги.

«Нам нужно было немного привыкнуть к тому, что какое-то время там было некомфортно, и мы искали способы попытаться ограничить наш риск везде, где это возможно», - сказал Уотсон на панели на Billington CyberSecurity Summit. «Сейчас мы как бы немного поработаем, чтобы вернуть это обратно и выяснить, какой должна быть наша позиция риска в целом».

Не только правительства штатов и местные органы власти стремятся защитить свои сети.

Средства, выделенные в двухпартийном законопроекте Сената, являются частью Закона о повышении кибербезопасности на уровне штатов и на местном уровне, который предусматривает создание программы грантов в Министерстве внутренней безопасности для предоставления финансирования правительственным учреждениям в течение четырех лет, при этом четверть средств будет направлена на другие цели. уязвимые сельские сообщества.

Мера Сената аналогична законопроекту, внесенному в Палату представителей Конгресса США. Иветт Кларк, председатель группы по кибербезопасности Комитета внутренней безопасности Палаты представителей, которая также предоставит миллионы финансовых средств для финансирования кибербезопасности правительствам штатов и местным властям. Законопроект был принят Палатой представителей в июле, и на прошлой неделе Кларк пообещал продолжать добиваться прогресса в законодательстве и других законопроектах, связанных с кибербезопасностью.

«Доказательства очевидны, наши противники знают о недостатках киберпространства Америки и готовы ими воспользоваться. Они будут продолжать бороться с этими недостатками, только если мы не устраним их немедленно», - сказал Кларк на виртуальном мероприятии, организованном Национальным альянсом кибербезопасности.

Осведомленность об угрозах кибербезопасности резко возросла на федеральном уровне после серии крупных атак на правительственные учреждения и крупные компании, такие как Colonial Pipeline и производителя мяса JBS USA, в последние месяцы, обе из которых ненадолго прервали обслуживание потребителей.

Такая осведомленность может быть благом для властей штата и местных властей, а большее внимание может привлечь больше ресурсов.

«Это в интересах всех, - сказал Пинкус о безопасности.«Я думаю, что за последние полтора года было больше признания, чем было раньше, так что это положительный момент». ***(MAGGIE MILLER. Congress looks to strengthen government's aging cyber infrastructure // The Hill (https://thehill.com/policy/cybersecurity/576189-congress-looks-to-strengthen-governments-aging-cyber-infrastructure). 12.10.2021).***

***

«Законодатели США ввели закон, требующий сообщать о выплатах выкупа в течение 48 часов с момента транзакции. Законопроект, выдвинутый сенатором Элизабет Уоррен, штат Массачусетс, и член палаты представителей Дебора Росс, DN.C., потребует от Министерства внутренней безопасности создать добровольный веб-сайт для регистрации выплат выкупа и поручить DHS провести всестороннее исследование. корреляции между программами-вымогателями и криптовалютой.

В заявлении во вторник законодатели заявили, что в случае его принятия Закон о раскрытии информации о программах-вымогателях предоставит важные данные, которые «укрепят наше понимание того, как работают киберпреступные предприятия, и составят более полное представление об угрозе программ-вымогателей».

Уоррен добавил: «Число атак программ-вымогателей стремительно растет, но у нас нет критически важных данных для борьбы с киберпреступниками. В моем счете с конгрессменом Росс будут установлены требования к раскрытию информации при уплате выкупа и позволят нам узнать, сколько денег киберпреступники выкачивают у американских организаций для финансирования преступных предприятий. - и помогите нам пойти за ними».

Законопроект:

Требовать от жертв программ-вымогателей (за исключением физических лиц) раскрывать информацию о выплатах выкупа не позднее, чем через 48 часов после даты выплаты;

Требовать от жертв сообщать о затребованной и уплаченной сумме, типе используемой валюты и любой известной информации о субъектах угрозы;

Требовать от DHS обнародовать информацию, раскрытую в течение предыдущего года, за исключением идентифицирующей информации;

Требовать от DHS создания веб-сайта, через который люди могут добровольно сообщать об уплате выкупа;

Поручите секретарю DHS провести исследование общих черт между атаками программ-вымогателей и криптовалютами и предоставить рекомендации по защите ИТ-систем.

Соглашаясь с положениями, Меган Стифель, которая была директором по киберполитике в Совете национальной безопасности при администрации Обамы, говорит ISMG: «Прошло время требовать отчетности о платежах... Чтобы начать сокращать количество жертв, нам нужна информация об этих инцидентах, а не просто традиционный обмен информацией об индикаторах киберугроз... но информация о деталях платежа - банкноте, кошельке, сумме и т. д.»

Стифель, который в настоящее время является исполнительным директором по Северной и Южной Америке в Global Cyber Alliance, добавляет: «Без такой информации мы не знаем всего масштаба проблемы и серьезно ограничены в наших возможностях по разработке политики и юридических мер реагирования на Лучше сразись с этим».

«Угроза нашей национальной безопасности»

Представитель Росс сказал о законопроекте: «Атаки программ-вымогателей становятся все более распространенными с каждым годом, угрожая нашей

национальной безопасности, экономике и критически важной инфраструктуре. К сожалению, поскольку от жертв не требуется сообщать об атаках или платежах федеральным властям, нам не хватает критически важных данных. чтобы понять эти киберпреступные предприятия и противостоять этим вторжениям ».

Росс сказал, что закон «введет важные требования к отчетности» и что США «не могут продолжать бороться с атаками программ-вымогателей, связав одну руку за спиной».

Уоррен и Росс привели данные фирмы SonicWall, занимающейся кибербезопасностью, согласно которой количество атак программ-вымогателей выросло на 62% во всем мире в период с 2019 по 2020 год и на 158% в Северной Америке. В 2020 году ФБР получило около 2500 жалоб на вымогателей, что на 20% больше, чем в прошлом году, с заявленными потерями в размере 29 миллионов долларов.

Компания Chainalysis, занимающаяся аналитикой блокчейнов, указала, что жертвы по всему миру заплатили почти 350 миллионов долларов в качестве выкупа в 2020 году, что на 300% больше, чем в предыдущем году. По данным компании, средний размер выплат увеличился на 170% и составил 312 000 долларов.

Аналогичный закон был принят на прошлой неделе лидерами сенатского комитета по внутренней безопасности и делам правительства. Законопроект, выдвинутый председателем комитета Гэри Петерсом, штат Мичиган, и высокопоставленным членом Робом Портманом, штат Огайо, потребует от определенных организаций сообщать о выплате выкупа в течение 24 часов с момента доставки. Кроме того, владельцы и операторы критически важной инфраструктуры должны будут сообщать об инцидентах безопасности в Агентство по кибербезопасности и безопасности инфраструктуры в течение 72 часов с момента обнаружения.

Законопроект Питерса и Портмана был принят комитетом голосовым голосованием в среду.

Нет консенсуса среди экспертов

Стифель из Global Cyber Alliance говорит: «Общие требования [здесь] необходимы и в целом движутся в правильном направлении. Я предвижу сопротивление отрасли, ссылаясь на бремя, особенно в условиях инцидента, но важно помнить, как многое из этого можно предотвратить, в первую очередь, следуя известным передовым методам кибербезопасности».

Скотт Шакелфорд, директор программы кибербезопасности и управления интернетом в Университете Индианы, говорит: «Этот закон, если он будет принят, прольет некоторый свет на очень темный рынок и, вероятно, также в первую очередь лишит фирмы стимулов платить выкуп. из-за боязни разглашения».

Тем не менее, похоже, нет консенсуса по этим мандатам.

Фон Велч, заместитель вице-президента по информационной безопасности и исполнительный директор по инновациям в области кибербезопасности в Университете Индианы, сказал ISMG: «Требование представить отчет в течение 48 часов очень интересно. Это подразумевает некоторую оперативную срочность… … И я считаю, что это должно быть оправдано - особенно в этом случае, когда жертва

все еще находится в процессе восстановления и забирает ключевые ресурсы из этого восстановления ».

Тим Уэйд, бывший технический менеджер по сетям и безопасности в ВВС США, а в настоящее время технический директор охранной фирмы Vectra AI, говорит: «Я сомневаюсь в благоразумности принудительного принудительного раскрытия информации частными лицами, которые считают, что такое раскрытие не в их лучших интересах. интересы или наилучшие интересы заинтересованных сторон и акционеров».

Другое законодательство о кибербезопасности

В другом месте на этой неделе высокопоставленный член Комитета внутренней безопасности Палаты представителей Джон Катко, штат Вирджиния, и член палаты представителей Эбигейл Спанбергер, штат Вирджиния,представили законопроект, который поможет правительству определить «системно важную критическую инфраструктуру».В случае принятия CISA получит право определять группы как «системно важные» и работать с отраслевыми агентствами по управлению рисками для улучшения программ кибербезопасности.

А в понедельник сенатор Петерс и Портман представили еще один законопроект, который внесет поправки в Федеральный закон о модернизации информационной безопасности 2014 года и налагает требования к отчетности об инцидентах для федеральных агентств.

Законопроект также подтвердит роль CISA в качестве ведущей организации после кибератак и потребует от Управления управления и бюджета предоставить рекомендации по оптимальному финансированию кибербезопасности для федеральных агентств». ***(Dan Gunderman. New Bill Would Require Ransom Disclosure Within 48 Hours // Information Security Media Group, Corp. (https://www.govinfosecurity.com/new-bill-would-require-ransom-disclosure-within-48-hours-a-17689). 07.10.2021).***

***

«В письме Конгресса, направленном в пятницу главам четырех федеральных агентств, говорилось, что администрации Байдена срочно необходимо продолжить борьбу с программами-вымогателями. Это включает в себя особое внимание к инфраструктуре криптовалюты, которая делает возможной эти кибератаки, говорят четыре депутата-демократа.

Письмо, написанное сенатором Эдом Марки, штат Массачусетс, и Шелдоном Уайтхаусом, доктор медицинских наук, и представителями Джима Ланжевена, доктор медицинских наук, и Тедом Лиу, штат Калифорния, адресовано руководителям отделов. Государства, национальной безопасности, юстиции и казначейства - Энтони Блинкен, Алехандро Майоркас, Меррик Гарланд и Джанет Йеллен соответственно - отмечая: «Мы настоятельно призываем [департаменты] использовать все доступные варианты для защиты американских сообществ и инфраструктуры от растущей угрозы программ-вымогателей.»

В письме законодатели призывают к «более тесной координации» между ведомствами, чтобы рассмотреть роль криптовалюты в содействии атакам. В 2021 году произошла волна громких атак, включая атаки на колониальный

трубопроводы временную остановку поставок топлива на восточное побережье; производитель мяса JBS USA; и поставщик управляемых услуг Kaseya, который затронул около 1500 дочерних организаций.

Четыре отдела не сразу ответили на запрос Information Security Media Group о комментариях.

«Сложная, опасная и дорогая проблема»

В своем письме законодатели называют программы-вымогатели «все более сложной, опасной и дорогостоящей проблемой для правительства, частных корпораций и малого бизнеса».Они ссылаются на данные за 2020 год из Центра жалоб на интернет-преступления ФБР (IC3), который получил почти 2500 сообщений о вымогательстве с соответствующими потерями на сумму 29,1 миллиона долларов. По словам законодателей, с 2019 года количество зарегистрированных инцидентов увеличилось на 20%, а сумма выкупа, требуемая хакерами, увеличилась на 225%. Что еще хуже, добавляют они, от 70% до 75% атак программ-вымогателей остаются незарегистрированными.

Марки, Уайтхаус, Ланжевен и Лиу говорят, что этот рост «угрожает национальной безопасности», поскольку злоумышленники могут нарушить работу критически важной инфраструктуры и переместить конфиденциальные данные.

Роль криптовалюты

Законодатели говорят, что криптовалюта «способствовала этому взрывному росту», «предлагая простые, быстрые и трудные для отслеживания методы отмывания незаконных доходов».Они призывают к усилению соблюдения существующих законов о борьбе с отмыванием денег и финансовых преступлениях, чтобы предотвратить атаки программ-вымогателей и помочь в восстановлении выкупа в криптовалюте.

По их словам, эта работа будет опираться на международное партнерство: «Многие атаки с использованием программ-вымогателей происходят в юрисдикциях, находящихся за пределами досягаемости внутренних правоохранительных органов США, что требует от агентств США работать с иностранными партнерами и биржами криптовалюты, чтобы захватить платежи программ-вымогателей или другие связанные активы.

Злоумышленники, продолжают законодатели, проживают в основном в России, Китае и Северной Корее, которые «являются странами, которые активно или негласно поддерживали атаки программ-вымогателей против США и препятствовали усилиям США по выводу выкупа за криптовалюту».

Комментируя пятничное письмо, Уильям Каллахан, бывший специальный агент, отвечающий за Управление по борьбе с наркотиками, сказал ISMG: «Федеральные правоохранительные органы расследуют использование криптовалюты в незаконных целях с первых дней расследования Шелкового пути, почти 10»

'Признайте срочность'

Законодатели высоко оценивают недавние усилия Белого дома «признать безотлагательность» угрозы вымогателей, ссылаясь на усилия Министерства юстиции вернуть более 2,7 миллиона долларов в криптовалюте после атаки на Colonial Pipeline. Они также хвалят санкции Министерства финансов против Suex,

российской криптовалютной биржи, которая якобы помогает участникам программ-вымогателей.

На прошлой неделе Министерство юстиции также объявило, что создаст Национальную группу по борьбе с криптовалютами, или NCET, для отслеживания и восстановления активов, утраченных в результате мошенничества и вымогательства, включая криптовалютные платежи группам программ-вымогателей.

«Мы считаем, что расширение усилий по изъятию выкупа за криптовалюту и увеличение затрат, связанных с уплатой выкупа, безусловно, может помочь предотвратить атаки программ-вымогателей, снизив их прибыльность и изменив стимулы злоумышленников», - отмечают законодатели.

И Каллахан, в настоящее время директор по правительственным и стратегическим вопросам компании Blockchain Intelligence Group, добавляет: «Незаконное использование криптовалюты требует не только общегосударственного подхода, но и общегосударственного подхода, как и в случае с наркотиками. незаконного оборота наркотиков для борьбы с транснациональными преступными организациями, занимающимися незаконным оборотом наркотиков».

Каллахан считает, что эти усилия потребуют дополнительного финансирования от Конгресса.

Нил Джонс, пропагандист кибербезопасности компании Egnyte, говорит ISMG, что «с ростом количества атак с использованием программ-вымогателей и увеличивающимися выплатами вымогателей становится ясно, что нынешние подходы к борьбе с программами-вымогателями просто не работают».

Джонс высоко оценивает недавние усилия Конгресса по введению законодательства об отчетности, которое предоставило бы правительству США механизм для оценки и использования критически важных данных о кибератаках. По его словам, это, среди прочего, также может помочь переломить ситуацию.

Тайлер Фаррар, бывший офицер службы шифрования ВМС США, а в настоящее время - директор по информационной безопасности охранной фирмы Exabeam, также говорит, что для предотвращения этих атак с криптоблокировкой и защиты критически важной инфраструктуры потребуется «сообщать о рисках и атаках в режиме реального времени».Это курс, который Конгресс начал проводить в последние недели…». ***(Dan Gunderman. Democratic Lawmakers Urge Agencies to Act on Ransomware // Information Security Media Group, Corp. (https://www.govinfosecurity.com/democratic-lawmakers-urge-agencies-to-act-on-ransomware-a-17716). 11.10.2021).***

***

«Йонатан Стрим-Амит, технический директор и соучредитель Cybereason, дает представление о том, почему кибербезопасность является национальной безопасностью для всех стран.

После нескольких месяцев эскалации кибератак, которые затронули поставщиков критически важной инфраструктуры, цепочку поставок продуктов питания и даже нарушили распространение вакцин против COVID-19 и больницы,

которые изо всех сил пытались лечить пациентов с COVID, пора подвести черту на песке. Одна вещь, которая становится все более очевидной по мере того, как стираются границы для кибератак, - это то, что кибербезопасность - это национальная безопасность для всех стран.

Руководители 24 ведущих технологических компаний, поставщиков критически важной инфраструктуры, банков, страховых компаний и образовательных учреждений недавно встретились в Белом доме с президентом Байденоми ведущими советниками. После встречи Белый дом озвучил ряд смелых инициатив.

Например, Национальный институт стандартов и технологий (NIST) будет сотрудничать с партнерами из частного сектора в разработке основы для повышения безопасности и целостности цепочки поставок. Они также официально расширили Инициативу по кибербезопасности промышленных систем контроля за пределы электроэнергетики, включив в нее трубопроводы природного газа.

Крупные технологические компании согласились участвовать в различных инициативах. Apple улучшит безопасность цепочки поставок, Google расширит программы нулевого доверия, Microsoft активизирует усилия по интеграции кибербезопасности в системы, а Amazon сделает свои тренинги по внутренней безопасности доступными для общественности бесплатно.

Образование и обучение

Однако одним из самых обнадеживающих аспектов встречи был упор на образование и обучение. Руководители Code.org, Girls Who Code и Техасского университета объявили о программах по обучению студентов основам кибербезопасности, расширению существующих и разработке новых краткосрочных навыков в областях, связанных с киберпространством, чтобы помочь устранить пробел в навыках кибербезопасности и предоставить стипендии и возможности карьерного роста более доступны и доступны для недостаточно представленных групп.

…нарушения в SolarWinds, за которым следуют атаки против уязвимых серверов Microsoft Exchange, и массированные атаки вымогателей против Colonial PipelineиJBS Meat Packing показали, что государственный и частный сектор должен работать вместе, чтобы остановить киберугрозы. Пора перестать полагаться на устаревшие технологии, разработанные для защиты от угроз 20-летней давности, и пора инвестировать в передовые решения по предотвращению, обнаружению и обеспечению устойчивости.

Кибератаки национального государства

Мы также должны бороться с эскалацией кибершпионажа и кибератак на национальном уровне путем введения финансового регулирования биткойнов и других криптовалют для борьбы с программами-вымогателями и ограничения возможности монетизации киберпреступности, а также законодательства, обновляющего штрафы, связанные с киберпреступлениями, сотрудничать с нашими союзниками обновить договоры об экстрадиции киберпреступников и наладить глобальное сотрудничество в борьбе с ними.

После того, как Соединенные Штаты и Европейский союз осудили Китай за атаку Microsoft Exchange Server, это стало тревожным сигналом для других

противников, являющихся национальными государствами, о том, что в будущем кибератаки на глобальные цели будут стоить дорого. Требуется больше осуждения наряду с установлением четких правил ведения наступательных операций.

Мы сталкиваемся с постоянно развивающимся и расширяющимся ландшафтом угроз и все более изощренными атаками, стирающими границы между кибератаками и кибершпионажем. Потребуются совместные усилия многих стран, поставщиков из частного и государственного секторов, а также правительственных агентств для обмена разведданными и знаниями, чтобы улучшить нашу способность бороться с нарастающей волной продвинутой киберпреступности». ***(Cybersecurity is national security for all nations // Open Access Government (https://www.openaccessgovernment.org/cybersecurity-is-national-security-for-all-nations/122414/). 14.10.2021).***

***

«В напряженный день Конгресса, посвященный законодательству о кибербезопасности, Палата представителей США приняла в среду несколько законопроектов, направленных как на безопасность цепочки поставок программного обеспечения, так и на безопасность телекоммуникационных систем.

Закон Министерства внутренней безопасности об управлении рисками в цепочке поставок программного обеспечения от 2021 года, спонсируемый членом палаты представителей Ричи Торрес, штат Нью-Йорк, вице-председателем Комитета национальной безопасности Палаты представителей, потребует от заместителя министра DHS по управлению издать ведомственные инструкции, требующие от подрядчиков DHS. предоставлять ведомости материалов по программному обеспечению или SBOM, в которых указывается происхождение каждого компонента программного обеспечения, предоставленного DHS.

Он прошел в нижнюю палату в среду почти единогласно - 412 голосами против 2.

«DHS должно подавать пример»

Этот законопроект, по словам Торреса, поможет избежать инцидентов, таких как атака SolarWinds, которую предположительно совершила поддерживаемая Россией группа Nobelium. В нем злоумышленники организовали атаку на цепочку поставок, используя программное обеспечение Orion SolarWinds, взломав около 100 организаций по всему миру, а также девять федеральных агентств, включая DHS. По данным Microsoft, злоумышленник, стоящий за многомесячной шпионской кампанией, специально нацелился на государственные учреждения, занимающиеся внешней политикой.

В своем заявлении Торрес сказал: «Крайне важно, чтобы DHS обладало способностью защищать свои собственные сети и повышать осведомленность об информационных и коммуникационных технологиях или услугах, которые оно покупает. Как федеральный лидер в сфере кибербезопасности, DHS должно подавать пример путем модернизации способов защиты своих сетей».

Закон основан на указе президента Джо Байдена от мая 2021 года, направленном на комплексное повышение безопасности цепочки поставок

федерального правительства для обеспечения прозрачности и эффективного управления потенциальными угрозами.

«Предотвращать, обнаруживать и реагировать»

«Безопасность и целостность программного обеспечения, приобретенного DHS, является неотъемлемой частью национальной безопасности. Мой законопроект обеспечит доступ департаменту для предотвращения, обнаружения и реагирования на будущие кибератаки.… Я призываю своих коллег в Сенате поднять и принять это важный законодательный акт», - сказал Торрес.

Джейк Уильямс, бывший член элитной хакерской группы Агентства национальной безопасности, сказал ISMG: «Этот закон закладывает основу для внедрения спецификаций программного обеспечения не только в федеральном правительстве, но и во всей ИТ-индустрии».

Ссылаясь на 180-дневный крайний срок для выполнения требований и проблемы со сторонними компонентами, Уильямс, соучредитель и технический директор охранной фирмы BreachQuest, добавляет: «Хотя это определенно шаг в правильном направлении для кибербезопасности, первоначальное соответствие будет сложным и дорогостоящим. Я ожидаю, что мы будем в ужасе, узнав, что некоторые небезопасные компоненты бессознательно встроены в широко используемое корпоративное программное обеспечение».

Нил Джонс, проповедник кибербезопасности компании Egnyte, говорит: «Законопроект представителя Торреса улучшит положение [DHS] для выявления потенциальных уязвимостей и даст больше возможностей задавать вопросы до того, как произойдет нарушение».

По сообщениям Associated Press, в ходе кампании SolarWinds злоумышленники получили доступ к учетным записям электронной почты высших руководителей DHS, в том числе бывшего исполняющего обязанности секретаря DHS Чада Вольфа.

В апреле администрация Байдена официально наложила санкции на Россию за шпионскую операцию. Администрация также наложила санкции на более 30 российских компаний и частных лиц, обвиняемых в предоставлении инструментов, инфраструктуры и технологий для различных кибероперацией, связанных с федеральными выборами, и выслала 10 российских дипломатов из США.

Телеком Фокус

Палата представителей также приняла двухпартийный законопроект, спонсируемый в среду представителем меньшинства Палаты представителей Стива Скализа, Род-Луи, и членом палаты представителей Анны Эшу, Калифорния. Законопроект запрещает Федеральной комиссии по связи проверять или выдавать лицензии на новое оборудование компаниям, включенным в«Список покрываемого оборудования или услуг»Федеральной комиссии по связи, которые якобы представляют угрозу национальной безопасности. Мера принята 420 голосами против 4.

Закон о безопасном оборудовании предотвратит дальнейшее использование и продажу оборудования китайских фирм, таких как Huawei, ZTE, Hytera, Hikvision и Dahua, в США.

Huawei ранее опровергала утверждения о том, что представляет угрозу национальной безопасности США.

И Конгресс, и администрация Трампа ранее предпринимали шаги, чтобы заблокировать доступ организаций, которые они считали опасными, на рынок США.

«[Законопроект] не позволит Китаю проникнуть в американские телекоммуникационные сети и поставить под угрозу безопасность и национальную безопасность американского народа при отправке данных через Интернет», - говорится в заявлении Скализ.

«[Законопроект] является сильным сигналом коммунистической партии Китая о том, что Америка привержена обеспечению безопасности наших сетей и защите частной жизни и безопасности наших граждан», - добавил он.

Сенатор Марко Рубио, штат Флорида, и Эд Марки, штат Массачусетс, представили аналогичный законв Сенате в мае, который еще не принят.

«Ограничивая использование сетевых технологий, производимых китайскими государственными фирмами, законопроект представителя Scalise поможет защитить конфиденциальные данные правительства США», - говорит Джонс из Egnyte.

Другие принятые документы

Палата представителей также приняла закон, который предписывает FCC создать консультативный совет по безопасности телекоммуникационных сетей. Другой законопроект - Закон о стратегии в области информационных и коммуникационных технологий - потребует от должностных лиц Министерства торговли оценки конкурентоспособности компаний в цепочке поставок технологий, согласно Комитету Палаты представителей по энергетике и торговле, от имени которого были выставлены счета.

В совместном заявлении в среду председатель Комитета по энергетике и торговле Палаты представителей Фрэнк Паллоне, DN.J., и Майк Дойл, штат Пенсильвания, отметили: «Вместе эти счета повысят надежность сети, защитят от подозрительного оборудования, которое представляет собой риск. для нашей национальной безопасности, поддержки небольших поставщиков сетей связи и повышения экономической конкурентоспособности нашей цепочки поставок технологий».

Если в конечном итоге законопроекты о цепочке поставок и телекоммуникациях будут приняты, добавляет Джонс из Egnyte, правительству необходимо будет обеспечить, чтобы новые требования к программному обеспечению не создавали «длительных бюрократических препятствий».Но он говорит, что эти счета «беспроигрышны для правительства и граждан США». ***(Dan Gunderman. House Passes Bills on Both Supply Chain, Telecom Security // Information Security Media Group, Corp. (https://www.govinfosecurity.com/house-passes-bills-on-both-supply-chain-telecom-security-a-17777). 21.10.2021).***

***

«Госдепартамент США планирует создать новое бюро киберпространства и цифровой политики, чтобы противостоять глобальным

вызовам кибербезопасности, таким как атаки программ-вымогателей, сообщает Wall Street Journal в понедельник. Реструктуризация также будет включать создание отдельной должности специального представителя по критически важным и новым технологиям, сообщает журнал со ссылкой на неустановленных официальных лиц США.

Капитальный ремонт, о котором должно быть объявлено на следующей неделе, является последним из ряда шагов, предпринятых администрацией Байдена за последние месяцы для решения проблем международной кибербезопасности, таких как взлом правительственных сетей США, вмешательство в выборы и кража интеллектуальной собственности.

В мае президент Джо Байден издал распоряжение, направленное на улучшение системы кибербезопасности США после разрушительной атаки программ-вымогателей, в результате которой был остановлен крупный нефтепровод в США, что вызвало обеспокоенность по поводу повсеместной нехватки газа на Восточном побережье. Предполагается, что преступное предприятие, которое с тех пор заявило о своем расформировании, базируется в России.

Эта новость появилась после того, как Microsoft заявила ранее в понедельник, что то же самое российское агентство, которое, как считается, несет ответственность за прошлогоднюю массовую кибератаку SolarWinds, в последние месяцы нацелено на компьютерные сети сотен других компаний и организаций. Испорченное обновление программного обеспечения, которое, как утверждают спецслужбы США, вероятно, возникло в России, было использовано для получения доступа к системам тысяч клиентов SolarWinds, включая федеральные агентства, крупные технологические компании и больницы. Россия отрицает свою причастность…». ***(Steven Musil. State Department reportedly plans new cybersecurity office // CNET (https://www.cnet.com/tech/services-and-software/state-department-reportedly-plans-new-cybersecurity-office/). 25.10.2021).***

***

«Президент Джо Байден подписал законопроект, направленный на повышение кибербезопасности школ K-12 и снижение их уязвимости для атак программ-вымогателей.

Эта мера предписывает федеральному агентству по кибербезопасности и безопасности инфраструктуры изучить киберриски, с которыми сталкиваются начальные и средние школы, и разработать рекомендации, которые помогут школам справиться с этими рисками.

В исследовании будут оцениваться проблемы, с которыми школы сталкиваются при обеспечении безопасности своих систем и конфиденциальных данных об учениках и сотрудниках. У агентства есть 120 дней на то, чтобы завершить рассмотрение и отчитаться перед Конгрессом. Закон, принятый Палатой представителей и Сенатом США единогласно, также требует, чтобы федеральное агентство разработало инструменты онлайн-обучения для школьных чиновников.

Школы сильно пострадали от киберпреступников. Некоторые районы стали жертвами атак программ-вымогателей, которые захватывают компьютерные

системы и удерживают их в заложниках, пока их жертвы не заплатят выкуп или не восстановят систему самостоятельно.

По словам Дуга Левина, национального директора K12 Security Information Exchange, некоммерческой организации, отслеживающей информацию, с 2016 года произошло более 1200 киберинцидентов, затронувших государственные школы K-12 во всех 50 штатах». ***(Jenni Bergal. Biden Signs School Cybersecurity Bill // Nextgov (https://www.nextgov.com/cybersecurity/2021/10/biden-signs-school-cybersecurity-bill/186017/). 12.10.2021).***

***

«Удаленная работа изменила то, как работают команды. Примерно 41% американских сотрудников работают удаленно, поэтому компаниям пришлось заменить многие стандартные операции более гибкими цифровыми альтернативами. Меры кибербезопасности также стали более гибкими.

Аутентификация пользователей одновременно более важна и сложна в удаленной облачной среде, чем централизованные рабочие места в прошлом. Команды кибербезопасности нуждаются в гибких, масштабируемых решениях для проверки того, что пользователи говорят. Цифровые подписи - идеальное решение.

Даже на традиционном рабочем месте цифровые подписи могут помочь улучшить усилия по кибербезопасности. Вот как это сделать.

Цифровые и электронные подписи

Прежде чем идти дальше, важно понять, что здесь означает фраза «цифровые подписи».Многие источники используют термины «цифровая подпись» и «электронная подпись» как синонимы, но это не совсем верно. Электронные и цифровые подписи похожи на прямоугольники и квадраты, поскольку все цифровые подписи являются электронными, но не все электронные подписи являются цифровыми.

Электронная подпись или электронная подпись означает юридическое согласие стороны с соглашением. Они включают некоторый метод проверки личности подписавшего и предоставляют запись для каждого шага процесса, называемого контрольным журналом. Это позволяет выявить любое вмешательство, которое могло произойти, и гарантирует, что подпись действительна и безопасна.

Цифровые подписи - это особый тип электронной подписи, обеспечивающий дополнительную безопасность. Они используют криптографию для защиты процесса и большинство используют многофакторную аутентификацию (MFA) для проверки личности подписывающих сторон.

Стандартные электронные подписи не имеют таких функций, как MFA и цифровые сертификаты, что делает их менее безопасными. Следовательно, любые усилия по кибербезопасности, внедряющие электронные подписи, должны предпочесть цифровые подписи.

Типы цифровых подписей

Важно отметить, что цифровые подписи также относятся к более конкретным категориям. Сертификаты цифровой подписи (DSC) можно разделить на три

различных класса в зависимости от их безопасности и соответствующих приложений.

DSC класса 1 не используют MFA для проверки личности подписывающих лиц, используя только адрес электронной почты и имя пользователя. Таким образом, они используются в приложениях с меньшим риском, но не подходят для юридических документов или более конфиденциальных данных.

DSC класса 2 проверяют личность пользователей, сравнивая их с предварительно проверенной базой данных.Поскольку это обеспечивает большую безопасность, их достаточно для приложений с умеренным риском, таких как электронная подача налоговых документов, возможно, их наиболее распространенный вариант использования.

ЦИВ класса 3 являются наиболее безопасными, но наименее удобными. Это потому, что они требуют наличия полномочий для личной проверки личности подписавшего.Они относительно редки, часто встречаются только в юридических средах с высоким уровнем риска и не работают для удаленных сотрудников. Однако они очень безопасны.

Больше, чем просто подписание документов

Цифровые подписи чаще всего используются вместо физических подписей в юридических документах.Однако, хотя это может быть их наиболее распространенный вариант использования, он далеко не единственный. DSC могут проверять практически любой тип цифровой связи, при этом некоторые решения для подписи поддерживают 1500 или более интеграцийс другими приложениями.

Наиболее известное применение DSC за пределами подписания документов - это криптовалюта. Блокчейны используют цифровые подписи для защиты криптовалютных транзакций, гарантируя, что только законный владелец может разрешить сделку со своими токенами. Пока пользователи защищают свои закрытые ключи, DSC гарантируют, что никто не сможет перемещать их криптовалюту от их имени.

Тот же принцип применяется к большинству транзакций блокчейна, независимо от того, связаны они с криптовалютой или нет.Он также подчеркивает важность цифровых подписей в усилиях по кибербезопасности.Если этих инструментов достаточно для чего-то столь же безопасного, как блокчейн, у него есть значительный потенциал безопасности.

Проверка через хеширование

Первое качество DSC, которое делает их полезным инструментом кибербезопасности, - это то, как они используют хеширование для проверки Хеширование заменяет данные на хэш-код, уникальный идентификатор фиксированной длины. Это значение хеш-функции изменится при малейшем изменении исходного файла, вплоть до одного байта, и никакие два кода не совпадают.

Поскольку каждое значение хеш-функции уникально и позволяет отслеживать любые изменения в файле, хеширование является отличным инструментом проверки. Если что-то происходит с данными между двумя точками, пользователи могут определить, сравнив его хеш-значение с исходным файлом. Все изменения, будь то хакерские или программные ошибки, будут видны.

Такой уровень видимости критически важен для удаленных сотрудников. Когда сотрудники не могут физически присутствовать для совместной работы, им нужно доказательство того, что то, что они получают, на самом деле исходит от их коллег. Это доказывает использование DSC хеширования для проверки подлинности транзакции и предоставления истории изменений.

Более строгие методы аутентификации

Цифровые подписи дополнительно повышают безопасность, предлагая более строгий контроль аутентификации, чем стандартные электронные подписи. Хотя пароли по-прежнему являются наиболее распространенным способом проверки личности пользователей, их недостаточно для большинства процессов безопасности. Согласно отчету Verizon о расследовании утечек данных за 2021 год, 61% всех нарушений были связаны с учетными данными.

Все, что вызывает беспокойство, должно использовать что-то более надежное, чем простое имя пользователя и пароль, для аутентификации личности пользователя.Пароли слишком подвержены ошибкам, атакам методом перебора и заполнению учетных данных.Поскольку многие решения DSC класса 2 используют MFA для проверки подписывающих лиц, они обеспечивают большую защиту.

Часто цитируемая цитата Алекса Винерта из Microsoft утверждает, что MFA снижает вероятность взлома аккаунтов на 99,9%. Такой уровень безопасности при аутентификации в сочетании с прозрачностью хеширования обеспечивает гораздо больше спокойствия в удаленных приложениях, чем другие методы. Использование DSC делает маловероятным нарушение удаленной связи.

Повышенная продуктивность

Цифровые подписи также предлагают некоторые косвенные преимущества в плане безопасности. По сравнению с физическими подписями DSC намного более эффективны. С учетом дополнительной работы, связанной с удаленной подписью документов, такой как сканирование или отправка подписанных документов по факсу, сравнительная эффективность DSC в этих приложениях еще выше.

Вермонтсократил время утверждения контрактов на 75%,когда перешел на цифровую подпись в правительственной документации. Такая значительная экономия времени может существенно повлиять на усилия по обеспечению кибербезопасности.У ИТ-команд часто очень загруженный график, и большая эффективность позволяет им более тщательно сосредоточиться на возникающих угрозах.

Группам по кибербезопасности нужно больше времени, чтобы учесть нехватку персонала. Одному только Министерству внутренней безопасности нужно еще 1700 сотрудников, чтобы в достаточной мере противостоять угрозам, с которыми оно сталкивается. Команды безопасности могут больше сосредоточиться на критических задачах, сэкономив время на задачах, не связанных с добавлением ценности, с помощью DSC, уменьшая нехватку рабочей силы.

Снижение затрат

Точно так же внедрение цифровых подписей может сэкономить деньги, которые также необходимы многим командам ИТ-безопасности.Около62% опрошенных организаций планируют сократить свои ИТ-бюджеты в ответ на

убытки, связанные с COVID.В то же время нарастают киберугрозы, на устранение которых часто требуется увеличение расходов.

Цифровые подписи могут сэкономить предприятиям значительную сумму денег, позволяя увеличить расходы на безопасность. Например, по оценке Банка Монреаля, только на бумажных расходах можно сэкономить 100 миллионов долларов, перейдя на цифровые подписи. Такой уровень экономии, вероятно, позволит организациям более комфортно тратить больше на кибербезопасность.

Имея больше денег, группы по кибербезопасности могут внедрять новые технологии, такие как решения для автоматического мониторинга. Затраты на такие стратегии, как переход к архитектуре с нулевым доверием, не будут столь значительными в свете этой экономии.

Цифровые подписи должны быть частью всех усилий по обеспечению кибербезопасности

Цифровые подписи обладают впечатляющим потенциалом для усилий по обеспечению кибербезопасности, особенно при удаленной работе.Поскольку потребность в удаленной проверке пользователей и защищенной связи возрастает, DSC представляют собой идеальное решение.

Трудно игнорировать безопасность, эффективность и экономию времени DSC. По мере того как группы ИТ-безопасности сталкиваются с растущими проблемами по всем этим направлениям, преимущества цифровых подписей становятся все более очевидными. Любые усилия по обеспечению безопасности должны, по крайней мере, учитывать, как эти процессы могут улучшить свои рабочие процессы». ***(DEVIN PARTIDA. Can Digital Signatures Assist in Cybersecurity Efforts? // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/can-digital-signatures-assist-in-cybersecurity-efforts/). 21.10.2021).***

***

«Фирма по обучению кибербезопасности KnowBe4 выпустила отчет о состоянии конфиденциальности и безопасности за 2021 год, в котором подробно описывается ужасающее состояние осведомленности и практики сотрудников.

Отчет включает ответы 1000 сотрудников малых и средних предприятий (SMB) и крупных корпораций в США.

Он попытался определить, сколько обучения кибербезопасности прошли сотрудники, и какое влияние оно оказало на осведомленность сотрудников об общих рисках кибербезопасности.

В отчете было обнаружено, что сотрудники не могут идентифицировать атаки социальной инженерии, ожидания в отношении безопасности для стандартных и привилегированных пользователей и то, как риски кибербезопасности могут отрицательно повлиять на их работодателей.

Осведомленность сотрудников о рисках кибербезопасности минимальна в правительстве и здравоохранении

Согласно отчету об осведомленности сотрудников KnowBe4, около четверти (24%) сотрудников считают, что переход по подозрительным ссылкам или прикрепленным файлам практически не несет риска.

Точно так же менее трети (31%) сотрудников считают, что разрешать членам семьи и друзьям использовать рабочие устройства в нерабочее время рискованно или представляет собой серьезный риск. Эта практика разрывает цепочку человеческих брандмауэров и может привести к раскрытию информации. Аналогичное число (31%) также считает, что использование пароля по умолчанию на маршрутизаторе представляет собой значительную угрозу безопасности.

В то время как компрометация корпоративной электронной почты или мошенничество со стороны генерального директора - растущая проблема, которая стоит миллионы долларов, менее трети (31%) сотрудников понимают «очень хорошо» и могут объяснить это другим.

Кроме того, только 14% и 22% государственных служащих и работников здравоохранения могут с уверенностью описать высшему руководству негативные последствия рисков кибербезопасности. Это очень далеко от 47% и 50% в сфере технологий и финансов соответственно.

Точно так же сотрудники в правительстве и здравоохранении меньше всего разбирались в атаках социальной инженерии. Согласно отчету, только 15% государственных служащих «очень хорошо» понимали пять типов угроз социальной инженерии. Эти риски безопасности включают фишинг, целевой фишинг, компрометацию корпоративной электронной почты, вишинг и смишинг. Однако у работников здравоохранения и образования дела обстоят немного лучше - 16% и 17% соответственно. В лучшем случае 39% и 41% сотрудников финансового и технологического секторов соответственно могли с уверенностью объяснить угрозы социальной инженерии.

COVID-19 помешал обучению сотрудников кибербезопасности

В то время как обучение кибербезопасности помогло повысить осведомленность сотрудников, пандемия помешала обучению сотрудников.

Следовательно, чуть более половины (55%) сотрудников прошли непрерывное обучение по вопросам кибербезопасности и конфиденциальности данных во время пандемии.

Почти у четверти (23%) обучение по вопросам кибербезопасности было остановлено в начале блокировки, в то время как у 22% обучение было временно приостановлено, а затем возобновлено во время пандемии.

Правительство и здравоохранение имели самый высокий процент (65% и 59%) сотрудников, которые продолжали проходить обучение по вопросам кибербезопасности во время пандемии.

Однако KnowBe4 рекомендует непрерывное обучение и тестирование в области кибербезопасности для поддержания осведомленности сотрудников.

По заявлению компании, организациям следует «отправлять фишинговые сообщения вашим пользователям не реже одного раза в месяц», чтобы определить процент подверженных фишингу сотрудников, которые могут стать жертвами фишинговых атак.

Обучение кибербезопасности положительно влияет на осведомленность сотрудников

Существует связь между обучающими кампаниями по кибербезопасности и их восприятием рисков кибербезопасности.

В финансовой отрасли было проведено обучение по повышению осведомленности сотрудников в области кибербезопасности: 91% сотрудников прошли обучение в той или иной форме, по сравнению с 88% в сфере технологий, 84% в правительстве и 76% в сфере здравоохранения.

Согласно отчету KnowBe4 по безопасности, сотрудники, прошедшие обучение один раз в месяц, на 34% реже нажимали на подозрительные ссылки или вложения по сравнению с теми, кто проходил обучение не чаще двух раз в год. Точно так же они на 26% чаще полагают, что повторное использование пароля рискованно.

Удивительно, но государственные и медицинские работники получали больше обучения, даже и постоянно во время пандемии, но дела шли хуже, чем в других секторах.

Однако исследование не смогло объяснить, почему усиленное обучение не привело к повышению осведомленности сотрудников в этих секторах.

Сотрудники не применяют то, что они знают, для снижения рисков безопасности

Несмотря на понимание влияния рисков кибербезопасности, большинство сотрудников не практикуют то, что знают.

В то время как 52% сотрудников, вероятно, сообщат об инциденте безопасности, только 27%, вероятно, сделают это, в то время как 21% не уверены в том, что они будут делать, или просто откажутся сообщить.

Точно так же, хотя сотрудники также понимали риски безопасности слабых и повторно используемых паролей, только менее половины (46%) выбрали использование уникальных паролей на каждом устройстве и в каждом приложении.

Однако треть (34%) считает, что простое использование специальных символов, таких как «&» или «$», является лучшим методом создания надежного пароля.

Очевидно, обучение кибербезопасности положительно повлияло на сотрудников, особенно в сфере технологий и финансов, хотя и не в желаемых пропорциях.

Что наиболее важно, отчет показывает, что непрерывное повышение осведомленности сотрудников было более эффективным в снижении рисков кибербезопасности». ***(ALICIA HOPE. Report Shows Appalling State of Employee Awareness of Common Cyber Security Risks // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/report-shows-appalling-state-of-employee-awareness-of-common-cyber-security-risks/). 25.10.2021).***

***

«Госсекретарь США Энтони Блинкен объявил в понедельник, что Госдепартамент создаст новое бюро и посланника для управления киберполитикой, обновив его на фоне тревоги по поводу роста хакерских атак.

В служебной записке для персонала Блинкен сказал, что обзор показал необходимость структурных изменений в том, «как Государственный департамент должен адаптироваться к вызовам 21-го века».

Он объявил о планах, при условии утверждения Конгрессом, по созданию Бюро киберпространства и цифровой политики с новым специальным посланником по критически важным и новым технологиям.

«Эта структура предоставит нам большее лидерство и подотчетность для реализации дипломатической повестки дня в рамках межведомственного и зарубежного сотрудничества», - написал Блинкен.

Он сказал, что представит более подробную информацию в своем выступлении в среду в Институте дипломатической службы, учебном центре Госдепартамента в пригороде Вашингтона.

Представитель Госдепартамента Нед Прайс сообщил журналистам, что посланник сосредоточится на «трех ключевых областях: безопасность международного киберпространства, международная цифроваяполитикаи цифровая свобода».

Цифровой рывок происходит на фоне растущей озабоченности по поводу того, что Соединенным Штатам необходимо подготовиться к затяжным конфликтам и сбоям на киберфронте…». ***(US State Department sets up cyber bureau, envoy amid hacking alarm // Tech Xplore (https://techxplore.com/news/2021-10-state-department-cyber-bureau-envoy.html). 26.10.2021).***

***

«21 октября 2021 года Бюро промышленности и безопасности (BIS) Министерства торговли США опубликовало новые меры экспортного контроля в отношении определенных элементов кибербезопасности, которые запрещают экспорт или перепродажу хакерских инструментов авторитарным режимам, и создало новое лицензионное исключение для них. Новые правила нацелены на ужесточение экспортного контроля над инструментами кибербезопасности, включая программное обеспечение для вторжений, наблюдение за сетью Интернет-протокола (IP) и соответствующие технологии, которые могут использоваться злоумышленниками для проведения злонамеренных действий в киберпространстве и наблюдения. BIS запрашивает публичные комментарии до 6 декабря 2021 года для возможного пересмотра до того, как временное окончательное правило вступит в силу 19 января 2022 года.

BIS утверждает, что эти меры контроля носят узкий характер, сосредоточены на конкретном оборудовании, программном обеспечении и технологиях для кибер-вторжений и сетевого наблюдения, и, в сочетании с новым исключением из лицензии, они должны иметь ограниченное влияние. Правило предусматривает меры контроля кибербезопасности, ранее согласованные в многосторонних Вассенаарских договоренностях, приводя меры контроля США в соответствие с теми, которые уже приняты ЕС и другими юрисдикциями. Однако производители сетевой инфраструктуры, поставщики программного обеспечения и услуг для кибербезопасности, фирмы, занимающиеся криминалистической ИТ-экспертизой, программы выявления ошибок, а также те, кто занимается тестированием и исследованием уязвимостей, могут почувствовать влияние правила. Кроме того, экспорт в страны, вызывающие озабоченность по поводу национальной

безопасности, такие как Китай и Россия, будет строго ограничен, а компании, работающие с Cypress,

Это нормотворчество дает возможность компаниям, занимающимся деятельностью в области кибербезопасности, оценить, действительно ли меры контроля достаточно узки, чтобы исключить их законную рутинную деловую деятельность, и предоставить BIS комментарии о любых непредвиденных последствиях этих мер контроля.

Фон

Эти новые меры экспортного контроля в области кибербезопасности замыкают цикл предлагаемого правила, выпущенного BIS в 2015 году, для реализации многостороннего контроля, согласованного с Вассенаарскими договоренностями в 2013 году. После выпуска предлагаемого правила BIS получил огромное количество откликов от отрасли, в том числе сотни комментариев общественности официально, критикуя усилия как имеющие серьезные негативные непредвиденные последствия для законной трансграничной работы по кибербезопасности. Общие темы критики включали в себя чрезмерно широкие меры контроля в определенном объеме инструментов и технологий, введение обременительных требований экспортного лицензирования, которые затрудняли бы работу хакеров в белых шляпах и участников программы вознаграждения за ошибки, а также ограничения на разработка программного обеспечения для защиты от вторжений будет препятствовать международным исследованиям в области кибербезопасности.

BIS пересмотрела меры контроля в Вассенааре для решения этих проблем, что привело к многостороннему принятию пересмотренных мер контроля в 2017 году. Это новое временное окончательное правило от BIS реализует самую последнюю версию.

Обзор новых средств контроля кибербезопасности

BIS устанавливает новые меры контроля над некоторыми элементами кибербезопасности по причинам национальной безопасности (NS) и борьбы с терроризмом (AT) путем создания новых классификационных номеров экспортного контроля (ECCN) в Списке контроля за торговлей (CCL) и определений в Управлении экспорта. Регламент (EAR). Кроме того, BIS создает новое лицензионное исключение для санкционированного экспорта в области кибербезопасности (ACE), разрешая экспортные транзакции с этими новыми контролируемыми товарами в большинство пунктов назначения, ограничивая экспорт в группу стран, вызывающих озабоченность по поводу национальной безопасности.

Краткое описание новых элементов управления приведено ниже. Мы рады поговорить с компаниями более подробно о нюансах, которые могут повлиять на их бизнес:

BIS добавляет новые ECCN 4A005 (оборудование) и 4D004 (программное обеспечение), а также обновленный параграф 4E001.a и новый параграф.c (технология) в категорию 4 CCL, где регулируются элементы вычислений и обработки. Эти новые средства контроля охватывают оборудование, программное обеспечение и технологии, используемые для кибер вторжений. Однако новые

элементы управления предусматривают предоставление базовых обновлений и обновлений программного обеспечения, а также действия, связанные с раскрытием уязвимостей и реагированием на киберинциденты. BIS также вносит поправки в 5A004 для систем, оборудования и компонентов для устранения, ослабления или обхода информационной безопасности, чтобы связать элементы в новом 4A005.

BIS вносит поправки в ECCN 5A001, который регулирует чувствительную телекоммуникационную инфраструктуру, с новым параграфом 5A001.j, касающимся систем или оборудования сетевого наблюдения IP (интернет-протокол). Соответствующие обновления производятся в ECCNs 5B001 (испытательное, инспекционное и производственное оборудование), 5D001 (программное обеспечение) и 5E001 (технология) для элементов, относящихся к новому 5A001.j.

Определения. Термины «реагирование на киберинциденты» и «раскрытие уязвимостей» добавляются в раздел определений EAR в части 772.

Реагирование на киберинциденты означает процесс обмена необходимой информацией об инциденте кибербезопасности с лицами или организациями, ответственными за проведение или координацию действий по устранению инцидента кибербезопасности.

Раскрытие уязвимости означает процесс идентификации, сообщения об уязвимости или сообщения об уязвимости, или анализа уязвимости с лицами или организациями, ответственными за проведение или координацию исправлений с целью устранения уязвимости.

Исключения из новых элементов управления:

Опубликованная информация. Программное обеспечение и технологии, которые находятся в общественном достоянии и которые соответствуют требованиям, чтобы считаться «опубликованной» информацией в соответствии с 15 CFR § 734.7, останутся не подпадающими под действие EAR и, таким образом, исключены из этого контроля.

Элементы, контролируемые шифрованием. Когда элемент кибербезопасности также включает в себя функции информационной безопасности, так что он подлежит контролю за шифрованием в Категории 5, Часть 2 EAR, эти средства управления шифрованием будут иметь преимущественную силу при условии, что функциональность информационной безопасности остается присутствующей и может использоваться в конечном элементе или исполняемом файле кибербезопасности. программное обеспечение. Однако средства управления шифрованием не имеют приоритета для исходного кода программного обеспечения или технологии, реализующей функции, контролируемые в другом месте CCL, или для любого элемента, в котором функциональные возможности защиты информации отсутствуют, удалены или отсутствуют по иным причинам.

Скрытое управление прослушиванием. Элементы, которые уже контролируются по причинам скрытого прослушивания (SL) в другом ECCN, будут по-прежнему классифицироваться в соответствии с соответствующим ECCN, контролируемым SL.

Новое исключение из лицензии ACE

BIS также создает новую лицензию на экспорт разрешенных кибербезопасных исключений в § 740.22 EAR. Это очевидный ответ на критику отрасли в 2015 году, поскольку BIS заявила, что ее намерение заключается в том, чтобы «не препятствовать законным исследованиям в области кибербезопасности и действиям по реагированию на инциденты».Исключение начинается с определений следующих терминов для конкретного использования в контексте исключения ACE: «элементы кибербезопасности», «цифровые артефакты», «благоприятное обращение с конечным пользователем кибербезопасности» и «конечный пользователь в правительстве».

Обратите внимание, что похожие термины используются в других местах с другим значением в EAR. Например, GOV исключения из лицензии в § 740.11 EAR для экспорта государственным конечным пользователям и исключение из лицензии ENC в § 740.17 EAR для экспорта шифрования по-разному определяют понятие конечного пользователя из государственного бюджета. Исключение из лицензии ACE рассматривает этот термин в более широком смысле, охватывая традиционные правительственные функции, а также правительственные исследовательские учреждения, организации и физических лиц, которые действуют от имени правительства, а также организации частного сектора, такие как розничные или оптовые фирмы, занимающиеся производством., распространение или предоставление оборонных изделий или услуг.

Как пояснили BIS, исключение из лицензии ACE разрешает экспорт, реэкспорт и передачу (внутри страны) предметов кибербезопасности в большинство пунктов назначения, за исключением регионов, на которые распространяется торговое эмбарго. Исключение также предусматривает ограничительный подход к странам, вызывающим озабоченность по поводу национальной безопасности, таким как Китай и Россия. В частности, ACE не разрешает экспорт для государственных конечных пользователей в группах стран D: 1, D: 2, D: 3, D: 4 или D: 5, а также для негосударственных конечных пользователей в группе стран D: 1 или D: 5. Тем не менее, BIS действительно предусматривал льготы для некоторых видов экспорта в страны группы D, которые также включены в список ближайших союзников группы стран A: 6, в частности, Кипр, Израиль и Тайвань. Кроме того, ACE исключения из лицензии не разрешает конечное использование, если у экспортера есть основания знать, что элемент кибербезопасности «будет использоваться для нарушения конфиденциальности,

Комментарии. Хотя BIS утверждает, что оно соответствующим образом адаптировало новые меры контроля для узкого воздействия, отрасль откладывает дату вступления в силу. В частности, BIS запрашивает комментарии, чтобы «обеспечить всестороннее рассмотрение потенциального воздействия этого правила, включая комментарии о потенциальных затратах на соблюдение… и любом влиянии этого правила на законную деятельность в области кибербезопасности».

По мере того, как компании рассматривают вопрос о том, следует ли отправлять комментарии, они должны оценить влияние этих средств контроля на их бизнес-операции, есть ли более эффективные способы обозначить границы контролируемых продуктов и могут ли они предложить более точные определения,

отражающие понимание отрасли терминологии, используемой в правило».***(Melissa Duffy, Jim Koenig, Tyler Newby, David Feder, Jean Chang. Being a White-Hat Hacker Just Got Tougher: U.S Commerce Department Issues New Cybersecurity Export Controls on Intrusion and Surveillance Tools// Fenwick & West LLP (https://www.fenwick.com/insights/publications/being-a-white-hat-hacker-just-got-tougher-u-s-commerce-department-issues-new-cybersecurity-export-controls-on-intrusion-and-surveillance-tools). 21.10.2021).***

***

«На этой неделе стало известно о запуске постоянного предложения по оплате эксплойтов нулевого дня для программного обеспечения виртуальной частной сети (VPN) Windows, несмотря на то, что США обдумывают новые правила экспорта инструментов, которые могут быть использованы в кибератаках против США.

Исследователи отметили, что эти события сигнализируют о том, что сообщество специалистов по кибербезопасности США переходит в наступление против национальных государств, но они могут не иметь большого эффекта.

Zerodium, который управляет высококлассными, дорогостоящими сторонними программами по борьбе с ошибками, часто от имени западных правительств объявляет, что ищет эксплойты, влияющие на Windows ExpressVPN, NordVPN и Surfshark. В частности, компания хочет «раскрытия информации, утечки IP-адреса или удаленного выполнения кода», - говорится в сообщении компании. «Повышение локальных привилегий выходит за рамки компетенции».

Злоумышленники прячутся за VPN, чтобы скрыть свое местоположение и IP-адреса. В совокупности ExpressVPN, NordVPN и Surfshark обслуживают десятки миллионов пользователей по всему миру.

Похоже, что эта попытка является реакцией на атаки национальных государств, такие как вредоносное ПО DevilsTounge в июле прошлого года, развёрнутое против правительственных учреждений и должностных лиц по всему миру, благодаря ошибке Microsoft 0-day. Перед этой атакой хакеры потребовали 500 000 долларов за информацию об обнаруженном ими эксплойте Zoom Windows, который позволял им шпионить за частными конференциями на платформе.

Регулирование экспорта кибербезопасности

Бюро промышленности и безопасности (BIS) Министерства торговли США объявило о новых правилах экспорта «определенных предметов», которые могут быть использованы в кибератаках.

«Соединенные Штаты привержены работе с нашими многосторонними партнерами, чтобы сдерживать распространение определенных технологий, которые могут быть использованы для злонамеренных действий, угрожающих кибербезопасности и правам человека».Министр торговли США Джина Раймондо рассказала о новых правилах.«Временное окончательное правило Министерства торговли, вводящее экспортный контроль в отношении определенных элементов кибербезопасности, представляет собой надлежащим образом адаптированный подход, который защищает национальную безопасность Америки от

злонамеренных киберпреступников, обеспечивая при этом законную деятельность в области кибербезопасности».

И хотя усилия правительства США, безусловно, того стоят, по словам Криса Клементса, с Cerberus Sentinel, он не уверен, что эти усилия существенно повлияют на атаки.

«Во-первых, некоторые из крупнейших поставщиков такого программного обеспечения находятся за пределами США, где регулирование может не повлиять на них», - сказал Клементс. «Во-вторых, многие из наиболее часто используемых инструментов имеют открытый исходный код, и мне неясно, как эти правила повлияют на их распространение».

Он добавил: «Даже если обычные хостинговые организации с открытым исходным кодом, такие как GitHub или GitLab, будут вводить ограничения GeoIP на загрузку такого специального программного обеспечения для вторжений, для запрещенной страны будет тривиально просто использовать VPN через общего поставщика VPN, чтобы обойти такое ограничения."

Клементс добавил, что у злоумышленников нет никаких моральных или этических проблем с использованием пиратских версий программного обеспечения, такого как Cobalt Strike.

Bug-Bounty Backfire

Когда дело доходит до Zerodium, использующего деньги для привлечения внимания к уязвимостям Windows, не работая в тесном сотрудничестве с пострадавшими, Бен Пик из nVisium объяснил Threatpost, что это может привести к обратным результатам.

«Вопрос о том, что третья сторона, такая как Zerodium, исследует уязвимости в службах конфиденциальности, является спорным вопросом», - сказал Пик. «Обнаруженные уязвимости могут позволить однозначно идентифицировать отдельных злоумышленников, тем самым предотвращая преступления, которые в противном случае были бы скрыты».

Кроме того, эти усилия по защите безопасности некоторых могут быть предприняты за счет конфиденциальности других пользователей, добавил он.

«Этими уязвимостями можно так же легко злоупотребить, чтобы нарушить конфиденциальность множества людей, которые используют услуги VPN в законных целях», - сказал Пик.

Пик объяснил, что в конечном итоге обнаружение основных уязвимостей может упростить взлом правительственных данных.

«Некоторые уязвимости могут использоваться другими VPN-сервисами, использующими аналогичный базовый код, что подвергает риску огромные объемы частных и государственных данных», - сказал он Threatpost. «Поскольку Zerodium, похоже, не работает с самими службами VPN для повышения их общей безопасности, любые выявленные уязвимости, скорее всего, будут использованы для нарушения конфиденциальности невинных конечных пользователей. Это создало бы опасный прецедент для служб поиска ошибок в целом». ***(Becky Bracken. U.S. Ban on Sales of Cyberattack Tools Is Anemic, Experts Warn // Threatpost (https://threatpost.com/us-ban-cyberattack-tools-zerodium/175654/). 21.10.2021).***

***

«После атаки SolarWinds в прошлом году президент Байден в мае издал указ, в котором пропагандирует обязательные спецификации программного обеспечения, или SBOM, для повышения прозрачности программного обеспечения и противодействия атакам на цепочки поставок.

Для справки: SBOM - это машиночитаемые документы, которые предоставляют исчерпывающий отчет о компонентах, используемых для создания программного продукта, включая программное обеспечение с открытым исходным кодом. Меня как специалиста по безопасности воодушевляет мандат SBOM, потому что это шаг к обеспечению большей прозрачности для программного обеспечения, которое все организации должны покупать и использовать.

Со времени указа производители и покупатели программного обеспечения пытались понять, как SBOM поддерживают безопасность цепочки поставок. Несомненно, многие видят в этом головную боль, но я считаю, что это разумная гарантия. Отчасти наша проблема с цепочками поставок заключается в том, что мы слишком им доверяем. Мы узнали о преимуществах модели безопасности с нулевым доверием и применили эту концепцию к нашим сетям и конечным точкам, но мы не совсем поняли, как это сделать для наших цепочек поставок. Мы по-прежнему в значительной степени полагаемся на трудоемкие анкеты, которые увековечивают постоянную зависимость от доверия как основы безопасности цепочки поставок.

Причина, по которой нам нужны такие вещи, как SBOM, заключается в том, что мы не можем доверять нашим цепочкам поставок, и поэтому нам нужно, чтобы они былипрозрачными. SBOM являются ступенькой к достижению этой прозрачности и позволяют нам начать движение к подходу нулевого доверия к цепочкам поставок программного обеспечения.

Рэйчел Ботсман, известный эксперт по доверию и преподаватель Оксфордского университета, описала проблему следующим образом: «Одна из ошибок, которые я слышу, заключается в том, что способ укрепить доверие - это прозрачность.Это обычное повествование.Но если вам нужно, чтобы всебыло прозрачно, то вы практически отказались от доверия. Делая все прозрачным, вы уменьшаете потребность в доверии ».SBOM, обеспечивая нам большую прозрачность, позволяют нам применять больше подходов с нулевым доверием в нашей цепочке поставок.

Уверенность в неизвестном через SBOM

Теперь мы не можем эффективно работать в среде, которая действительно остается на уровне нулевого доверия. Должно произойти некоторое укрепление доверия.Боцман говорит об определении доверия как «уверенных отношений с неизвестным».Когда дело доходит до наших цепочек поставок, существует множество неизвестных, но SBOM также предлагают способ обрести уверенность в неизвестном.

В частности, я считаю, что способность человека создавать SBOM с легкостью и в большом масштабе сильно коррелирует со зрелостью и / или современностью их методов разработки программного обеспечения. Если чьи-то

методы разработки программного обеспечения незрелы или устарели, создание SBOM, как правило, будет затруднено.

Если я попрошу поставщика программного обеспечения создать SBOM, а он, похоже, не сможет это сделать, это заставит меня усомниться в их методах разработки программного обеспечения. Я бы меньше доверял неизвестным факторам, связанным с этим поставщиком программного обеспечения.

Независимо от того, хотят ли они на самом деле показать мне SBOM, простое знание того, что они могут легко создать SBOM, дает мне уверенность в том, что их методы разработки программного обеспечения являются современными или достаточно зрелыми, чтобы противостоять широкому кругу общих проблем, связанных с уязвимыми или плохо поддерживаемое программное обеспечение.

Выходя за рамки SBOM

SBOM - отличный первый шаг к прозрачности цепочки поставок, но еще многое предстоит сделать. По аналогии, многие приравнивают SBOM к этикеткам с ингредиентами на пищевых продуктах. С этой точки зрения мы видим параллели между нашей цепочкой поставок программного обеспечения и цепочкой поставок продуктов питания. Следовательно, необходимость в сквозном происхождении и сопротивлении взлому должна быть очевидна.

По этой причине меня воодушевляет предложенная Google структурауровней цепочки поставок для программных артефактов(SLSA), которая приближает нас к общему языку, повышающему прозрачность и целостность нашей цепочки поставок программного обеспечения.

Однако для некоторого программного обеспечения, которое выполняет критически важные функции (например, безопасность), еда не является адекватным сравнением. Возможно, уместнее будет сравнить этот тип программного обеспечения смедициной. Эта аналогия вызывает дополнительные соображения. Например, этикетка с фактами о лекарствах на лекарствах включает не только ингредиенты, но также инструкции по применению и противопоказания (то есть, что искать в случае, если что-то пойдет не так). Более того, как мы все видели с вакциной COVID-19, лекарства должны пройти тщательную проверку и тестирование, прежде чем они будут одобрены для использования.

Каким образом эти шаги будут реализованы, вероятно, будет обсуждаться в течение некоторого времени, но необходимость в них не должна подвергаться сомнению. Пока у нас не будет лучшего контроля над цепочкой поставок программного обеспечения, мы продолжим нашу диету из отравленных фруктов. Мы можем стать сильнее с помощью этой диеты, но она также может нас убить. Я бы предпочел не рисковать». ***(Sounil Yu. Mandating a Zero-Trust Approach for Software Supply Chains // Threatpost (https://threatpost.com/mandate-zero-trust-software-supply-chains/175333/). 13.10.2021).***

***

«Американская ассоциация кинокомпаний (Motion Picture Association, MPA) призывает внести изменения в постановление правительства США о кибербезопасности, чтобы оно помогало эффективнее бороться с пиратством. Помимо прочего, считают в MPA, постановление должно обязать IaaS-

провайдеров, в том числе хостинговые сервисы, операторов DNS-серверов и обратных прокси, а также криптовалютные биржи тщательно проверять личность иностранных клиентов.

В январе нынешнего года Дональд Трамп, в то время занимавший должность президента США, подписал указ, согласно которому американские облачные компании должны вести учет иностранных клиентов, чтобы помочь властям отслеживать людей, совершающих киберпреступления, в том числе нарушающих авторские права. Указ призван лишить киберпреступников возможности использовать продукты IaaS (Infrastructure as a Service - инфраструктура как услуга) на территории США, и для этого необходимо обязать такие сервисы должным образом проверять личность иностранных клиентов.

Документ был с радостью встречен группами правообладателей (включая MPA), которые все время жалуются на анонимных операторов пиратских сайтов и сервисов, пользующихся услугами американских регистраторов доменов, хостинговых компаний, сетей распространения контента (CDN), прокси-сервисов и даже криптовалютных бирж. Поэтому, когда Министерство торговли США запустило общественное обсуждение путей реализации данного указа, MPA откликнулась незамедлительно. Согласно MPA, указ поможет в борьбе с пиратством, но только при правильных условиях.

Указ уже и так обязывает online-сервисы устанавливать личность потенциальных нарушителей авторских прав. Однако, как отмечает MPA, операторы пиратских сайтов обычно используют ложную информацию о себе, поэтому "правила должны гарантировать, что проверка их личности обеспечивает высокую степень уверенности в том, что зарегистрированные личности являются подлинными".

Помимо прочего, IaaS-провайдеры должны не просто проверять информацию при регистрации учетной записи. Они должны быть уверены в том, что эта информация остается достоверной на протяжении всего времени, пока клиент использует их продукты.

По мнению MPA, проверка личности должна проводиться не только в отношении зарубежных клиентов, но и американских. В конце концов, операторами пиратских сайтов необязательно являются лишь иностранцы.

Ассоциация предложила три шага по обеспечению эффективного и корректного выполнения новых требований IaaS-провайдерами.

Во-первых, online-сервисы должны предлагать инструмент, позволяющий заинтересованным сторонам уведомлять их о случаях использования клиентами поддельных личностей. Во-вторых, они должны удалять учетные записи клиентов, использующих поддельные личности. Третий шаг направлен на самих IaaS-провайдеров - за неисполнение указа на них должны налагаться штрафы.

По этой причине правила должны охватывать широкий спектр услуг, включая web-хостинг, обратные прокси-серверы, CDN, DNS-серверы, сервисы защиты от DDoS-атак, регистраторов доменов, обработчиков платежей, рекламные сети и криптовалютные биржи.

Роль хостинг-провайдеров очевидна, но MPA подчеркивает, что криптовалютные биржи и DNS-серверы также играют важную роль в экосистеме

пиратства. Так, криптовалюта стала популярным среди пиратов средством анонимного получения и хранения платежей. В свою очередь, DNS-серверы переводят web-адреса в соответствующие IP-адреса, что является ключевой функцией интернета, необходимой для работы сайтов, в том числе пиратских.

На данный момент многие биржи криптовалюты уже используют процедуры тщательной проверки, но MPA явно видит возможности для улучшения. Для DNS-серверов все может оказаться сложнее, поскольку их клиентами редко бывают операторы сайтов». ***(Кинокомпании США хотят привлечь криптобиржи к борьбе с пиратством // SecurityLab.ru (https://www.securitylab.ru/news/526041.php). 8.10.2021).***

***

Країни ЄС та Великобританія

«В решении от 30 июня 2021 года Апелляционный суд Версаля счел, что предвзятое отношение не может быть исправлено для юридического лица. В этом деле, касающемся компании, ставшей жертвой программы-вымогателя, судьи напомнили, что возмещение морального ущерба предполагает, что юридическое лицо «продемонстрирует конкретное ухудшение его репутации или своего имиджа среди клиентов».

Это решение позволяет нам пересмотреть правила компенсации, применимые, когда компания становится жертвой компьютерной атаки.

Необходимое обоснование финансовых потерь в случае кибератаки

Что касается кибератак, компания-жертва традиционно может ссылаться на несколько категорий ущерба, которые подразделяются на (i) финансовый ущерб, (ii) моральный ущерб и (iii) материальный ущерб.

В деле, поданном в Апелляционный суд Версаля, факты были следующими:

Бывший сотрудник компании перед увольнением создал программу, которая позволяла ему извлекать данные с почтовых серверов компании. Затем этот же сотрудник отправил программу-вымогатель своему бывшему работодателю, отправив «анонимное» электронное письмо, в котором указал, что владеет конфиденциальными данными компании. В этом письме были приведены конкретные примеры, которые также содержали угрозы раскрыть клиентам, партнерам, сотрудникам и конкурентам компании, если она не переведет миллион евро на различные счета BITCOINS.

В первой инстанции Уголовный суд Нантера обязал преступника выплатить потерпевшей компании сумму в размере 325 930,59 евро, разбитую следующим образом:

315 930 евро за финансовые потери в счет возмещения затрат и сборов за кризисную коммуникацию, комплексную проверку, связанную с процедурой с CNIL, затраты, связанные с поиском технических доказательств, а также гонорары, судебные издержки и управление;

10 000 евро в качестве компенсации морального вреда;

2000 евро в качестве процессуальной компенсации.

Фактически, финансовые потери могут покрывать, в зависимости от случая:

Упущенные доходы влияют на работу бизнеса: они могут быть связаны с лишением или нехваткой денежных средств, перебоями в поставках и т. д.;

На потерю возможности получить прибыль можно ссылаться, в частности, когда деятельность прекращена или когда компания потеряла контракт;

Дополнительная стоимость может взиматься при сбоях в работе предприятия.

Строгий контроль проводится по подтверждающим документам, предоставленным потерпевшим. Поэтому для жертвы кибератаки крайне важно собрать вещественные доказательства различных убытков, связанных с этим типом бедствий.

Однако в настоящем деле Суд отмечает, что доказательства, представленные потерпевшей компанией, недостаточны в том смысле, что

счета были выставлены не для компании-жертвы, а для третьей компании

не было никаких доказательств, подтверждающих финансовое предположение о авансированных затратах.

Апелляционный суд также подтверждает необходимость оправдания понесенных убытков.

Эта позиция вытекает из нескольких предыдущих решений и, в частности, из решения Апелляционного суда Лиона от 2014 года. Мировые судьи второй степени напомнили о важности демонстрации реальности финансового ущерба, объяснив, что в настоящем В деле жертва не обосновала, что потеря данных повлияла на ее промышленное производство или качество ее отношений с клиентами. Напомним, что во французском гражданском праве целью возмещения ущерба является восстановление прежнего положения жертвы.

Способы устранения кибератаки подлежат суверенной оценке судьи первой инстанции. Последние пытаются проверить существенность ущерба с точки зрения элементов, оправданных потерпевшим, чтобы подтвердить понесенные убытки и упущенную выгоду.

Особенности компенсации морального вреда

Что касается морального вреда, в прокомментированном решении от 30 июня 2021 г. напоминается, что это ущерб, затрагивающий внебрачные и неэкономические интересы. Это касается юридического лица в случае нанесения ущерба его репутации и / или его имиджу.

Это решение дает разъяснения относительно характеристики морального ущерба и действительности его обращения, в том числе в присутствии юридического лица.

Таким образом, Апелляционный суд Версаля счел, что:

Ущерб привязанности может быть возмещен только физическим лицом, а не юридическим лицом; а также

Для получения компенсации морального вреда юридические лица должны «продемонстрировать клиентам конкретное ухудшение своей репутации или имиджа».

Суд указывает, что юридические лица не могут страдать от стресса, беспокойства, разочарования или аффекта. Эти потери связаны, как физические

лица. В случае компании моральный ущерб возникнет в результате доказательства ущерба репутации или имиджу потерпевшей компании.

В случае компании моральный ущерб возникнет в результате доказательства ущерба репутации или имиджу потерпевшей компании.

Юридические лица - это вымышленные существа. По этой причине права и прерогативы, предоставленные и признанные физическим лицам, не могут быть применимы к ним в целом. Однако прецедентное право признает, что юридические лица имеют внебедственные интересы (честь, репутация, справедливое обращение и т. д.).

Заметим здесь, что принцип компенсации морального вреда юридическим лицам, как он упоминается в этом решении, обязательно соответствует иному значению, чем принцип компенсации физическим лицам, наделенным настоящими эмоциями. Компании или организации не могут «испытывать стресс» или испытывать чувство «беспокойства». Тем не менее, на них могут сильно повлиять факты, влияющие на их репутацию и ухудшающие их имидж.

В этом решении также содержится призыв принять во внимание требования к доказательству ущерба в результате кибератаки. Таким образом, необходимо обосновать, как это нападение повлияло на положение жертвы, атакже на существенность и затраты, связанные с мерами, принятыми для восстановления нормальной ситуации…» ***(Stŭphane Astier, Jessica Moraly. Victimes de ranзongiciels : quel prŭjudice indemnisable? // HAAS Avocats (https://info.haas-avocats.com/droit-digital/victimes-de-rancongiciels-quel-prejudice-indemnisable). 10.10.2021).***

***

«С момента создания подгруппы Европейской комиссии по совместным интеллектуальным транспортным системам, целью которой является внедрение инфраструктуры автомобильной кибербезопасности в масштабах всего ЕС, автомобильная промышленность стала рассматривать эффективную кибербезопасность как ключевое технологическое препятствие для дальнейшей автоматизации транспортной инфраструктуры.

В недавнем техническом документе, выпущенном консалтинговой компанией Horiba Mira, освещаются некоторые из причин, по которым автомобильная кибербезопасность представляет собой уникальные проблемы, которые распространяются на весь жизненный цикл транспортного средства. Во-первых, хотя определенный уровень уверенности в том, что транспортное средство может справиться с угрозами кибербезопасности, может быть предоставлено перед покупкой, возможность борьбы с угрозами должна поддерживаться посредством обновлений программного обеспечения и постоянного мониторинга, если мы хотим сохранить доверие потребителей.

Далеко за пределами ИТ-безопасности

Автомобильную кибербезопасность часто обсуждают через призму ИТ-безопасности, но на самом деле она выходит далеко за рамки этого.

Автономные транспортные средства полагаются на ввод данных, чтобы полностью определять свое окружение. Им не хватает человеческого сознания, чтобы судить, когда может случиться что-то плохое. Любое подавление, подделка

или подделка источника данных, вводимых в транспортное средство, может быть использовано для неправильного использования этого транспортного средства. Следовательно, при оценке угрозы кибербезопасности реальное взаимодействие современных автомобилей (даже с ограниченным уровнем автоматизации) и потенциально опасные для жизни последствия кибератаки означают, что транспортные средства нельзя рассматривать так же, как другие ИТ-системы. Это больше, чем просто «компьютеры на колесах».

Как подчеркивает Хориба Мира, источники кибератак на автомобиль выходят далеко за рамки тех, с которыми сталкиваются компьютеры. Примеры включают в себя манипуляции с бортовыми датчиками и внешними источниками данных, которые могут фальсифицировать «осведомленность» транспортного средства о своем окружении. Традиционные ИТ-меры не могут использоваться для эффективного противодействия этому, поскольку эти подходы обычно основаны на обнаружении вторжений. Любые угрозы, которые не требуют вмешательства в бортовые системы, могут быть использованы для предоставления фальшивых входных данных автомобилю.

Даже в современном автомобиле (с потенциально ограниченной автоматизацией, но с множеством вводов данных) существует множество способов доступа к бортовой электронике для злонамеренного взятия под контроль. История, опубликованная Wired в 2015 году, в которой подробно рассказывается о том, как хакеры дистанционно отключили трансмиссию Jeep Cherokee, является свидетельством того уровня контроля, который может быть получен.

Получение контроля над транспортным средством может привести к значительному ущербу и риску для жизни, если это позволит осуществлять гнусную деятельность. С такими физическими последствиями обычно не сталкиваются в мире ИТ-безопасности.

Богатый гобелен угроз

Одной из других причин уникальности проблемы, создаваемой автомобильной кибербезопасностью, является количество идентифицируемых агентов угроз. Потенциальное воздействие взлома на сеть автономных транспортных средств означает, что каждый, от недобросовестных пользователей до государств-изгоев, может представлять угрозу. Поэтому по мере развития сети автономных и подключенных транспортных средств при разработке решений проблемы кибербезопасности необходимо учитывать широкий спектр стратегий. С другой стороны, это обеспечивает богатый потенциал для инноваций в решениях для защиты как сети, так и транспортных средств, которые она поддерживает.

Защитить себя

Важно отметить, что защита, доступная для инноваций в области кибербезопасности, очень разнообразна. Решение, предназначенное для защиты всей сети от взлома из состояния мошенничества, сильно отличается от решения, которое направлено на то, чтобы помешать одному недобросовестному пользователю физический доступ к определенному транспортному средству, но оба они необходимы для поддержания сети и защиты ее пользователей, и оба потенциально могут быть запатентованы.

Если вы разрабатываете какой-либо тип технологии в этой области, заявка на патент может позволить вам получить эксклюзивные права на свои инновации и защитить свои инвестиции в НИОКР». ***(TERENCE BRODERICK. Solving the unique challenges of automotive cybersecurity for connected and autonomous vehicles // URQUHART-DYKES & LORD LLP (https://www.udl.co.uk/insights/solving-the-unique-challenges-of-automotive-cybersecurity-for-connected-and-autonomous-vehicles). 13.10.2021).***

***

«Глава Национального центра кибербезопасности (NCSC) предупредила, что кибератаки, в ходе которых хакеры проникают внутрь компьютерных сетей и блокируют их владельцев до тех пор, пока они не заплатят выкуп, представляют собой «самую непосредственную опасность» для британских предприятий в киберпространстве.

Линди Кэмерон сказала, что ее агентство, подразделение GCHQ, и Национальное агентство по борьбе с преступностью оценили, что киберпреступники, базирующиеся в России и ее соседях, несут ответственность за большинство «разрушительных» атак программ-вымогателей на Великобританию.

По ее словам, подобные атаки представляют угрозу для всех, от крупных компаний до местных советов и школ.

Выступая на конференции Chatham House Cyber 2021, г-жа Кэмерон предупредила, что недостаточно организаций были готовы к угрозе или протестировали свою киберзащиту.

В последнее время все чаще преступные группировки угрожают опубликовать некоторые данные, к которым у них есть доступ.

Совет округа Хакни пострадал от одной атаки, которая привела к серьезным сбоям в работе служб и ИТ-систем на несколько месяцев…

Были некоторые признаки того, что активность, связанная с Россией, снизилась за лето, но эксперты по кибербезопасности полагают, что большая часть этого может быть связана с тем, что хакеры ушли на летние каникулы, а не с каким-либо фундаментальным отклонением от очень прибыльной бизнес-модели.

Г-жа Кэмерон сказала, что программы-вымогатели останутся привлекательными, пока организации останутся уязвимыми и будут готовы платить. Она сказала, что правительство ясно дало понять, что выплата выкупа просто придает смелости преступным группам.

Помимо улучшения своей защиты, она также сказала, что Великобритания будет стремиться провести «устойчивую, проактивную» кампанию, чтобы помешать тем, кто наносит ущерб Великобритании, включая банды вымогателей.

Это будет включать в себя ряд методов, включая недавно созданные Национальные киберсилы, которые могут проводить наступательные хакерские операции.

В своем широкомасштабном выступлении г-жа Кэмерон, которая проработала чуть более года в качестве главы NCSC, заявила, что пандемия продолжает бросать тень на кибербезопасность и, вероятно, будет оставаться таковой на долгие годы.

«Злоумышленники продолжают пытаться получить доступ к информации, связанной с Covid, будь то данные о новых вариантах или планах закупок вакцин», - сказала она.

«Некоторые группы могут также стремиться использовать эту информацию, чтобы подорвать доверие общества к реакции правительства на пандемию. И преступники теперь регулярно используют атаки на тему Covid как способ обмана общественности».

Она также сослалась на недавние разоблачения шпионского ПО Pegasus, продаваемого компанией NSO Group, заявив, что NCSC поднял «красный флаг» в отношении растущего коммерческого рынка сложных продуктов, которые можно использовать для взлома телефонов людей и выполнения наблюдение.

На прошлой неделе решением британского суда было установлено, что шпионское ПО NSO использовалось для взлома телефонов бывшей жены правителя Дубая...» ***(Gordon Corera. UK cyber head says Russia responsible for 'devastating' ransomware attacks // BBC (https://www.bbc.com/news/uk-58877433). 11.10.2021).***

***

«Кембриджский университет приостановил предложенное партнерство на 400 млн фунтов стерлингов с Объединенными Арабскими Эмиратами (ОАЭ) из-за предполагаемого использования шпионского ПО Pegasus, сообщил его вице-канцлер.

На прошлой неделе Высокий суд признал, что правитель Дубая приказал взломать телефон своей бывшей жены.

В июле университет заявил, что ведет переговоры с ОАЭ о потенциальном партнерстве.

Профессор Стивен Туп, вице-канцлер Кембриджа, сказал, что теперь это «приостановлено».

Выступая в университетской студенческой газете Varsity, он сказал: «Разоблачение Pegasus заставило нас решить, что сейчас не время для реализации действительно амбициозных планов такого рода в ОАЭ.

«Это всегда вопрос тонкого баланса: конечно, вы должны оценить возможности, которые предоставляются, чтобы изменить мир к лучшему, и риски для репутации целого ряда важных для университета ценностей.

«В университете существуют отношения на уровне факультетов и отдельных академических кругов, но нет разговоров о большом проекте.

«Это все пока отложено».

Высокий суд постановил, что шейх Мохаммед Аль Мактум вмешался в деятельность британского правосудия, приказав взломать телефон своей бывшей жены, принцессы Иордании Хайи.

По словам суда, телефоны ее адвокатов, баронессы Фионы Шеклтон и Ника Мэннерса, также стали мишенью во время их дела о разводе.

В своем постановлении суд заявил, что для взлома использовалось программное обеспечение под названием Pegasus от израильской компании NSO Group.

Шейх Мохаммед отрицал какие-либо сведения о взломе.

Представитель Кембриджского университета сказал, что он подошел к предлагаемому партнерству с ОАЭ «непредвзято и тщательно взвесив возможности внести свой вклад в жизнь общества - посредством совместных исследований, образования и инноваций - против любых проблем».

«Мы будем размышлять в течение следующих нескольких месяцев, прежде чем продолжить оценку наших долгосрочных вариантов с нашими партнерами и университетским сообществом», - добавил он». ***(Cambridge University pauses J400m UAE deal over spyware claim // BBC (https://www.bbc.com/news/uk-england-cambridgeshire-58926039). 15.10.2021).***

***

Китай

«Китайські хакери успішно зламали iPhone 13 Pro та iOS 15.0.2. за рекордно короткий час на Міжнародному змаганні з кібербезпеки.

Експерти з безпеки змогли обійти захист нового смартфона за допомогою Safari за одну секунду. На пошук вразливостей їм знадобилося кілька місяців, але вони змогли отримати дані про користувачів після злому захисту Apple.

З метою безпеки, про принцип роботи не стали повідомляти. Швидше за все він відбувався за допомогою посилання в Safari, після натискання на яку шкідливий код обходив захист iPhone 13 та iOS 15.

Після використання вразливостей хакери отримали доступ до галереї смартфона, додатків і особистих даних власника.

На заході експерти займалися зломом не тільки пристроїв Apple – ентузіастам вдалося обійти захист Windows 10, Microsoft Exchange і Google Chrome.

Jailbreak для iOS 15 може з’явитися найближчим часом, якщо зловмисники дізнаються про принцип роботи уразливості…» ***(Микола Олефіренко. Хакери зламали iPhone 13 з iOS 15 за одну секунду // Факти ICTV (https://life.fakty.com.ua/ua/tekhnolohii/hakery-zlamaly-iphone-13-z-ios-15-za-odnu-sekundu/). 18.10.2021).***

***

Російська Федерація та країни ЄАЕС

«Порядка 50 уязвимостей электронного правительства оперативно были обнаружены и устранены работниками АО «Национальные информационные технологии» Министерства цифрового развития, инноваций и аэрокосмической промышленности РК….

Об этом стало известно по итогам пилотирования независимыми исследователями по кибербезопасности национальной платформы Bug Bounty из более чем 10 стран.

Рост числа преступлений в сфере информационных технологий сопровождается повышением требований к защищенности и устойчивости информационных систем организаций.

В этой связи АО «НИТ» подключилось к национальной программе обеспечения безопасности сервисов и приложений – Bug Bounty. Это позволяет обеспечить более высокий уровень защиты кибербезопасности системы и ресурсов электронного правительства.

«Ежедневно хакерским атакам подвергаются тысячи информационных систем, в том числе госорганов. Для нас важно надежное хранение и обеспечение защиты данных электронного правительства и его компонентов. Благодаря сотрудничеству мы получаем не только повышение уровня защищенности своих систем, но и экономим собственные ресурсы» - отметил председатель правления АО «Национальные информационные технологии» Ростислав Коняшкин.

В декабре прошлого года министр цифрового развития, инноваций и аэрокосмической промышленности РК Багдат Мусин анонсировал запуск Bug Bounty - программы для государственных органов. Тогда в рамках закрытого тестирования были получены критические уязвимости от исследователей, которые могут повлиять на большую часть казахстанского сегмента интернета.

«Мировой опыт показывает, что подключение крупных IT компаний к программам Bug Bounty представляет саму компанию как серьезно относящуюся к кибербезопасности, делая ее более прозрачной для своих клиентов. АО «НИТ» первыми из госсектора подключился к национальной программе Bug Bounty, мы рады и поддерживаем данное решение, так как это показывает зрелость в подходе защиты информационных систем» - поделился президент ОЮЛ «Центр анализа и расследования кибер атак» Олжас Сатиев.

BugBounty – специальная программа, в ходе которой компания привлекает сторонних специалистов по кибербезопасности для тестирования своего программного обеспечения на уязвимости за вознаграждение.

Данная программа функционирует в таких компаниях как Google, Facebook и Mozilla, и сделала их системы более надежными, при этом сэкономив на найме дополнительных специалистов по информационной безопасности.

Оператором национальной Bug Bounty площадки является компания TSARKA – лидер услуг по кибербезопасности в Центральной Азии.

27 октября Касым-Жомарт Токаев посетил ежегодный международный технологический форум «Digital Bridge». Глава государства высказал недовольство качеством интернета и связи в стране.

Глава государства подверг критике результативность работы вице-министров, ответственных за цифровизацию в Казахстане». ***(Белые хакеры будут искать уязвимости eGov.kz // ИА BaigeNews.kz (https://baigenews.kz/news/belye_khakery_budut_iskat_uyazvimosti_egov-kz/). 27.10.2021).***

***

«Заместитель председателя Правительства России Дмитрий Чернышенко рассказал о масштабировании Национального киберполигона.

Теперь, по словам вице-премьера, к национальной площадке по желанию будут подключаться коммерческие компании, обладающие соответствующей инфраструктурой для тренировки отражения кибератак.

В рамках инициативы первым к Национальному киберполигону присоединился киберполигон Центра компетенций НТИ «Технологии транспортировки электроэнергии и распределенных интеллектуальных энергосистем» на базе МЭИ, на котором регулярно проводятся киберучения для организаций сферы электроэнергетики. В настоящий момент заключено соглашение о сотрудничестве в области интеграции киберполигонов.

«С 2021 г. киберполигон будет расширяться за счет интеграции частных коммерческих киберполигонов в единую национальную инфраструктуру. Первым участником инициативы стал Центр НТИ МЭИ, чей киберполигон ориентирован на отработку навыков противодействия кибератакам в энергетической отрасли. Его подключение к промышленному сегменту Национального киберполигона позволит создать единую инфраструктуру, имитирующую типовое устройство организаций топливно-энергетического комплекса. Интеграция существенно расширит технологические возможности и позволит проводить более масштабные учения с максимальной реалистичностью исследуемых процессов. Объединение сценариев атак и их отражения на единой площадке сформирует список угроз, с которыми могут столкнуться российские предприятия. Такой опыт будет полезен для усиления информационной безопасности отдельных компаний и для расширения общей базы национального киберполигона», – сказал вице-премьер Дмитрий Чернышенко.

Развитие Национального киберполигона входит в список мероприятий национальной программы «Цифровая экономика». Ответственным исполнителем является «Ростелеком-Солар» – дочерняя компания «Ростелекома». Курирует реализацию мероприятия Минцифры России.

«Отраслевой сегмент киберполигона включает цифровую версию ИТ-инфраструктуры компании определенного сектора экономики. Это не реальный двойник, а усредненная копия. Интеграция существующих инфраструктур позволит расширить возможности Национального киберполигона, сделает его более функциональным. Развивать Национальный киберполигон нам также помогают образовательные учреждения – за последний год три вуза открыли собственные киберполигоны, на которых тренируются студенты и сотрудники местных компаний», – отметил замглавы Минцифры России Александр Шойтов.

Список компаний, присоединившихся к киберполигону, будет пополняться на протяжении всего периода реализации национальной программы. «Ростелеком-Солар» ведет переговоры с рядом крупных российских корпораций…

Киберполигон – это цифровые копии типовых ИТ-инфраструктур организаций ключевых отраслей. Цифровые копии позволяют без риска реального ущерба воспроизводить компьютерные атаки, характерные для конкретного сектора экономики, и отрабатывать меры по выявлению и предотвращению». ***(Национальный киберполигон объединит коммерческие площадки по отражению компьютерных атак // CNews (https://www.cnews.ru/news/line/2021-10-15_natsionalnyj_kiberpoligon). 15.10.2021).***

***

Австралія

«Хотя киберстрахование может сыграть положительную роль в повышении кибербезопасности, выплата выкупа страховщиками должна быть запрещена, согласно новому политическому документу Центра совместных исследований кибербезопасности (CSCRC). Как киберстрахование может помешать (или помочь) кибербезопасности в Австралии.

В документе утверждается, что практика страховщиков, включающая выплаты выкупа в состав полисов киберстрахования, непреднамеренно подпитывает эпидемию программ-вымогателей и потенциально приводит к тому, что организации перестают заботиться о кибербезопасности.

«В этом программном документе исследуется ряд вопросов, связанных с киберстрахованием, с акцентом на то, как оно может препятствовать и способствовать повышению кибербезопасности в экономике Австралии», - сказала Рэйчел Фальк, генеральный директор CSCRC.«Мы считаем, что выплата выкупов страховщиками помогает стимулировать незаконную торговлю программами-вымогателями. Когда речь идет о программах-вымогателях и страховании от киберпреступлений, жизненно важно то, что мы начинаем морить киберпреступников голодом и разорвать цепочку платежей, не давая страховщикам платить выкуп.»

Другие проблемы, поднятые в документе, включают отсутствие ясности в отношении включений и исключений в полисы австралийского киберстрахования, что может привести к тому, что застрахованные предприятия не имеют права требовать претензий, а также широкие полномочия страховщиков в случае кибер-события, которые имеют по сути, может сделать их теневыми директорами.

Однако, несмотря на подводные камни, г-жа Фальк сказала, что киберстрахование может сыграть положительную роль в повышении кибербезопасности.

«Страховщики могут предпринять действительно практические шаги для повышения кибербезопасности в Австралии в рамках своих предложений по страхованию от киберпространства», - сказала г-жа Фальк.«Они могут установить минимальные стандарты кибербезопасности для покрытия.Они могут работать с другими организациями, такими как поставщики телекоммуникационных услуг, чтобы предлагать «комплексные» продукты кибербезопасности как часть политик. И они могут способствовать соблюдению нормативных требований, отказываясь покрывать расходы, связанные с несообщаемым нарушением ».

В аналитическом документе содержатся 4 ключевые рекомендации, касающиеся:

• выплата выкупа или вымогательства страховщиками

• ясность в отношении управления рисками андеррайтинга киберстрахования и четкое определение того, что покрывается, а что нет.

• разработка страховщиками Контрольного списка кибербезопасности для МСП, и

• возможности для страховщиков сотрудничать с другими поставщиками услуг, чтобы предлагать «комплексные пакеты» для повышения кибербезопасности». ***(Cyber insurance drives ransomware threat // CCH Australia Limited (https://pinpoint.cch.com.au/news/csh-da-filter!WKAP_TAL_YACLTNEWS_REFERENCE/legauUio3433463sl1292274494/cyber-insurance-drives-ransomware-threat). 12.10.2021).***

***

«13 октября 2021 года министр внутренних дел обнародовал «новый комплексный» план действий в отношении программ-вымогателей. В соответствии с этим планом правительство Австралии объявило о предстоящих законодательных и операционных / политических реформах, направленных на более надежную защиту отдельных лиц, предприятий и критически важной инфраструктуры по всей Австралии от программ-вымогателей. В Плане излагаются текущие инициативы, уже предпринятые правительством для улучшения кибербезопасности в целом, а также будущие законодательные реформы, направленные конкретно на предотвращение и сдерживание атак программ-вымогателей.

В Плане также четко излагается политическая позиция Содружества в отношении выплаты выкупа, а именно, что Содружество не одобряет выплату выкупа. Ранее мы давали рекомендации относительно юридических рисков, связанных с выплатой выкупа.

Ключевые законодательные инициативы

В соответствии с планом ключевые будущие инициативы по сдерживанию атак программ-вымогателей включают:

Конкретные обязательные отчеты об инцидентах с программами-вымогателями перед австралийским правительством - однако правительство указало, что это будет применяться только к предприятиям с оборотом, превышающим 10 миллионов долларов в год. В настоящее время добровольным отчитывающимся субъектом является Австралийский центр кибербезопасности (ACSC), учреждение Австралийского управления сигналов, и мы ожидаем, что он продолжит получать отчеты от имени правительства в соответствии с новым законодательством.

Законодательная реформа, чтобы правоохранительные органы могли расследовать и конфисковывать платежи от программ-вымогателей в криптовалюте.

Вводится отдельное преступление для всех форм кибервымогательства. Предположительно, это будет распространяться не только на программы-вымогатели, но и на другие формы кибер-вымогательства, такие как отказ в обслуживании.

Криминализация покупки или продажи вредоносного ПО для совершения компьютерных преступлений.

Криминализация действий с украденными данными, заведомо полученными в ходе совершения отдельного уголовного преступления, с тем чтобы киберпреступники, которые лишают жертву своих данных или публично раскрывают конфиденциальные данные жертвы, подлежат более строгому наказанию. Учитывая, что он будет выходить за рамки операций с данными, украденными в ходе атаки с использованием программ-вымогателей, до операций с данными, украденными в ходе других уголовных преступлений, будет интересно увидеть фактический масштаб этого нового преступления и его применение к тем, кто «ворует» " данные.

Отдельное преступление с отягчающими обстоятельствами для киберпреступников, стремящихся атаковать критически важную инфраструктуру (как предлагается регулировать Законом о внесении поправок в законодательство о безопасности (критическая инфраструктура) 2020 (законопроект SOCI)). Правительство указало, что это будет означать увеличение штрафов, учитывая важность этих активов для Австралии.

Международное сотрудничество

План также указывает на намерение правительства работать с международными партнерами (в совместных операциях с партнерами) для выявления, расследования, пресечения и судебного преследования злонамеренных киберпреступников, участвующих в киберпреступности, а также для обращения к государствам, которые поддерживают киберпреступников. Предположительно, это будет включать сотрудничество в области наступательных кибернетических способностей.

Вскоре аналогичный закон может быть принят в США.

В прошлом месяце в Сенат США был внесен двухпартийный законопроект, который требует, чтобы владельцы и операторы критически важной инфраструктуры сообщали соответствующему федеральному агентству о любых «скрытых киберинцидентах» и любых платежах с использованием программ-вымогателей. Организации, сообщающие о платежах с использованием программ-вымогателей, должны будут провести комплексную проверку имеющихся альтернатив, в том числе возможности восстановления после атаки с использованием программ-вымогателей без предъявления требования об оплате. Это соответствует руководству Государственного департамента, согласно которому перед выплатой выкупа организации должны проконсультироваться с Государственным департаментом, чтобы свести к минимуму риск непреднамеренного финансирования запрещенных организаций, отдельных лиц или деятельности посредством выплаты выкупа.

Оба пункта соответствуют стратегиям, которые мы обычно рекомендуем для снижения риска совершения преступления в соответствии с Уголовным кодексом Австралии в отношении законов о борьбе с отмыванием денег и финансированием терроризма, включая, в контексте Австралии, уведомление и поддержание связи с одним или обоими из них. ACSC или Федеральная полиция Австралии». ***(Andrew Hannay, Cheng Lim and Sean Field. Australian Government unveils its Ransomware Action Plan// King & Wood Mallesons***

(https://www.kwm.com/en/au/knowledge/insights/australian-government-unveils-its-ransomware-action-plan-20211014). 14.10.2021).

***

«Хотя киберстрахование может сыграть положительную роль в повышении кибербезопасности, выплата выкупа страховщиками должна быть запрещена, согласно новому политическому документу Центра совместных исследований кибербезопасности (CSCRC): Underwritten or oversold? Как киберстрахование может помешать (или помочь) кибербезопасности в Австралии.

В документе утверждается, что практика страховщиков, включающая выплаты выкупа в полисы киберстрахования, непреднамеренно подпитывает эпидемию программ-вымогателей и потенциально приводит к тому, что организации не проявляют осторожности в вопросах кибербезопасности.

«В этом программном документе исследуется ряд вопросов, связанных с киберстрахованием, с упором на то, как оно может препятствовать и способствовать повышению кибербезопасности в экономике Австралии», - заявила генеральный директор CSCRC Рэйчел Фальк. «Мы считаем, что выплата выкупов страховщиками помогает стимулировать незаконную торговлю программами-вымогателями. Когда речь идет о программах-вымогателях и страховании от киберпреступлений, жизненно важно то, что мы начинаем морить киберпреступников голодом и разорвать цепочку платежей, не давая страховщикам платить выкуп.»

Другие проблемы, поднятые в документе, включают отсутствие ясности в отношении включений и исключений в полисы австралийского киберстрахования, что может привести к тому, что застрахованные предприятия не имеют права требовать претензий, а также широкие полномочия страховщиков в случае кибер-события, которые имеют по сути, может сделать их теневыми директорами.

Однако, несмотря на подводные камни, г-жа Фальк сказала, что киберстрахование может сыграть положительную роль в повышении кибербезопасности.

«Страховщики могут предпринять действительно практические шаги для повышения кибербезопасности в Австралии в рамках своих предложений по страхованию от киберпространства», - сказала г-жа Фальк. «Они могут установить минимальные стандарты кибербезопасности для покрытия. Они могут работать с другими организациями, такими как поставщики телекоммуникационных услуг, чтобы предлагать «комплексные» продукты кибербезопасности как часть политик. И они могут способствовать соблюдению нормативных требований, отказываясь покрывать расходы, связанные с несообщаемым нарушением».

В аналитическом документе содержатся 4 ключевые рекомендации, касающиеся:

• выплата выкупа или вымогательства страховщиками

• ясность в отношении управления рисками андеррайтинга киберстрахования и четкое определение того, что покрывается, а что нет.

• разработка страховщиками Контрольного списка кибербезопасности для МСП, и

• возможности для страховщиков сотрудничать с другими поставщиками услуг, чтобы предлагать «комплексные пакеты» для повышения кибербезопасности». ***(Cyber insurance drives ransomware threat // CCH Australia Limited. (https://pinpoint.cch.com.au/news/csh-da-filter!WKAP_TAL_YACLTNEWS_REFERENCE/legauUio3433463sl1292274494/cyber-insurance-drives-ransomware-threat). 12.10.2021).***

***

Інші країни

«Министерство общественной безопасности Вьетнама («MPS») опубликовало проект указа о санкциях за административные нарушения в области кибербезопасности («Проект указа») для общественных консультаций 20 сентября 2021 года. Период общественных консультаций завершится 18 ноября 2021 года. Дата - 1 декабря 2021 года.

Этот проект Указа, задуманный как консолидация положений об административных санкциях за нарушения, совершаемые в киберпространстве, является последним из проектов инструментов, представленных MPS в соответствии с Законом о кибербезопасности 2018 («Закон о кибербезопасности»).До этого в 2019 году был выпущен отдельный проект указа, расширяющий, среди прочего, требование о локализации данных в Законе о кибербезопасности, а ранее в этом году - проект Указа о защите персональных данных («Проект Указа о PDP»). В случае принятия в нынешней формулировке проект Указа отменяет ряд положений об административных санкциях в области почтовых услуг, телекоммуникаций, радиочастот, информационных технологий и электронных транзакций в соответствии с действующим Указом 15/2020 / ND-CP.

Этот проект Указа определяет действия, составляющие административные правонарушения, соответствующие санкции и меры по исправлению положения. Его в основном можно разделить на следующие три категории: (i) нарушения в отношении защиты персональных данных, (ii) нарушения кибербезопасности и (iii) нарушения информационной безопасности. Проект указа охватывает нарушения положений, в частности, Закона о кибербезопасности и проекта Указа о PDP. Мы отмечаем, что этот проект Указа, по всей видимости, основан на версии проекта Указа PDP, которая не была доведена до сведения общественности.

Ожидается, что предложенная в проекте указа сфера действия вне юрисдикции повлияет на национальные и оффшорные компании. В частности, проект указа включает санкции за нарушение еще не введенного в действие положения о локализации данных Закона о кибербезопасности, которое требует хранения определенных типов данных во Вьетнаме и установления местного присутствия, а также предлагаемых требований проекта Указа PDP для трансграничная передача персональных данных. Хотя требования к локализации данных и трансграничной передаче персональных данных уже давно являются

темами дискуссий из-за обеспокоенности, среди прочего, административным / финансовым бременем и воздействием на данные / торговые потоки, этот проект постановления, по-видимому, отражает намерение правительства продвигать их вперед.

В зависимости от нарушения денежные штрафы могут составлять от 10 до 100 миллионов донгов (примерно 440 - 4400 долларов США). Проект Указа также предусматривает, что штрафы, налагаемые на компании, могут быть двукратными. В серьезных случаях (например, при повторных нарушениях) штраф может составлять пятикратный или 5% от выручки компании-нарушителя на вьетнамском рынке…» ***(Yen Vu, Eunjung Han. Vietnam: Draft Decree on Cybersecurity Sanctions and PI Violations // Rouse International Limited (https://rouse.com/insights/news/2021/vietnam-draft-decree-on-sanctions-against-cybersecurity-and-personal-data-protection-violations). 08.10.2021).***

***

«Исследователю удалось взломать 70% из 5000 образцов сетей Wi-Fi в своем родном городе Тель-Авив, чтобы доказать, что домашние сети сильно незащищены и их легко взломать.

Исследователь безопасности CyberArk Идо Хорвич сначала бродил по центру города с оборудованием для сниффинга WiFi, чтобы собрать образцы из 5000 сетевых хэшей для использования в исследовании.

Затем исследователь использовал уязвимость, позволяющую получить хэш PMKID, обычно генерируемый для целей роуминга.

Чтобы собрать хэши PMKID, Хорвич использовал сетевую карту за 50 долларов, которая может выступать в качестве монитора и инструмента для внедрения пакетов, и проанализировал их с помощью WireShark в Ubuntu, оба являются бесплатными программами.

Хэш PMKID состоит из SSID сети, парольной фразы, MAC-адреса и статического целого числа.

Используя ранее открытый метод Йенса «Атома» Штеуба (ведущего разработчика Hashcat), исследователь собрал PMKID, которые будут взломаны для получения пароля.

«Технология Atom является бесклиентной, поэтому необходимость фиксировать логин пользователя в реальном времени и необходимость подключения пользователей к сети вообще устарели», - поясняет Хорвич в отчете.

«Более того, злоумышленнику требуется всего лишь захватить один кадр и устранить неправильные пароли и искаженные кадры, которые мешают процессу взлома».

Сначала были проведены «атаки по маске», чтобы определить, установили ли какие-либо пользователи номер своего мобильного телефона в качестве пароля Wi-Fi, что является обычным явлением в Израиле.

Для взлома таких паролей необходимо вычислить все варианты номеров для израильских телефонных номеров, а это десять цифр, начинающихся с 05, так что это всего восемь цифр.

Используя стандартный ноутбук, исследователь этим методом взломал 2200 паролей со средней скоростью девять минут на один пароль.

Следующая фаза атаки включала стандартную атаку по словарю с использованием словаря Rockyou.txt.

Это привело к быстрому взлому еще 1359 паролей, в большинстве из которых использовались только символы нижнего регистра.

Плохая практика безопасности

Следуя этому простому и недорогому методу взлома, исследователь взломал примерно 70% паролей для выбранных сетей Wi-Fi.

Исследование показывает, что большинство людей не устанавливают надежный пароль для своих сетей Wi-Fi, даже если они рискуют быть взломанными.

Если ваш пароль Wi-Fi взломан, любой может получить доступ к вашей домашней сети, изменить настройки вашего маршрутизатора и, возможно, переключиться на ваши личные устройства, используя недостатки…». ***(Bill Toulas. Researcher cracked 70% of WiFi networks sampled in Tel Aviv // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/researcher-cracked-70-percent-of-wifi-networks-sampled-in-tel-aviv/). 26.10.2021).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Российские хакеры, стоящие за успешным взломом федеральных агентств США в 2020 году, в последние месяцы пытались проникнуть в правительственные сети Америки и Европы.

Об этом сообщает CNN со ссылкой на аналитиков по кибербезопасности, отслеживающих деятельность группы.

Группа взломала несколько технологических компаний, о чем ранее не сообщалось, рассказал журналистам старший вице-президент и технический директор компании по кибербезопасности Mandiant Чарльз Кармакал. По его словам, хакеры также использовали новые инструменты и методы в некоторых своих операциях в этом году.

«Группа скомпрометировала несколько государственных структур, организаций, занимающихся политическими и внешнеполитическими вопросами, а также поставщиков технологий, обеспечивающих прямой или косвенный доступ к конечным целевым организациям в Северной Америке и Европе», - сказав Кармакал.

Однако он отказался назвать поставщиков технологий. Неясно также, к каким именно данным, если это имело место, получили доступ хакеры.

Официальный представитель США, знакомый с ситуацией, сообщил журналистам, что федеральные агентства отслеживают последние действия российских хакеров.

«Этот вопрос поднимался на недавних заседаниях Совета национальной безопасности», - отметил чиновник на условиях анонимности.

Упоминаемая группа российских хакеров наиболее известна тем, что использовала программное обеспечение, созданное американским федеральным подрядчиком SolarWinds, для взлома по меньшей мере девяти агентств США. О произошедшем стало известно в декабре 2020 года». ***(Катерина Комолова. Российские хакеры пытались проникнуть в правительственные сети США и Европы – CNN // UNIAN.NET (https://www.unian.net/science/rossiyskie-hakery-pytalis-proniknut-v-pravitelstvennye-seti-ssha-i-evropy-cnn-novosti-11569429.html). 07.10.2021).***

***

«Депутаты Европарламента обеспокоены системным агрессивным поведением Китая, России и Северной Кореи в киберпространстве, включая многочисленные кибератаки против государственных учреждений и частных компаний.

Об этом говорится в отчете, принятом Европарламентом 7 октября. Отчет поддержал 591 европарламентарий, 65 проголосовали против, 26 воздержались.

«В последние несколько лет наблюдается непрерывный рост вредоносных кибероперацией. ЕС и его государства-члены должны усилить обороноспособность, чтобы успешно реагировать на эти киберугрозы. Поэтому чрезвычайно важно усилить сотрудничество между странами-членами и институтами ЕС, НАТО, США и другими стратегическими партнерами», - сказал докладчик Урмас Паэт.

Депутаты Европарламента призывают к комплексному набору мер и последовательной политики в сфере IT, а также к улучшению военной координации в киберзащите для укрепления киберстойкости ЕС.

Европарламент рекомендует создать совместное киберподразделение для улучшения обмена информацией между институтами, органами и агентствами ЕС и для создания безопасной и быстрой информационной сети.

Отмечается, что в отличие от других военных областей, инфраструктура киберпространства в основном принадлежит частным компаниям, которые находятся преимущественно вне юрисдикции ЕС. Это приводит к тому, что страны ЕС становятся технологически зависимыми от третьих сторон. Поэтому депутаты Европарламента предупреждают, что ЕС должен стать более технологически независимым, внедрять инновации и больше инвестировать в возможности киберзащиты и персонал.

В отчете призывается к совместным и скоординированным ответам на кибератаки, которые также должны включать НАТО, эти ответы могут включать введение санкций против враждебных субъектов, угрожающих интересам евроатлантической безопасности.

В отчете также упоминается скандал со шпионским программным обеспечением Pegasus в качестве примера того, как шпионили за большим количеством журналистов, правозащитников, избранных представителей и других граждан ЕС». ***(Александр Топчий. Европарламент отреагировал на системные агрессивные кибератаки со стороны России, Китая и КНДР // UNIAN.NET***

(https://www.unian.net/science/evroparlament-otreagiroval-na-sistemnye-agressivnye-kiberataki-so-storony-rossii-kitaya-i-kndr-novosti-11569813.html). 07.10.2021).

***

«Большинство американцев обеспокоены кибератаками на критически важные объекты инфраструктуры, в частности на финансовый сектор и сектор национальной безопасности. Об этом свидетельствуют данные опроса, который провели Центр связей с общественностью Associated Press-NORC и Институт Пирсона Чикагского университета.

Исследование показало, что примерно три четверти опрошенных особенно обеспокоены кибератаками со стороны российского и китайского правительств, а чуть больше половины — из-за атак со стороны преступных кибергрупп.

Атаки на финансовые учреждения вызвали серьезную обеспокоенность: более 90% респондентов были очень или частично обеспокоены угрозами для своих данных в случае атаки на них. Более 90% респондентов также были озабочены атаками на системы национальной безопасности и обороны, медицинские учреждения и сектор энергетики.

— Общественность явно обеспокоена кибератаками, и многие американцы рассматривают их как потенциальный результат международного конфликта. Результаты опроса показывают, что американцев гораздо больше беспокоят кибератаки из Китая и РФ, чем те, что принадлежат к другим правительствам, группам или отдельным лицам, — заявила исполнительный директор отдела внешних связей Института Пирсона Шейла Кохантеб.

Существует значительный раскол в беспокойстве по возрасту респондентов. Более 75% респондентов старше 60 лет были обеспокоены кибератаками, тогда как менее половины респондентов в возрасте от 18 до 29 лет также были обеспокоены. Согласно опросу, пожилые люди также были более обеспокоены атаками со стороны правительств России или Китая, чем молодежь…». ***(Марія Степанюк. В США почти три четверти граждан обеспокоены кибератаками со стороны РФ и Китая // Факты ICTV (https://fakty.com.ua/ru/svit/svitovi-novyny/20211011-u-ssha-majzhe-try-chverti-gromadyan-sturbovani-kiberatakamy-z-boku-rf-ta-kytayu/). 11.10.2021).***

***

«Правительство Нидерландов заявляет, что может использовать спецслужбы или военные службы для противодействия кибератакам, в том числе атакам программ-вымогателей, которые угрожают национальной безопасности страны.

«Если атака программы-вымогателя, независимо от того, преследует ли он финансовую цель, пересекает порог (проявления) угрозы национальной безопасности, например, из-за сбоя в жизненно важных секторах, то правительство также имеет в своем распоряжении другие ресурсы», - сказал Датч Министр иностранных дел Бен Кнапен сказал в письме, отвечая на парламентский запрос о том, как страна может потенциально отреагировать на атаки программ-вымогателей.

Кнапен говорит, что важно, чтобы государства были привлечены к ответственности, и могут быть приняты такие меры, как санкции, если их действия нарушают принятые стандарты поведения в киберпространстве, такие как обеспечение трансграничных преступных кибероперацией, в том числе против атак программ-вымогателей.

«Примером последнего является отключение ИТ-инфраструктуры (или ее отключение), которая является частью инфраструктуры атаки или неправильно используется для цифрового шпионажа или саботажа. В дополнение к действиям служб разведки и безопасности (I&V), Нидерланды также могут ответить вооруженными силами », - отмечает Кнапен.

Кроме того, Кнапен говорит, что киберкомандование обороны может также осуществлять контратаку, используя вооруженные силы, чтобы предотвратить действия противника или защитить существенные интересы государства, в зависимости от международно-правовой основы и после решения правительства.

Хьюго ван ден Торн, менеджер по безопасности в Outpost24, сообщил Information Security Media Group, что в письме конкретно описывается структурированный совместный подход к предотвращению и реагированию на атаки с выкупом.

«Согласно письму, некоторые субъекты угроз достигли того же уровня возможностей, что и субъекты, спонсируемые государством, что является причиной для беспокойства и пересмотра совместных действий. Если определенные (финансовые) пороговые значения будут превышены, военные могут быть привлечены к помощь с дипломатической точки зрения, путем обмена разведданными, помощи в проведении тейкдаунов или, в конечном счете, в проведении контратак », - отмечает Тоорн.

Юридические соображения

По словам Кнапена, поскольку в международном праве нет согласованного определения цифровых программ-вымогателей, то, каким образом операции с программами-вымогателями квалифицируются для реагирования, необходимо рассматривать в индивидуальном порядке.

Международно-правовая база действительно предлагает возможность принятия контрмер при определенных обстоятельствах, особенно в отношении определения закона об ответственности государства за контрмеры в киберпространстве, которое гласит: «Контрмеры - это действия (или бездействие), которые обычно представляют собой нарушение обязательства по международному праву, но являются законными, потому что они являются ответом на предыдущее нарушение обязательства по международному праву другим государством », - отмечает Кнапен.

Джейк Уильямс, технический директор компании BreachQuest, занимающейся кибербезопасностью, говорит, что то, как голландцы решают проблему с негосударственными субъектами, имеет большое значение.

«В основном противодействие военным ответам на программы-вымогатели и киберпреступность заключается в том, что это ответ на проблему правоохранительных органов. В этом документе освещаются вопросы атрибуции при определении того, спонсируется ли операция государством, санкционируется

государством или просто игнорируется государством. Фактически, это По-видимому, это указывает на то, что использование в военных целях является законным вариантом, поскольку непринятие мер в отношении субъектов-вымогателей, действующих из ваших границ, ничем не отличается от фактического спонсирования действия ", - отмечает Уильямс, бывший член элитной хакерской группы Агентства национальной безопасности США.

Кнапен говорит, что Нидерланды сосредоточатся на инструментах для конкретной реализации стандартов, при этом приоритет будет отдан инициативе по продвижению ответственного поведения государства в киберпространстве в контексте международной безопасности в рамках Организации Объединенных Наций.

«Нидерланды будут уделять особое внимание внедрению стандартов, касающихся программ-вымогателей», - отмечает Кнапен.

Дипломатические разветвления

По словам Кнапена, страны привлекаются к ответственности за свои действия и бездействие посредством дипломатических ответных мер, таких как действия против трансграничных преступных кибероперацій и таких мер, каксанкции, которые более действенны, если они разработаны в широком контексте коалиции.

«Таким образом, в рамках ЕС Нидерланды были движущей силой набора инструментов кибердипломатии ЕС и принятия девятого режима киберсанкций ЕС в мае 2019 года, и Нидерланды привержены дальнейшему развитию этих инструментов. Это дает ЕС хорошие возможности. инструменты для более быстрого и решительного реагирования на киберинциденты. Недавние заявления и санкции ЕС показывают, что эти инструменты приносят конкретные результаты », - отмечает он.

Кнапен также настаивает на дипломатических каналах для двустороннего сотрудничества между странами в судебных расследованиях в отношении программ-вымогателей, что, по его словам, может быть полезно, если сотрудничество через международные судебные каналы недостаточно.«Затем Нидерланды могут подчеркнуть важность, придаваемую сотрудничеству по дипломатическим каналам», - говорит он.

Кроме того, Knapen заявляет, что Нидерланды продолжат свои усилия по содействию совместной разработке вариантов реагирования и обмену знаниями в рамках ЕС, НАТО и других альянсов с союзниками.

Торн заявляет, что предлагаемые невраждебные операции звучат очень разумно, учитывая, что голландские военные - и особенно голландское киберкомандование - обладают обширными возможностями и разведданными, чтобы помочь как государственным, так и частным компаниям в борьбе с программами-вымогателями.

Он добавляет, что «наступательные операции голландских военных следует тщательно продумать», поскольку они «могут вызвать больше дипломатических проблем». «Я бы не решился открыто предлагать военные наступательные операции, прежде чем определил все требования и пороги», - говорит Тоорн.

Уильямс отмечает, что документ, похоже, устанавливает юридическое обоснование в соответствии с международным правом для военных действий против стран, которые явно позволяют атакам программ-вымогателей продолжаться изнутри своих границ.

Предупредительные меры

В письме также описывается, как правительство Нидерландов повышает цифровую устойчивость Нидерландов. В нем говорится, что страна принимает различные меры в рамках Национальной программы кибербезопасности и своего комплексного подхода к киберпреступности.

«Во многих успешных кибератаках, включая программы-вымогатели, кажется, что основные меры кибербезопасности не были приняты в достаточной степени. Кроме того, многие предприниматели, особенно в малых и средних предприятиях, похоже, не считают себя потенциальными жертвами программ-вымогателей», - заявляет Кнапен. «Центр цифрового доверия (DTC) Министерства экономики и климата поэтому стремится предоставлять информацию о программах-вымогателях, например, рассказывая истории предпринимателей, ставших жертвами программ-вымогателей».

Кнапен также предупреждает, что ряд киберпреступных групп теперь обладают возможностями, не уступающими уровню государственных субъектов, и последствия атаки могут создать угрозу национальной безопасности из-за развертывания программ-вымогателей.

«В Нидерландах она еще не проявилась, [однако] эта угроза дополняет уже существующую, постоянно увеличивающуюся угрозу в киберпространстве», - отмечает Knapen. «Следственные службы, Служба разведки и безопасности и вооруженные силы пока недостаточно оснащены, чтобы принимать структурные меры против субъектов, которые представляют угрозу национальной безопасности посредством атаки программ-вымогателей».

И Уильямс отмечает: «Хотя я не предвижу военных вторжений, связанных с программами-вымогателями, в ближайшем будущем, этот документ является серьезным сигналом для стран, просто игнорирующих субъектов, действующих внутри их границ. Учитывая акцент на установлении стандарта международного права, документ может также предназначены для стимулирования конструктивных разговоров на международном уровне об угрозе программ-вымогателей». ***(Prajeet Nair. Netherlands Says Armed Forces May Combat Ransomware Attacks// Information Security Media Group, Corp. (https://www.govinfosecurity.com/netherlands-says-armed-forces-may-combat-ransomware-attacks-a-17703). 08.10.2021).***

***

«Когда в этом году элитная команда российских правительственных хакеров попыталась взломать сотни разведывательных целей, они использовали умный инструмент, чтобы замести следы: мобильные и домашние компьютерные сети ничего не подозревающих американцев, по словам нескольких экспертов по кибербезопасности.

По словам экспертов, хакеры, которые, как считается, работают на Службу внешней разведки России, использовали так называемые «резидентные прокси-серверы IP», чтобы получить доступ и избежать обнаружения.

В ходе длящейся хакерской атаки, раскрытой Microsoft в понедельник, сообщается, что компания уведомила «609 клиентов о том, что с мая они подвергались атакам 22 868 раз», причем показатель успешности выражался низкими однозначными числами. Microsoft назвала российскую хакерскую группу «Нобелиум». Эту же группу обвинили в причастности к атаке на SolarWinds, раскрытой в декабре прошлого года.

Основными целями хакерской кампании, которая, как предполагается, продолжается, являются «правительственные организации и другие организации, занимающиеся вопросами, представляющими интерес для России», - сказал Чарльз Кармакал, старший вице-президент компании по кибербезопасности Mandiant, которая работала с Microsoft. для выявления предполагаемых атак со стороны России. Кармакал сказал, что хакеры использовали резидентные IP-прокси, представляющие собой IP-адреса, связанные с определенным местоположением, которые можно приобрести в Интернете.

Предполагаемые жертвы включают правительственные учреждения США, неправительственные организации и фирмы, занимающиеся компьютерной безопасностью, по словам анонимного источника Bloomberg.

Посольство России в Вашингтоне не комментирует ситуацию.

Как и в случае со взломом SolarWinds, российские хакеры атаковали организации, «являющиеся неотъемлемой частью глобальной цепочки поставок ИТ», согласно сообщению Microsoft. Они использовали обходной путь, чтобы попытаться взломать свои конечные цели.

При взломе SolarWinds, предоставляющей программное обеспечение для мониторинга ИТ и инструменты управления, злоумышленники поместили вредоносное ПО в обновления для популярного программного продукта. Обновив программное обеспечение, клиенты SolarWinds непреднамеренно установили цифровой бэкдор, который впоследствии можно было использовать для дальнейшего проникновения. В конечном итоге в результате дальнейших атак пострадали около 100 компаний и девять государственных агентств США.

По словам Microsoft, в недавних кибератаках хакеры сосредоточились на компаниях, которые предоставляли технологические услуги конечным целям. При этом они, возможно, пытались найти более слабое звено и, возможно, обойти меры безопасности предполагаемой жертвы. В одном примере, подробно описанном Microsoft, они взломали четырех разных провайдеров, прежде чем добраться до конечной цели. Поставщики технологических услуг подвергались атакам с использованием различных средств, включая вредоносное ПО, целевой фишинг и попытки подбора паролей.

Используя резидентные IP-прокси, попытки хакеров взломать сеть будут казаться менее подозрительными, исходящими от мобильных телефонов США или домашних интернет-сетей, а не с компьютеров в России. Со стороны атака российского хакера может выглядеть как попытка сотрудника войти в систему со своего мобильного телефона…» ***(Романов Роман. Российские хакеры***

использовали домашние сети, чтобы скрыть свои атаки на госучреждения // Internetua (http://internetua.com/rossiiskie-hakery-ispolzovali-domashnie-seti-cstoby-skryt-svoi-ataki-na-gosucsrejdeniya). 26.10.2021).

***

Створення та функціонування кібервійськ

«Правительство объявило, что его агентство по кибератакам, известное как Национальные киберсилы, будет базироваться в Ланкашире.

Организация нацелена на противодействие угрозам со стороны преступников, террористов и враждебных государств.

Действующий с апреля 2020 года, он впервые включает в себя сотрудников из МИ-6, кибер-шпионского агентства GCHQ и военных под единым командованием.

Министр иностранных дел Лиз Трасс заявила, что это «противостоит агрессивному поведению».

Национальные киберсилы (NCF) будут базироваться в Самлесбери, где находится авиационный завод военной технологической компании BAE Systems, ис 1922 года активно участвует в разработке военных самолетов.

Правительство заявило, что до 2030 года он будет размещен в специально построенном помещении и получит более 5 миллиардов фунтов стерлингов инвестиций.

Представитель консерваторов заявила, что он станет «домом для тысяч кибер-хакеров и аналитиков» и создаст сотни рабочих мест в сфере бизнеса и права.

Подрывная тактика

О существовании NCF премьер-министр официально сообщил только в ноябре 2020 года.

Цель состоит в том, чтобы, когда британские вооруженные силы вступают в бой, кибероперации будут тесно сотрудничать с традиционными вооруженными силами, с потенциальными сценариями, включая взлом операторов ПВО противника.

Тактика может включать в себя нарушение работы мобильного телефона подозреваемого или компьютерных серверов киберпреступной группы для предотвращения такой угрозы, как атака WannaCry в 2017 году, в результате которой часть сотрудников NHS и других организаций была уничтожена путем шифрования их данных.

Другие методы могут включать общение с злоумышленниками, чтобы подорвать их моральный дух и отговорить их…» ***(National Cyber Force to be based in Samlesbury // BBC (https://www.bbc.com/news/uk-england-lancashire-58779337). 03.10.2021).***

***

«У вечері 4 жовтня користувачі соціальних мереж Facebook, Instagram та месенджера WhatsApp повідомили про збій у їхній роботі. За попередніми підрахунками, через глобальний збій у Facebook, Марк Цукерберг за декілька годин втратив понад 6 мільярдів доларів.А користувачі соцмереж могли втратити свої особисті дані.

Окрім того, надійшли повідомлення про проблеми із роботою Twitter, Telegram, TikTok, сервісів Google та Amazon, музичного сервісу Spotify, стримінгового відеосервісу Netflix, телекомунікаційної компанії Virgin Media, а також низки інших сайтів та сервісів. Робота основних платформ відновилася тільки близько 1:00 за українським часом.

Про наслідки збою у роботі соцмереж та крадіжку акаунтів — в ефірі Українського радіо розповів експерт з кібербезпеки Дмитро Снопченко.

Які причини збою у роботі соцмереж

«Уже відомо, що саме трапилося й експерти Facebook називають причиною банальну людську помилку: під час оновлення DNS-серверів працівники випадково видалили головний запис Facebook», — пояснив експерт.

За його словами, сервери Facebook працювали, але коли користувачі зі своїх пристроїв вводили Facebook.com у браузері, браузер не знаходив Facebook.com, через що користувачі не могли зайти на свої акаунти.

Витік даних користувачів

Експерт вважає, що інформація про крадіжку мільярда чи півтора мільярда акаунтів користувачів є «однозначним фейком, який розповсюдили зловмисники», які нібито хочуть отримати з цього фінансову вигоду.

«Вони скористалися даними користувачів, які Facebook втратив під час витоку у 2019 році й подали ці пів мільйона старих даних як свіжу інформацію, яка нібито була вкрадена в Facebook щойно», — розповів фахівець.

Згодом зловмисники стверджували, що зламавши Facebook, їм вдалося отримати півтора мільярда свіжих даних користувачів, які вони виставили на продажу, зазначив Снопченко: «З’явився навіть покупець, який нібито заплатив їм за цю інформацію 5000 доларів. Але це звісно ж фейк».

Водночас аналітик зауважує, що інформація про те, що Facebook не дбає про безпеку — є неправдою, адже великих витоків інформації із мережі вже «дуже давно не траплялося».

«Якщо порівнювати Facebook із іншими корпораціями, то ситуація з безпекою є значно кращою. А витік 2019 року не був «витоком» у прямому розумінні, адже тоді була зібрана публічна інформація з акаунтів користувачів, але в масовому розмірі», — наголосив експерт.

Тому він переконує, що офіційно зареєстрованих зламів серверів Facebook насправді поки що не було: «Насправді корпорації постійно аналізують свою роботу та роблять відповідні висновки, оскільки розуміють наслідки таких збоїв. Наприклад, цей збій коштував Facebook 6,5 мільярдів доларів. Також такі збої є значними репутаційними ризиками».

Через це, на його думку, компанії несуть значні фінансові втрати й саме тому він вважає, що корпорації передусім зацікавлені у постійному вдосконаленні своїх систем.

Рекомендації щодо захисту приватності

Що ж стосується користувачів, то слід задуматися, де саме зберігати свою особисту інформацію, кому її довіряти і найважливіше — що робити у тому випадку, коли ця інформація зникне з мережі, розповів аналітик. З його слів, неважливо, через які саме технічні причини: відповідь на це питання потрібно знайти до того, як це відбудеться, щоби бути застрахованими від такого можливого колапсу.

«Насамперед користувачі повинні бути обачними, тобто розуміти, яку саме інформацію про себе, своє оточення, сім'ю, платіжні дані куди вони передають. Адже все, що одного разу потрапило до системи інтернет, залишається уже там назавжди», — зазначив Снопченко.

На його думку, хоч компанії є відповідальними за безпеку своїх серверів, остаточна відповідальність за особисті дані є все-таки на самих користувачах: «Користувач має бути обізнаним із наявними механізмами захисту особистих даних у мережі, які надають йому певні сервіси».

Якщо Facebook, Google чи інші сервіси надають можливість використовувати двофакторну аутентифікацію, перевіряти чи є безпечним з'єднання по HTTPS, то люди повинні користуватися цими інструментами з безпеки, запевняє фахівець. Також не слід забувати про антивірусні програми, адже це є технічним засобом для звичайного користувача, щоби перевірити файли на безпечність…». ***(Марк Омелянюк. Що спричинило збій у Facebook і як уберегтися від наступного. Пояснює експерт // АТ «НСТУ» (https://suspilne.media/170886-u-veresni-4g-vperse-otrimali-ponad-80-tisac-ukrainciv-mincifri/). 06.10.2021).***

***

«Google оголосила про плани автоматичного включення додаткового захисту акаунтів 150 млн. користувачів. Система безпеки торкнеться облікових записів тих користувачів, які зареєструвалися в сервісах пошуковика.

Йдеться про двофакторну аутентифікацію — ефективну систему захисту, яка містить як пароль від облікового запису, так і одноразовий код. При спробі входу до акаунту, система відправляє унікальний шифр на смартфон. Навіть якщо хакери зможуть зламати пароль для входу, дістатися до телефону вони не зможуть — саме в ньому і перебуватиме унікальний шифр.

– Двоетапна аутентифікація різко знижує шанси зловмисника отримати доступ до облікового запису, – заявили менеджери з продуків Google Абдель Карим Мардін і Гемма Кім.

Компанія оголосила про нововведення в місяць кібербезпеки, який почався 1 жовтня. Непопулярність подвійного захисту змусив Google піти на крайні заходи — за даними на 2018 рік, аутентифікацією користувалися близько 10% користувачів, що дозволяло хакерам отримати доступ до практично будь-яких облікових записів.

Крім того, ця система захисту тепер стала безшовною — отримати унікальний код для входу можна одним дотиком». ***(Микола Олефіренко. Двохетапна аутентифікація стане обов'язковою в сервісах Google: що це означає // Факти ICTV (https://life.fakty.com.ua/ua/tekhnolohii/dvohetapna-autentyfikatsiya-stane-obov-yazkovoyu-v-servisah-google-shho-tse-oznachaye/). 06.10.2021).***

***

«Роскомнадзор направил запрос сервису Twitch по поводу масштабной утечки. Он потребовал предоставить детальную информацию по этому инциденту.

Запрос направили в американский офис компании, сообщают «Ведомости». Если Twitch не ответит или откажется предоставлять данные в течение месяца, компании грозит штраф до пяти тысяч рублей по статье «непредоставление сведений (информации)».

Источник «Ведомостей» отметил, что в Роскомнадзор могут обратиться граждане, пострадавшие от утечки, и потребовать компенсацию: «Ситуация, когда личные данные пользователей оказываются в свободном доступе, неприемлема. На сегодняшний день жалоб от российских граждан по факту утечки персональных данных пользователей указанного интернет-сервиса в Роскомнадзор не поступало».

В своём Telegram-канале РКН также опубликовал небольшую памятку для граждан, которые хотели бы пожаловаться на разглашение своих персональных данных.

В начале октября текущего года неизвестный хакер опубликовал на 4chan пост под названием «Утечки Twitch, часть первая». Там он оставил ссылку на торрент-файл с архивом на 125 Гб, где содержались исходный код платформы и файлы проекта Vapor — предполагаемого конкурента Steam от Amazon Game Studios. Компания подтвердила «слив». В том же треде опубликовали таблицу с заработком 10 тысяч популярных стримеров с августа 2019 по сентябрь 2021 года, среди них были и российские». ***(Роскомнадзор потребовал от Twitch отчитаться о недавней масштабной утечке // РосКомСвобода (https://roskomsvoboda.org/post/rkn-sprashivayet-s-twitch/). 11.10.2021).***

***

«Консалтинговая компания Accenture подтвердила, что «нерегулярная активность» в ее ИТ-сетях в прошлом квартале, о которой она сообщила в августе, также привела к утечке конфиденциальной информации.

Базирующаяся в Дублине компания Accenture раскрыла утечку данных в пятницу в своем годовом отчете за финансовый год, закончившийся 31 августа, который она подала в качестве формы 10-K в Комиссию по ценным бумагам и биржам США, как впервые сообщил Bleeping Computer.

«В прошлом мы сталкивались, а в будущем мы можем снова столкнуться с инцидентами, связанными с безопасностью данных, в результате несанкционированного доступа к нашим системам и системам наших поставщиков услуг и несанкционированного получения наших данных и данных наших

клиентов, включая: непреднамеренное раскрытие, неправильная конфигурация систем, фишинг, атаки программ-вымогателей или вредоносных программ», - говорится в заявлении Accenture.

«Например, как сообщалось ранее, в течение четвертого квартала 2021 финансового года мы выявили нерегулярную деятельность в одной из наших сред, которая включала извлечение конфиденциальной информации третьей стороной, часть которой была сделана доступной для общественности третьей стороной. вечеринка.»

Компания Accenture впервые подтвердила 11 августа, что стала жертвой атаки, но отказалась сообщить какие-либо дополнительные подробности.

«С помощью наших средств управления безопасностью и протоколов мы выявили нерегулярную активность в одной из наших сред», - заявили в то время в компании Information Security Media Group.«Мы немедленно локализовали проблему и изолировали затронутые серверы. Мы полностью восстановили наши затронутые системы из резервной копии».

Компания добавила: «Никакого влияния на деятельность Accenture или на системы наших клиентов не оказало».

Согласно годовому отчету компании, первая атака произошла где-то в период с июня по август.

LockBit 2.0 берет кредит

Операция LockBit 2.0, предлагающая программу-вымогатель как услугу, взяла на себя ответственность за атаку, указав Accenture на своем сайте утечки данных в качестве жертвы и пригрозив утечкой украденных данных, если консалтинговая компания не заплатит выкуп. Это обычная тактика, используемая группами программ-вымогателей, у которых есть сайты утечки данных, чтобы заставить жертв заплатить выкуп или же служит предупреждением будущим жертвам, что, если они не заплатят, их украденная информация будет сброшена в сеть.

Но эксперты по безопасности предупреждают, что, хотя многие группы утверждают, что украли данные или, в частности, украли конфиденциальную информацию, злоумышленники часто лгути могут либо не украсть ничего ценного, либо вообще ничего.

Украденные данные сбрасываются

Похоже, что Accenture отказалась платить своим злоумышленникам, что привело к тому, что все украденные данные в конечном итоге были сброшены.

На своем сайте утечки LockBit теперь перечисляет для загрузки 2384 каталога, которые, по словам экспертов по безопасности, включают еще больше подкаталогов, как украденные у Accenture. К 22 августа группа закончила утечку украденных данных для бесплатной загрузки со своего сайта утечки данных.«Если вы заинтересованы в покупке баз данных, свяжитесь с нами», - говорится на сайте.

В августе репортер CNBC сообщил, что обзор просочившихся данных Accentureобнаружил то, что, по всей видимости, было «баллами PowerPoints, тематическими исследованиями, цитатами и т.п.».Accenture отказалась комментировать, уведомляла ли она напрямую каких-либо лиц или клиентов о нарушении, например, если личные данные их сотрудников могли быть раскрыты,

или другая информация, имеющая отношение к бизнес-партнерам или клиентам, была украдена.Вместо этого компания снова сослалась на заявление, опубликованное в августе.

Израильская компания по разведке угроз Kela заявляет, что консалтинговые компании входят в число организаций, наиболее уязвимых для атак программ-вымогателей. Несмотря на то, что не все жертвы публично становятся известными, из атак, отслеживаемых в течение последнего месяца жертвами, имена которых были названы через сайты утечки данных, Kela утверждает, что это основные секторы, на которые нацелены:

Производство и промышленные товары: 18% всех зарегистрированных атак программ-вымогателей;

Профессиональные услуги: 16%;

Инжиниринг и строительство: 8%;

Технологии: 8%;

Потребительский сектор и розничная торговля: 7%.

LockBit Keep Recruiting

LockBit работает как программа-вымогатель как услуга, что означает, что основные администраторы разрабатывают и поддерживают портал для вредоносных программ и утечки данных. Аффилированные лица, прошедшие предварительную проверку, принимают программы-вымогатели, заражают жертв и делятся полученной прибылью.

LockBit продолжал публиковать многочисленные сообщения о новых жертвах в последние недели, включая фирму по проектированию компьютерных систем в Нью-Джерси, региональную транспортную организацию Айдахо, корпоративные юридические фирмы в Австралии и Нью-Джерси, а также латиноамериканскую фирму по аутсорсингу бизнес-процессов.

Администраторы LockBit продолжают агрессивно продавать свои программы-вымогатели потенциальным аффилированным лицам, подчеркивая скорость, с которой их вредоносные системы криптоблокировки, утверждая, что никто еще не смог принудительно взломать это шифрование, и заявляя о способности вредоносного ПО распространяться в целевых сетях.

Возможно, неудивительно, что группа заявляет, что стремится нанимать партнеров с относительно продвинутыми навыками работы с программным обеспечением красной команды. «Мы сотрудничаем только с опытными пентестерами, которые являются настоящими профессионалами в таких инструментах, как Metasploit Framework и Cobalt Strike», - говорится в объявлении LockBit о новых филиалах, размещенном на сайте утечки данных.«С нашей помощью вы можете легко получить больше целей за выходные, чем с любой другой партнерской программой за неделю».

LockBit сообщает, что филиалы требуют выкуп.«Только вы решаете во время общения, сколько вам будет платить зашифрованная компания», - говорится в его рекламе.«Вы получаете оплату на свои личные электронные кошельки в любой валюте, после чего переводите нам процент от суммы выкупа».

Группа действительно перечисляет несколько предостережений, которые не станут неожиданностью для опытных аффилированных лиц, главное из которых:

«LockBit 2.0 не работает в постсоветских странах».Это типичное ограничение для русскоязычных групп программ-вымогателей, которые по-прежнемустараются избегать конфликтов с местными властями». ***(Mathew J. Schwartz. Accenture: Ransomware Attack Breached Proprietary Data // Information Security Media Group, Corp. (https://www.govinfosecurity.com/accenture-ransomware-attack-breached-proprietary-data-a-17751). 18.10.2021).***

***

«Почти во всех частях света люди ассоциируют слово «правительство» с порядком. Государственные услуги обеспечивают общественный порядок, экономическую стабильность и безопасность на всех уровнях. Однако последнее десятилетие утечки данных поставило это под сомнение. Федеральные и местные правительства борются с мировыми нарушениями и кибератаками. Недостатки безопасности данных настолько распространены в государственном секторе, что расходы, связанные с утечкой данных, выросли почти на 79% в годовом исчислении.

Как происходит утечка правительственных данных?

Несколько лет назад трудно было представить себе, что правительства станут жертвами кибератак. Общественность и правительства придерживаются высоких стандартов обеспечения безопасности и строгого соответствия данных.Однако государственный сектор включает множество государственных служб.(Посмотрите на вооруженные силы, правоохранительные органы, управление инфраструктурой, общественный транспорт и образовательные учреждения.) Итак, нет недостатка в цифровых следах, которые злоумышленники могут попытаться использовать.

В местных и федеральных органах власти утечка данных связана с любым инцидентом, когда злоумышленники получают доступ или распространяют конфиденциальную или защищенную информацию. Утечки данных могут происходить как физическими, так и цифровыми средствами. Злоумышленники часто комбинируют их с различными формами кибератак. (Вспомните схемы фишинга, атаки программ-вымогателей, вирусы, вредоносное и другое вредоносное ПО.) Утечки данных могут раскрыть конфиденциальные записи, номера социального страхования, финансовую информацию и другие конфиденциальные данные.Между тем строгие законы о конфиденциальности часто защищают их в государственном секторе.

Хорошо известные утечки правительственных данных

К сожалению, кибератаки и утечки данных, влияющие на государственный сектор, с годами становятся все более и более распространенными.Теперь правительства вкладывают большие средства в свои программы кибербезопасности в ответ на растущее количество вариантов атак, нацеленных на них.

В 2015 году злоумышленники взломали личные учетные данные более 190 миллионов избирателей из базы данных избирателей США, включая их имена, адреса, партийную принадлежность и другую личную контактную информацию. Неверно сконфигурированные базы данных избирателей позволили легко показать эту конфиденциальную информацию любому, кто просматривает Интернет. По-прежнему существуют некоторые конкурирующие теории относительно того, как

была вызвана эта утечка, в том числе российские субъекты угрозы. Факт остается фактом: владельцы базы данных недостаточно надежно управляли оцифровкой частных записей. Это открыло двери для ряда проблем с соответствием данных.

7 мая 2019 года злоумышленник ударил по правительственным сетевым системам Балтимора с новым вариантом программы-вымогателя, удерживая все серверы, за исключением основных служб, с целью выкупа. Злоумышленники скомпрометировали личные данные сотен тысяч людей. Это стало возможным из-за плохой ИТ-практики и недостаточного бюджета на технологии или страховки от кибератак.

Совсем недавно, в декабре 2020 года, федеральное правительство США столкнулось с самой серьезной утечкой данных, которую когда-либо видели США, из-за чувствительности получаемой информации и продолжительности нарушения. Это также повлияло на НАТО, правительство Великобритании, Microsoft и Европейский парламент. Нарушение данных не обнаруживалось в течение нескольких месяцев, в результате чего злоумышленники получили доступ к десяткам тысяч человек.

Сколько стоит утечка государственных данных?

Утечка государственных данных может привести к серьезным финансовым потерям. Они также выросли с годами. Согласно отчету о стоимости утечки данных за 2021 год, спонсируемому, анализируемому и публикуемому IBM Security, общие глобальные издержки от утечки данных в государственном секторе выросли почти на 79% в период с 2021 по 2020 год. Это общая средняя стоимость утечки данных в размере 1,93 миллиона долларов. Государственный сектор по-прежнему представляет собой гораздо меньший процент отраслей, затронутых утечкой данных.Однако агрессивный рост соответствующих затрат из года в год начинает показывать, насколько важными стали проекты в области кибербезопасности.

Риски и проблемы безопасности данных в правительстве

Сегодня государственным учреждениям предстоит нелегкая битва в борьбе с растущим всплеском кибершпионажа и вымогательства. Сейчас, как никогда ранее, государственному сектору необходимо сосредоточить внимание на своих мерах по усилению безопасности на всех уровнях инфраструктуры. В то же время сектору также необходимо поддерживать адекватные бюджеты для поддержки своих усилий по управлению данными и восстановлению после сбоев.

Государственные организации теперь имеют гораздо более явную цифровую мишень за спиной. Новое поколение злоумышленников с радостью принимает аспект утечки данных в государственном секторе, связанный с высоким риском и высоким вознаграждением. Таким образом, местные и федеральные органы власти должны провести тщательный анализ уязвимости. Им следует всесторонне изучить конфигурации баз данных и их соответствие требованиям конфиденциальности.

Очень немногие отрасли защищены от финансовых последствий утечки данных. 2021 год также показал нам, что злоумышленники сосредоточили свое внимание на государственном секторе. Это вызывает чувство безотлагательности для местных и федеральных властей. Им необходимо быть в курсе всех аспектов своей безопасности, сохраняя при этом конфиденциальность и защиту данных наивысшими приоритетами». ***(Josh Nadeau. Exploring the Costs, Risks and Causes***

of a Government Data Breach // IBM (https://securityintelligence.com/articles/costs-risks-causes-government-data-breach/?category=data-protection). 20.10.2021).

***

«Bitdefender выпустил отчет, в котором показано, как потребители различных возрастных групп и социально-демографических групп ведут себя на популярных платформах, приложениях и устройствах, влияя на риск кибербезопасности. Результаты показывают, что основные методы защиты данных, защиты личных данных и обмена информацией отсутствуют, несмотря на возросшие угрозы и повышенную озабоченность по поводу киберпреступности.

«Понимание тенденций поведения потребителей в области безопасности в Интернете имеет решающее значение для усиления кибербезопасности в обществе в целом», - сказал Богдан Ботезату, директор по исследованиям угроз и отчетности Bitdefender.

«Киберпреступники постоянно изучают новые способы использования человеческих слабостей для кражи конфиденциальных данных, вымогательства денег или закрепления внутри систем. Понимая повседневные практики кибербезопасности, мы можем лучше оценивать потенциальные риски и уязвимости, чтобы обучать потребителей способам более эффективной защиты, например, как использовать технологии предотвращения, обнаружения и защиты цифровых данных, чтобы предотвратить успешные атаки ».

В отчете, основанном на опросе, в ходе которого было опрошено более 10 000 потребительских интернет-пользователей в 11 странах, изучается использование популярных онлайн-платформ и сервисов, методы личной кибербезопасности, уровень подверженности угрозам и многое другое.

Повседневные практики кибербезопасности

Плохие пароли по-прежнему распространены- пятьдесят процентов опрошенных заявили, что они используют один пароль для всех онлайн-учетных записей, а 32% используют всего несколько паролей и повторно используют их для нескольких учетных записей. Двадцать семь процентов респондентов используют простые пароли, такие как 1234, для блокировки своих мобильных телефонов, а 11% вообще не блокируют свои мобильные телефоны. Простые пароли чаще всего используют молодые люди в возрасте от 18 до 44 лет, и мужчины чаще, чем женщины, сообщают, что используют простые пароли (31% по сравнению с 23%).

Многие не используют программное обеспечение для защиты кибербезопасности на мобильных телефонах. Удивительно, но почти 35% заявили, что не используют антивирус на своих мобильных телефонах. Наиболее частыми причинами этого были: 30% считают, что мобильным телефонам это не нужно, 22% считают, что это слишком дорого, и 16% считают, что безопасность встроена. Кроме того, в среднем 41% не используют частные браузеры и 52 % не используют VPN.

Мошенничество с мобильными телефонами является ведущим источником угроз - 61% респондентов заявили, что они столкнулись как минимум с одной угрозой мобильной кибербезопасности за последние 12 месяцев. Мошенничество с мобильными телефонами, включающее нежелательные текстовые сообщения и

звонки, было наиболее частой угрозой, отмеченной в опросе (36%), за ней следовали фишинг (23%), утечки данных (12%), имитация социальных сетей (11%), финансовое мошенничество (9%) и программы-вымогатели (8%). %.

Хотя немногие респонденты лично сталкивались с финансовым мошенничеством, он получил самый высокий рейтинг с точки зрения обеспокоенности: 41% заявили, что очень обеспокоены угрозой. Возрастная группа, наиболее обеспокоенная общими угрозами, - это люди в возрасте от 35 до 44 лет, за которыми следуют люди в возрасте от 25 до 34 лет.

Отсутствие надзора за детьми создает значительные риски для безопасности- родителей спрашивали, насколько они контролируют поведение своих детей в Интернете и установку приложений. Поразительно, но опрос показал, что в среднем 36% детей имеют полностью неконтролируемый доступ к компьютерам, мобильным телефонам и планшетам. Соединенные Штаты возглавили все другие страны в опросе с неконтролируемым доступом, приближающимся к 50%, по сравнению со всеми другими странами, которые сообщили о менее чем 40%.

Большинство потребителей сильно подвержены риску- при анализе всего поведения респондентов, от повторного использования пароля до количества онлайн-учетных записей и услуг, до обмена данными учетных записей и отсутствия служб безопасности на их устройствах, почти 60% потребителей были признаны «открытыми» или «скорее разоблачены».Лишь 11% респондентов можно охарактеризовать как «безопасные» с точки зрения их практики кибербезопасности.

Поведение в Интернете

Смартфоны чаще всего используются для доступа к онлайн-сервисам- 74% респондентов в основном получают доступ к онлайн-сервисам с помощью личного смартфона, а 61% из них используют операционную систему Android. Персональные ноутбуки заняли второе место с 45%, за ними следуют Smart TV с 30% и персональные настольные компьютеры с 28%.23% сообщают об использовании хотя бы одного рабочего устройства для доступа к личным онлайн-аккаунтам.

У большинства из них есть учетные записи в социальных сетях и онлайн-магазины - 63% респондентов сообщили, что у них есть учетные записи в социальных сетях, а 54% - учетные записи для онлайн-покупок. Среди других наиболее часто используемых услуг - потоковое видео - 40%, телекоммуникационные и медицинские платформы - 29% и коммунальные услуги - 28%.

Возраст и пол влияют на поведение цифровых платформ. В среднем на одного респондента используется восемь онлайн-платформ, поэтому в трех основных используемых платформах (Facebook, WhatsApp и Gmail) наблюдаются ключевые различия между возрастными группами и полом. На 51% женщины используют Facebook больше, чем мужчины (42%).В возрастной группе от 35 до 44 лет вероятность использования WhatsApp на 21% выше, чем у людей в возрасте от 18 до 22 лет, которые также на 26% реже используют Gmail по сравнению с людьми 55-65 лет.

Большинство пользователей понимают настройки конфиденциальности. Положительный вывод о конфиденциальности в Интернете показывает, что 51% пользователей знают, как изменить настройки конфиденциальности интернет-браузера, а 46% читают политики конфиденциальности при регистрации новых учетных записей. Однако 46% также заявляют, что им не нравится выбирать новые пароли для каждой новой учетной записи, а 38% не любят требования использовать многофакторную аутентификацию.

Персональные идентификационные данные обычно используются совместно- Персональные идентификационные данные, включая имя, дату рождения и даже физический адрес, обычно передаются в Интернете, причем мужчины с большей вероятностью поделятся своими данными, чем женщины. Пол - самая распространенная деталь, которую всегда или почти всегда сообщают 54% респондентов, за ней следуют имя (43%), личный адрес электронной почты и дата рождения (40%) и физический адрес (29%).Молодые люди в возрасте от 18 до 24 лет чаще делятся своей личной информацией, чем представители других возрастных групп». ***(Everyday cybersecurity practices inadequate among many online consumers // Help Net Security (https://www.helpnetsecurity.com/2021/10/14/everyday-cybersecurity-practices/). 14.10.2021).***

***

«На прошлой неделе Аргентина пострадала от одной из самых катастрофических утечек данных из возможных, поскольку доступ к правительственной базе данных, содержащей информацию о национальных удостоверениях личности каждого гражданина, был обнаружен для продажи в даркнете.

Национальный реестр лиц содержит изображения всех национальных удостоверений личности, выданных правительством, вместе со всей информацией, напечатанной на карточке в текстовом формате для облегчения поиска. В качестве доказательства взлома хакер опубликовал фотографии и личную информацию 44 знаменитостей страны, предложив за определенную плату просмотреть данные любого гражданина Аргентины.

Правительственная база данных взломана; неясно, были ли данные украдены, или виноват инсайдерский доступ

Registro Nacional de las Personas (RENAPER), или Национальный реестр лиц, представляет собой центральную правительственную базу данных, поддерживаемую Министерством внутренних дел Аргентины и широко используемую различными агентствами страны для поиска личной информации граждан. База данных содержит отсканированные изображения каждой выданной национальной идентификационной карты, а также текстовые записи отображаемой на них информации: полные имена, фотография лица, домашний адрес, национальный идентификационный номер, используемый для налоговых целей и трудоустройства, а также обработка штрих-кодов. используется внутренними системами.

Правительство Аргентины не считает, что это была утечка данных в том смысле, что посторонние проникли в систему и украли сохраненные

данные.Вместо этого они полагают, что сотрудник Министерства внутренних дел с авторизованным доступом к государственной базе данных предлагает информацию для продажи. В пресс-релизе агентства указано, что восемь сотрудников находятся под следствием на предмет возможной роли. Агентство также указало, что одна из его учетных записей VPN использовалась для запроса базы данных незадолго до того, как злоумышленник разместил в Twitter фотографии субъектов поиска.

Эта теория может быть связана с темным веб-листингом злоумышленника, который не предлагает на продажу какую-либо часть правительственной базы данных.Вместо этого листинг предлагает услуги поиска по именам, несмотря на то, что также утверждается, что он имеет полный доступ к информации о 45 миллионах зарегистрированных граждан страны. Это кажется очень трудоемким и рискованным способом заработать на взломе, который можно быстро отключить, отключив скомпрометированные учетные данные.Теория сотрудника, имеющего доступ за пределами одной конкретной учетной записи, имеет больше смысла, чем сторонняя сторона, которая пытается бесконечно использовать одну взломанную VPN для постоянного поиска денег.

Со своей стороны, злоумышленник утверждает, что он посторонний и что он украл все содержимое правительственной базы данных. Прежде чем аккаунт злоумышленника был заблокирован в Твиттере, он опубликовал личную информацию 44 аргентинских знаменитостей, включая Лионеля Месси и Серхио Агуэро, а также президента Альберто Фернандеса. Они также заявили, что могут предоставить информацию «от одного до двух миллионов человек» в качестве доказательства, хотя учетная запись, похоже, была удалена до того, как это произошло. Злоумышленник утверждает, что они взломали VPN, но это произошло из-за «неосторожных сотрудников», а не из-за внутренней угрозы.

Хронические проблемы с кибербезопасностью национального правительства Аргентины?

Взлом последовал за инцидентами «La Gorra Leaks», которые произошли в 2017 и 2019 годах, каждый из которых касается государственных счетов и баз данных.В ходе первоначального инцидента 2017 года была взломана учетная запись электронной почты и Twitter министра безопасности Аргентины, и хакер опубликовал скриншоты изображений и файлов. Инцидент получил больше освещения из-за реакции, чем из-за нарушения, поскольку эксперты по безопасности, освещавшие взлом и политическую оппозицию, подверглись рейдам только за то, что опубликовали об этом в блогах и социальных сетях. Эта закономерность повторилась в 2019 году, когда неизвестный хакер утекло 700 ГБ информации из государственных баз данных (около 200000 файлов PDF) на форумах и платформах обмена сообщениями в темной сети. Эта информация привела в замешательство некоторых политиков и сотрудников правоохранительных органов.

Само правительство также было источником беспокойства по поводу безопасности. В 2018 году и федеральное правительство, и город Буэнос-Айрес попытались принять меры, позволяющие правоохранительным органам использовать вредоносное ПО в рамках уголовных расследований. Законопроекты

подверглись широкой критике за отсутствие элементарной защиты конфиденциальности и безопасности и в конечном итоге были отклонены.

Тони Пеппер, генеральный директор Egress, взвесил риск, с которым столкнутся граждане Аргентины, если их национальные удостоверения личности будут бесплатно доступны в даркнете для всех, кто готов платить: «Учитывая, что данные миллионов подвергаются риску, граждане Аргентины теперь являются основными целями для последующие атаки, такие как финансовое мошенничество, изощренные попытки фишинга и мошенничество с выдачей себя за другое лицо, нацеленные на дальнейшую кражу личных данных, личных данных и даже их денег».

Ряд других экспертов по безопасности взвесили, что нужно изменить, чтобы защитить эти чрезвычайно конфиденциальные правительственные базы данных.По словам Сарью Найяра, генерального директора Gurucul: «Это демонстрирует необходимость для всех организаций использовать аналитику и машинное обучение для поиска и выявления необычных действий в сети. Маловероятно, что законному сотруднику понадобится скачать все записи. Хорошее аналитическое решение могло бы использовать данные в реальном времени, чтобы быстро выявить эту аномалию, что позволило бы исправить это до завершения загрузки ».

А Раджив Пимпласкар, главный исполнительный директор Veridium, видит в биометрии ответ: «Национальные системы идентификации должны отказаться от аутентификации на основе знаний (KBA), такой как PIN или пароли, и использовать биометрические методы, такие как лицо и отпечаток пальца. Биометрия снижает риск кражи учетных данных и бокового перемещения, которое может увеличить количество утечек данных.Доступны несколько бесконтактных биометрических решений, к которым можно получить доступ через потребительские смартфоны, что позволяет использовать различные варианты использования удаленной регистрации и проверки.Такие методы должны быть независимыми от устройств, чтобы обеспечить постоянный доступ и удобство использования для всех граждан, независимо от марки и модели их мобильного телефона». ***(SCOTT IKEDA. Argentinian Government Database Containing ID Card Information of Entire Country Made Available on Dark Web Forum // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/argentinian-government-database-containing-id-card-information-of-entire-country-made-available-on-dark-web-forum/). 25.10.2021).***

***

«Еще одно нарушение безопасности третьей стороной было зарегистрировано в Сингапуре, на этот раз затронувшее пациентов Fullerton Health и скомпрометировавшее личные данные, которые в «некоторых случаях» включали данные банковского счета. Затронутый поставщик Agape Connecting People, платформа которого упрощает запись на прием, впервые обнаружил нарушение 19 октября и, по-видимому, затронуло только Fullerton Health.

Поставщик медицинских услуг заявил, что ни одна из его собственных ИТ-систем, сети и баз данных не пострадала от взлома. Он подал отчеты как в

полицию, так и в Комиссию по защите личных данных, которая курирует Закон Сингапура о защите личных данных.

Компания Agape впервые обнаружила вторжение 19 октября и «немедленно приняла меры», чтобы изолировать и приостановить использование системы, говорится в заявлении поставщика в понедельник.

«Ни одна из наших основных инфраструктур не была взломана», - сказано в сообщении, добавив, что нарушение «похоже» ограничивается Fullerton Health. Однако он отметил, что все еще находится в процессе подтверждения того, что никакие другие клиенты не пострадали.

Описывая себя как социальное предприятие, Agape управляет контактным центром для обеспечения занятости малообеспеченных слоев населения, включая сокамерников, инвалидов, бывших преступников и матерей-одиночек. Он рассчитан на более чем 250 мест и призван к 2022 году оказать поддержку 1000 малоимущим лицам.

Agape заявила, что работает с экспертами по кибербезопасности над внедрением «смягчающих мер», чтобы минимизировать дальнейшее воздействие от взлома.

21 октября компания Fullerton Health сообщила, что «несколько дней назад» она была предупреждена о том, что личные данные ее клиентов могли быть раскрыты, и начала расследование. Было обнаружено, что неавторизованная сторона получила доступ к серверу, используемому Агапе, скомпрометировав личные данные пациентов, с которыми Агапе помогала записываться на прием.

Такие сведения включали имена, идентификационные номера и контактные данные, а также данные банковского счета в «некоторых случаях» и «определенную ограниченную информацию, связанную со здоровьем».По сообщению Fullerton Health, информация о кредитных картах или пароли не просочились. Компания обслуживает корпоративных клиентов и их сотрудников, у одного из которых, по крайней мере, было подтверждено, что их личные данные потенциально раскрыты.

Компания Fullerton Health заявила, что все еще работает над установлением числа и личности лиц, пострадавших от взлома. Специалисты по цифровой криминалистике и кибербезопасности были привлечены для помощи в расследовании, сказал поставщик медицинских услуг, добавив, что они также пытались определить основную причину и полную степень нарушения.

«Мы проводим тщательный анализ наших процессов и протоколов, касающихся безопасности данных и использования сторонних поставщиков услуг для дальнейшего усиления нашей информационной безопасности», - сказал Фуллертон Хелс.

Он сказал, что данные, касающиеся вакцинации COVID-19, проведенной в его центрах вакцинации, не были скомпрометированы, поскольку информация хранилась отдельно в системе, не переданной Agape.

В прошлом году в Сингапуре произошла волна атак на цепочки поставок, в результате которых были скомпрометированы личные данные, в частности, 580 000часто летающих пассажиров Singapore Airlines (SIA), 129 000 клиентов Singtel и

30 000 человек в результате инцидента, связанного с организацией e2i по подбору вакансий.

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, при этом заметно увеличилось количество программ-вымогателей, онлайн-мошенничества и фишинговых действий, связанных cCOVID-19, говорится в отчете Cyberзаиюль 2021 года. Агентство безопасности Сингапура (CSA).

Количество зарегистрированных атак программ-вымогателей резко увеличилось на 154% в 2020 году, когда было 89 инцидентов, по сравнению с 35 в 2019 году. В основном они затронулималый и средний бизнес(SMB) в различных секторах, включая производство, розничную торговлю и здравоохранение».***(Eileen Yu. Third-party data breach in Singapore hits healthcare provider // ZDNet (https://www.zdnet.com/article/third-party-data-breach-in-singapore-hits-healthcare-provider/). 26.10.2021).***

***

«Верховный суд Индии назначил независимую комиссию для расследования утверждений о том, что шпионское ПО, продаваемое правительствам, использовалось для взлома телефонов депутатов, активистов и журналистов.

Постановление Верховного суда последовало за многочисленными петициями о расследовании утверждений о незаконном слежении.

Номера телефонов целей были в базе данных, которая, как полагают, представляет интерес для клиентов израильской фирмы NSO.

Список просочился в основные новостные агентства 18 июля.

Индийский сайт новостей и общественного мнения The Wire и газета Indian Express были среди 16 международных СМИ, расследовавших список утечек и использование шпионского ПО Pegasus по всему миру.

НСО отрицает какие-либо нарушения. В нем говорилось, что программное обеспечение предназначалось для отслеживания преступников и террористов и продавалось только военным, правоохранительным органам и спецслужбам из стран с хорошей репутацией в области прав человека.

Суд дал комитету, который возглавит бывший судья Верховного суда, восемь недель на расследование обвинений.

Разоблачение шпионского ПО вызвало вопросы о том, незаконно ли индийское правительство следило за своими критиками, а в некоторых случаях даже за своими министрами.

Правительство назвало эти разоблачения «в высшей степени сенсационным» глобальным заговором.

Он утверждал, что не смог раскрыть никакой информации об использовании Pegasus по соображениям национальной безопасности. Тем не менее, он предложил сформировать комитет экспертов, чтобы изучить этот вопрос и «развеять любые неправильные рассказы».

В среду главный судья Индии Н.В. Рамана заявил, что суд назначает комитет под его надзором, чтобы «исследовать ложь и раскрыть правду», согласно индийскому сайту Bar and Bench.

Судья сказал, что предполагаемое нарушение неприкосновенности частной жизни требует рассмотрения, поскольку оно затрагивает права и свободы людей.Он добавил, что такая технология может также иметь «сдерживающий эффект» на свободу прессы в Индии.

Разоблачения Pegasus вызвали протесты в стране, и лидеры оппозиции подняли этот вопрос в парламенте Индии во время его сессии в сезон дождей.

Непонятно, откуда взялся этот список и сколько телефонов было взломано. Но из просочившейся базы данных, содержащей 500 000 номеров, более 300, как сообщается, принадлежат индийцам.

В число потенциальных целей входили основные лидеры оппозиции, активисты и официальные лица.

Несколько активистов и журналистов, в том числе те, которые, как сообщается, стали мишенью для шпионского ПО, обратились с просьбами о получении ответов от правительства вместе с запросом, проводимым действующим или вышедшим в отставку судьей высшего суда.

Петиции были объединены Верховным судом, который начал слушание дела 5 августа.

Во время слушания дела правительство подало «ограниченные показания под присягой», утверждая, что обвинения основаны на предположении и что «обвинения не имеют под собой никакого основания».

Генеральный солиситор Тушар Мехта также утверждал, что такие вопросы не могут быть предметом общественного обсуждения. «Ни одно правительство не будет обнародовать, какое программное обеспечение оно использует, чтобы позволить террористическим сетям изменять свои системы и избегать отслеживания», - сказал он.

Суд отметил, что он не хотел заставлять правительство раскрывать информацию о безопасности, а хотел только информацию о том, были ли перехвачены телефоны людей». ***(Pegasus row: India's top court orders probe into snooping allegations // BBC (https://www.bbc.com/news/world-asia-india-59059489). 27.10.2021).***

***

«Итальянский орган по защите данных Garante per la Protezione dei Dati Personali (GPDP) объявил о расследовании нарушения данных национального агентства по защите авторских прав.

Societa Italiana degli Autori ed Editori (SIAE) - это государственное учреждение, ответственное за защиту прав интеллектуальной собственности на творческие работы правообладателей.

Вчера GPDP объявила, что расследует, не украли ли хакеры личные данные зарегистрированных членов и сотрудников SIAE во время атаки с использованием программ-вымогателей.

«В отношении утечки данных, нанесенной Siae, Гарант защиты личных данных сообщает, что он начал расследование.

Итальянское общество авторов и издателей вчера уведомило Управление в рамках условий, установленных законодательством о конфиденциальности, о нарушении работы его серверов в результате хакерской атаки с целью вымогательства.

В настоящее время Гарант оценивает информацию, полученную от Компании, оставляя за собой право провести соответствующие расследования», - GPDP.

SIAE не ответила на электронные письма BleepingComputer с просьбой пояснить масштаб воздействия.

Данные, украденные во время атаки программы-вымогателя

Тем не менее, BleepingComputer обнаружил на портале вымогателей банды вымогателей Everest запись, в которой участники утверждали, что взломали SIAE и утекли 60 ГБ украденных данных.

Утечка данных банды Эвереста включает сканирование национального удостоверения личности и водительских прав, а также документы, относящиеся к контрактным соглашениям между SIAE и его членами.

Банда Everest утверждает, что украденные данные содержат контракты и другие данные, касающиеся итальянских знаменитостей, актеров, музыкантов, художников, авторов и авторитетных авторов в целом.

Поскольку SIAE является единственным сборщиком роялти в Италии, каждый создатель в стране имеет регистрацию на взломанной платформе.

Не получив выкупа, злоумышленники продают данные за 500 000 долларов…». ***(Bill Toulas. Italian celebs' data exposed in ransomware attack on SIAE // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/italian-celebs-data-exposed-in-ransomware-attack-on-siae/). 22.10.2021).***

***

«Киберпреступники предлагают приобрести базу с персональными данными автовладельцев, которые были зарегистрированы в Москве и Московской области с 2006 по 2020 годы. База содержит 50 миллионов записей.

Как сообщает «Коммерсантъ», на одном из форумов, специализирующихся на продаже баз данных и организации утечек информации, выставлен на продажу архив базы данных ГИБДД, который содержит 50 миллионов записей о водителях Москвы и Подмосковья. Стоимость архива – всего 800 долларов. По словам продавца, с которым связалось издание, в базе содержатся данные с 2006 по 2019 годы, но бонусом к покупке предлагаются данные 2020 года.

В образце базы содержатся следующие данные: модель и марка автомобиля, его регистрационный и VIN-номер, дата постановки научёт, мощность двигателя, ФИО владельца, дата его рождения, а также номер телефона. Продавец утверждает, что получил информацию от источника вГИБДД. Издание связалось с несколькими автовладельцами из образца базы, и все они подтвердили подлинность содержащейся там информации.

Базы данных ГИБДД уже нев первый раз выставляют на продажу: в августе 2020 года в интернете появилась база из миллиона строк с персональными данными столичных водителей — на профильных форумах стоимость таких баз разных лет варьируется от одной до 15 тысяч долларов. Все данные о зарегистрированных машинах и автовладельцах сегодня хранятся централизованно в Федеральной информационной системе (ФИС) ГИБДД.

Однако раньше у каждого регионального управления ГИБДД была собственная база, куда отгружались данные. Москва и Московская область до 2020 года могли отгружать данные параллельно в ФИС ив свои системы, затем перестали, и сейчас региональные системы выводятся из эксплуатации. Один источник издания предполагает, что утечка могла произойти на уровне регионов, другой уверен, что база могла быть получена в результате внешнего воздействия — например, путём эксплуатации уязвимости в системном программном обеспечении». ***(Александр Пономарёв. 50 миллионов записей об автовладельцах Москвы и Подмосковья выставили на продажу // Популярная Механика (https://www.popmech.ru/technologies/news-763763-50-millionov-zapisey-ob-avtovladelcah-moskvy-i-podmoskovya-vystavili-na-prodazhu/). 22.10.2021).***

***

«Американская компания Facebook подала иск в суд против гражданина Украины Александра Солонченко, который якобы украл и продал в даркнете личные данные 178 млн пользователей социальной сети.

Facebook утверждает, что в период с января 2018 года по сентябрь 2019 года Солонченко получил доступ к идентификационным данным аккаунтов и телефонным номерам 178 млн пользователей соцсети. По данным компании, для этого он применял специальное программное обеспечение, в автоматическом режиме направлявшее пользователям запросы через приложение Messenger.

В мае 2021 года господин Солонченко, на теневом форуме под ником solomame (в январе этого года сменил на barak_obama), как уточняется в иске, продал полученные данные на онлайн-форуме Raid Forums. Он также бесплатно выложил в интернете данные 10 млн пользователей украинского Приватбанка и французской аналитической компании, утверждают в Facebook. Для этого он создал специальную программу, имитирующую работу Android-приложения.

«Солонченко действовал в нарушение условий предоставления услуг и правил платформы», — указывается в исковой жалобе. Руководство Facebook рассчитывает, что суд обяжет Солонченко возместить ей ущерб и запретит ему пользоваться сервисами компании.

Позже этот же механизм был использован другими людьми для сбора уже 533 млн. строк, которые потом появились в открытом доступе». ***(Facebook обвинила украинца в краже данных 178 млн пользователей // SecurityLab.ru (https://www.securitylab.ru/news/525883.php). 23.10.2021).***

***

«FIN7, финансово мотивированная группа угроз, которая на протяжении шести лет нацелена на розничную торговлю, рестораны и гостиничный бизнес в США, создала веб-сайт, изображающий из себя охранную компанию для набора талантов, по данным компании Gemini Advisory, занимающейся разведкой мошенничества.

В отчете говорится, что группа угроз рекламировала вакансии в поддельной компании под названием Bastion Secure на российских порталах вакансий. Он добавляет, что цель мошенничества заключалась в том, чтобы заманить исследователей безопасности, которые могли бы помочь группе с помощью действий, связанных с тестированием на проникновение, чтобы обеспечить атаки программ-вымогателей.

Открытие

Gemini Advisory обнаружила мошенничество, когда источник сообщил компании, что с ними связались представители Bastion Secure, чтобы подать заявку на должность ИТ-специалиста. Хотя внешне веб-сайт казался легитимным, анализ его исходного кода показал, что он был фальшивым, говорят исследователи. Фактически, его код был идентичен коду законной компании по кибербезопасности Convergent Network Solutions, добавляют они.

Исследователи отмечают, что большинство страниц на сайте вернули ошибку 404, написанную на русском языке, что свидетельствует о происхождении его создателей. В прошлом группа FIN7 проводила аналогичные аферы. В 2018 году прокуратура обнаружила фальшивую компанию Combi Security, которая якобы занималась тестированием на проникновение и консультированием по вопросам безопасности...

Еще одним указателем на причастность FIN7, по мнению исследователей, была банда, использовавшая российские порталы вакансий, такие как zoon.ru, для процесса найма. По их словам, во время аферы Combi Security группа угроз разместила объявления о вакансиях на российских, украинских и узбекских сайтах по трудоустройству.

Ссылки на портале вакансий направляли пользователей на заблокированный в настоящее время веб-сайт www [.] Bastionsecure [.] Com. Архивные записи с четверга, проверенные Information Security Media Group, показывают, что злоумышленники, выдавая себя за Bastion Secure, заявили в объявлениях о вакансиях, что нанимают инженеров-реверс-инженеров, системных администраторов и программистов PHP, Python и C ++.

В нижнем колонтитуле веб-сайта были указаны контактные данные потенциальных сотрудников, включая адрес электронной почты и номер телефона в Израиле.The Wall Street Journal сообщает, что не получил ответа, когда написал на адрес электронной почты, но когда он позвонил по номеру телефона, русскоговорящий человек на стороне получателя звонка сказал: «Я просто человек. У меня есть не имеет ничего общего с какой-либо компанией, занимающейся кибербезопасностью».

Процесс найма

Используя информацию, предоставленную неизвестным источником Gemini Advisory, с которым Бастион связался с просьбой о приеме на работу, исследователи объяснили три этапа процесса найма:

Этап 1: Интервью с персоналом

Человек, представившийся представителем отдела кадров из Bastion Secure, связался с источником Gemini Advisory и спросил их, заинтересованы ли они в работе ИТ-специалистами в компании. Как только источник проявил интерес, они дали интервью в платформе обмена сообщениями Telegram. После собеседования их попросили сдать тестовые задания, подписать соглашение о неразглашении и загрузить несколько виртуальных машин на свой компьютер.

Этап 2: Задания

На втором этапе источнику было предложено установить определенные платформы и предоставить задания, «типичные для должности», по словам исследователей. Bastion также предостерег источника от установки антивирусного программного обеспечения на устройство и посоветовал им использовать только предписанные компанией инструменты или столкнуться с серьезными штрафами. Людям, заинтересованным в изучении новых инструментов, были предоставлены дополнительные ресурсы, которые можно было использовать как для законного тестирования на проникновение, так и для злонамеренных действий. Представитель Bastion Secure сообщил источнику, что эти инструменты помогут им управлять системами своих клиентов и обезопасить себя.

Этап 3: «Реальные» задания

Исследователи говорят, что на третьем и последнем этапе собеседования источнику было дано «реальное» задание, в котором его попросили провести тест на проникновение против одного из клиентов Bastion Secure. По словам исследователей, это насторожило источник, который сообщил исследователям, что Bastion Secure предоставляет доступ к сети клиента без каких-либо юридических расследований или документации и его интересуют только файловые системы и резервные копии.

По мнению исследователей, этот шаг означает, что «FIN7 продолжает расширяться в сферу программ-вымогателей».Аналитик по безопасности в Microsoft Ник Kapp сказал на саммите Mandiant Cyber Defense в сентябре, что FIN7 произвела программное обеспечение, использовавшееся во взломе, нарушившем деятельность Colonial Pipeline Co., сообщает The Wall Street Journal.

Старая тактика, новый поворот

Хотя этот процесс не нов, интересно посмотреть, как группы угроз отфильтровывают неподходящих кандидатов, говорит Роджер Граймс, пропагандист защиты на основе данных в компании по кибербезопасности KnowBe4.

«Эта [афера с набором персонала] продолжается уже несколько десятилетий, особенно в Индии, России и Китае. На всех крупных сайтах вакансий полно вакансий для злонамеренных компаний. Интересно то, как быстро они отфильтровывают кандидата, который придерживается этических норм и правил. заинтересован в том, чтобы не нарушать закон», - сказал он ISMG.

«Компании, занимающиеся вредоносным ПО, ищут самых сильных разработчиков, которых они могут найти, поэтому они рекламируют все необходимые навыки и требования для работы. Когда они подключаются к кандидату и начинают начальное собеседование, если кандидат задает какие-либо вопросы, которые могут указывать на то, что кандидат может иметь проблемы с намерением того, что он может делать, он немедленно отключается», - добавляет он.

Привлечение специалистов по безопасности для выполнения тяжелой работы по получению доступа к цели - которая затем будет настроена на то, чтобы взять на себя ответственность за любую обнаруженную преступную причастность - «в каком-то смысле блестяще», - говорит Крис Клементс, вице-президент по архитектуре решений. в Cerberus Sentinel.

«Учитывая низкую сумму объявленной оплаты труда, цели набора, вероятно, будут низкоквалифицированными или в очень бедных регионах мира. Опытные тестеры проникновения в развитом мире могут получать зарплату, во много раз превышающую ту, что, по-видимому, предлагает FIN7. Тем не менее, это указывает на то, что «Банды программ-вымогателей все чаще прибегают к целевым атакам на конкретных жертв, а не к бессистемным подходам … для компрометации целей», - говорит он ISMG.

Действие предпринято

Gemini Advisory отправила правоохранительным органам копию отчета, который, по его словам, был отредактирован только для публичного просмотра, чтобы защитить его источник.

В качестве превентивной меры гигант поисковых систем Google добавил доменное имя www [.] Bastionsecure [.] Com в свой черный список безопасного просмотра…». ***(Mihir Bagwe. FIN7 Sets Up Fake Pentesting Company Site to Recruit Talent // Information Security Media Group, Corp. (https://www.govinfosecurity.com/fin7-sets-up-fake-pentesting-company-site-to-recruit-talent-a-17783). 22.10.2021).***

***

«Государственный субъект, стоящий за кибератакой 2020 года, нацеленной на клиентов SolarWinds - Nobelium - продолжает свою кампанию по нацеливанию на глобальную цепочку поставок ИТ, согласно новому сообщению Microsoft, в котором говорится, что 140 торговых посредников и поставщиков технологических услуг были уведомлены о том, что они были подверглись нападению группы, и 14 были взломаны.

Microsoft предупреждает, что компания Nobelium, которую правительство США подключило к российской службе внешней разведки (SVR), теперь нацелена на партнеров, которые настраивают, развертывают и управляют облачными сервисами. Несколько экспертов по кибербезопасности утверждают, что это еще одно доказательство того, что российское правительство предпримет решительные шаги для сбора конфиденциальной информации.

В техническом руководстве, выпущенном вместе с рекомендацией, Microsoft предупреждает, что последняя тактика Nobelium не пытается использовать

уязвимости программного обеспечения. Вместо этого группа, как сообщается, использует спрей паролей, кражу токенов, злоупотребление API и целевой фишинг для взлома учетных записей пользователей и получения привилегированного доступа.

Том Берт, корпоративный вице-президент Microsoft по безопасности и доверию клиентов, говорит в консультативном заключении: «Мы считаем, что в конечном итоге Nobelium надеется использовать любой прямой доступ, который могут быть у торговых посредников к ИТ-системам своих клиентов, и с легкостью выдать себя за надежного технологического партнера организации. получить доступ к своим клиентам, находящимся ниже по цепочке.

«К счастью, мы обнаружили эту кампанию на ранних стадиях», - продолжает Берт, отмечая, что Microsoft начала наблюдение за деятельностью в мае 2021 года. «И мы делимся этими разработками, чтобы помочь [пострадавшим] принять своевременные меры, чтобы гарантировать, что Nobelium не будет более успешный.»

Nobelium APT: активная угроза

Microsoft добавляет, что эти атаки являются частью более широкой волны активности Nobelium в 2021 году. В период с 1 июля по 19 октября, говорится в сообщении, Microsoft сообщила 609 клиентам, что они подвергались атакам со стороны Nobelium 22 868 раз, хотя процент успешных попыток был ниже. младшие однозначные цифры.Для сравнения, Microsoft заявляет, что до 1 июля 2021 года она уведомляла клиентов об атаках на национальные государства 20 500 раз за три года.

Чарльз Кармакал, старший вице-президент и технический директор компании по обеспечению безопасности Mandiant, которая помогала идентифицировать эту новую волну активности, добавляет: «Этот путь атаки очень затрудняет обнаружение организациями-жертвами того, что они были скомпрометированы, и расследование действий, предпринятых угрозой. актер.

«[Это] смещает первоначальное вторжение с конечных целей, которыми в некоторых ситуациях являются организации с более развитой киберзащитой, на более мелких технологических партнеров», - продолжает Кармакал. «Подобно виктимологии, наблюдаемой в кампании 2020 года, целями этого вторжения, по-видимому, в конечном итоге становятся правительственные организации и другие организации, которые занимаются вопросами, представляющими интерес для России».

Джейк Уильямс, бывший член элитной хакерской команды Агентства национальной безопасности, соучредитель и технический директор охранной фирмы BreachQuest, называет Nobelium «поистине стойким противником» и предупреждает, что это «один из лучших игроков в экосистеме угроз. оставаясь незамеченным после попытки исправления ".

Кампания SolarWinds

Nobelium, который организовал кампанию SolarWinds, о которой Microsoft и FireEye сообщили в декабре 2020 года, взломал системы SolarWinds и распространил вредоносное обновление программного обеспечения Orion среди клиентов компании. Было взломано около 100 организаций по всему миру, и

последующие атаки произошли в девяти федеральных агентствах США, включая Министерство внутренней безопасности и Министерство финансов.

Президент Microsoft Брэд Смит заявилв феврале в эфире«60 минут»,что инцидент с SolarWinds, возможно, повлек за собой скоординированные усилия около 1000 инженеров.

В то время Смит заявил: «Я думаю, что с точки зрения разработки программного обеспечения, вероятно, будет справедливо сказать, что это самая крупная и изощренная атака, которую когда-либо видел мир».

Администрация президента Джо Байдена в апреле приписала шпионские усилия 2020 года СВР России.

«Более агрессивные действия»

По словам Дэнни Лопеса, бывшего генерального консула британского министерства иностранных дел и по делам Содружества и генерального директора компании Glasswall, эти недавние атаки показывают, что во всех секторах «традиционный подход к сетевой безопасности, основанный на замках и рвах, оставляет организации незащищенными» - потенциально предлагая «злоумышленникам вроде Nobelium полную свободу действий» в сети.

Джамиль Джаффер, бывший помощник советника президента Джорджа Буша в Белом доме, а также основатель и исполнительный директор Института национальной безопасности Университета Джорджа Мейсона, предупреждает: «Эта [деятельность, без сомнения] подчеркивает необходимость принятия более агрессивных мер для увеличения расходов в для сдерживания такой активности со стороны России».

Джаффер, старший вице-президент по стратегии, партнерству и корпоративному развитию IronNet Cybersecurity, продолжает: «Совершенно очевидно, что ранее введенные санкции как за хакерскую деятельность, так и за поддержку Россией атак программ-вымогателей недостаточно сдерживали российскую киберактивность против частных лиц в США».

Однако в сообщении Берт из Microsoft говорит: «Мы ясно понимаем, что национальные государства, включая Россию, не остановят подобные атаки в одночасье; [но] мы верим в такие шаги, как указ о кибербезопасности в США и более серьезные меры. координация и обмен информацией, которые мы наблюдали между промышленностью и правительством за последние два года, позволили нам лучше защищаться от них ».

Федеральные усилия

Последний маневр Nobelium подчеркивает огромную проблему кибербезопасности, с которой сталкиваются официальные лица США. Помимо введения экономических санкций против России, Байден развернул наступление на программы-вымогатели и их финансовую инфраструктуру, зайдя так далеко, что нацелился на конкретные криптовалютные биржи и установил «закрытую» критическую инфраструктуру для президента России Владимира во время июньского саммита.

На саммите Mandiant Cyber Defense Summit в Вашингтоне, округ Колумбия, в этом месяце генерал Пол Накасоне, возглавляющий Агентство национальной безопасности и киберкомандование США, назвал SolarWinds поворотным

моментом для страны, но отметил, что агентства США успешно перекрыли российскую разведку». ***(Dan Gunderman. Report: SolarWinds Hackers Targeting IT Supply Chain // Information Security Media Group, Corp. (https://www.govinfosecurity.com/report-solarwinds-hackers-targeting-supply-chain-a-17793). 25.10.2021).***

***

«После атаки программ-вымогателей в марте 2021 года компания Acer, один из крупнейших в мире производителей компьютеров и устройств, в течение недели подверглась еще двум кибератакам.

В понедельник Acer подтвердила Information Security Media Group, что 14 октября обнаружила изолированную атаку на свою местную систему послепродажного обслуживания в Индии, которая затрагивала данные пользователей, и сообщила, что уведомляет всех потенциально затронутых клиентов.

Кроме того, компания заявляет, что Acer Taiwan также подверглась атаке, однако компания сообщает, что атака на ее тайваньские системы не затрагивает никаких данных о клиентах.

DESORDEN актеры угрозы, как сообщается, взяли на себя ответственность за нападение в соответствии cDatabreaches.net.

«Чтобы доказать нашу точку зрения, что Acer значительно отстает в плане кибербезопасности в защите своих данных и представляет собой глобальную сеть уязвимых серверов, мы взломали и взломали сервер Acer Taiwan, сохраняя данные о его сотрудниках и информацию о продуктах», - заявили хакеры. новостной сайт, сообщается в субботу.

Ранее в марте банда вымогателей REvil разместила на своем «новостном» сайте в даркнете данные, которые, по ее утверждению, являются данными компании Acer. От тайваньской фирмы требовалось 50 миллионов долларов. Сообщается, что атака могла воспользоваться уязвимостью ProxyLogon на локальном сервере Microsoft Exchange без исправлений.

Acer - один из крупнейших в мире производителей ПК, смартфонов, устройств и другого оборудования, включая настольные мониторы. Согласно январскому анализу, опубликованному IDC, в четвертом квартале 2020 года она заняла пятое место в мире по поставкам ПК: за квартал было поставлено более 6,5 миллионов настольных компьютеров и ноутбуков.

Детали атаки

14 октября злоумышленники разместили на популярном хакерском форуме заметку, в которой утверждали, что они извлекли 60 ГБ файлов и баз данных с серверов Acer в Индии. Acer сообщает, что сюда входят данные о клиентах, компаниях, счетах и финансовые данные.

«После обнаружения мы немедленно инициировали наши протоколы безопасности и провели полное сканирование наших систем. Мы уведомляем всех потенциально затронутых клиентов в Индии, в то время как атакованная тайваньская система не использует данные клиентов», - сказал ISMG представитель Acer Стивен Чанг.

Чанг далее заявляет, что компания сообщила об инциденте в местные правоохранительные органы и соответствующие органы, и что это не оказывает существенного влияния на ее операции и непрерывность бизнеса.

В опубликованной заметке на хакерском форуме также утверждается, что у него есть доступ к более чем 3000 наборов данных для входа в систему розничных продавцов и дистрибьюторов Acer в Индии.

Однако DESORDEN пояснил Databreaches.net, что не требовал отдельной оплаты за нарушение тайваньского доступа, и проинформировал Acer о необходимости закрыть уязвимость. Однако до сих пор неясно, требует ли злоумышленник выкуп за атаку в Индии.

Согласно Databreaches.net, злоумышленникив последующем сообщении описали себя как бывших соратников Хаоса. Однако группа утверждала, что это DESORDEN Group, что означает хаос и беспорядок.

«Раньше вы могли знать нас как ChaosCC, но сегодня мы больше не связаны с ChaosCC», - сообщили Databreaches.net злоумышленники. Группа в основном нацелена на сети цепочек поставок и общественные услуги;его новостной веб-сайт утверждает, что если жертвы не платят деньги, злоумышленники продают украденные данные на черном рынке.

Джейк Уильямс, ранее входивший в состав элитной хакерской группы Агентства национальной безопасности, а в настоящее время технический директор BreachQuest, отмечает, что подробные сведения о любых атаках на ИТ-системы Acer - прошлых или текущих - пока неизвестны. Однако при наличии нескольких атак на данную организацию обычно возникают системные проблемы с безопасностью.

«Большинство событий реагирования на инциденты вызывают значительные инвестиции в безопасность со стороны организации, чтобы предотвратить повторение событий. В этом случае легко сделать вывод, что вложения в безопасность не были осуществлены так, как хотелось бы», - говорит Уильямс.«В случае с Acer мы также должны учитывать, что они являются производителями и обладают значительными активами OT. Они, как правило, имеют гораздо более длительный жизненный цикл замены и часто работают на неподдерживаемом оборудовании и программном обеспечении, что создает дополнительные возможности для атак. для обеспечения безопасности в любом случае OT вдвойне эффективен. Их многонациональное присутствие также затрудняет обеспечение безопасности всей сети».

Мартовская атака

Acer пострадали от вымогателей банды Revil, он же Sobinokibi, в марте,который требовал 50000000 $ от тайваньской фирмы, в соответствии с Bleeping Computer, который первый сообщил об атаке и с тех пор опубликовал копию искупительных записок.

ISMG получила доступ к нескольким снимкам экрана с сайта даркнета REvil, на которых показаны данные клиентов, формы платежных приложений и другая информация, которую, по утверждениям банды, украла у Acer во время атаки.

REvil известен тем, что использует метод двойного вымогательства, нацеленный на жертв. Группа не только использует криптоблокирующее

вредоносное ПО для шифрования данных и файлов в пострадавшей организации, но и киберпреступники затем крадут и угрожают опубликовать эту информацию, если требования не будут выполнены.

DESORDEN также предупредил Acer, что в ближайшее время в Интернете будет больше утечек данных». ***(Prajeet Nair. Acer Taiwan and India Hit in 2nd and 3rd Attacks of 2021// Information Security Media Group, Corp. (https://www.govinfosecurity.com/acer-taiwan-india-hit-in-2nd-3rd-attacks-2021-a-17754). 18.10.2021).***

***

«Мы находимся в разгаре «киберпандемии». В 2020 году COVID-19 ускорил переход к удаленной работе, и программное обеспечение, используемое для этих атак, стало проще выполнять, количество атак программ-вымогателей быстро увеличилось и продолжит расти в 2021 году:

Только в США количество атак за последние девять месяцев увеличилось на 300%.

Более 60% атак программ-вымогателей нацелены на отрасли с критически важной инфраструктурой, в первую очередь на здравоохранение, коммунальные услуги и производство.

Коммунальные предприятия США подвергались атакам 300 раз в неделю, что всего за два месяца увеличилось на 50%.

Основной целью киберпреступников были сети операционных технологий (OT), которые соединяют между собой промышленные системы управления (ICS), которые управляют нашей критически важной инфраструктурой. По мере того, как такие сервисы, как электросети, водоочистные сооружения, транспорт и системы здравоохранения, все больше интегрируют свои операционные технологические системы с Интернетом вещей - например, с помощью удаленных датчиков и мониторинга - это создает новую границу рисков, где могут появиться миллионы точек уязвимости и новые векторы. могут быть использованы хакерами.

Эти атаки имеют огромные последствия не только для предприятий, но и для сообществ, городов, штатов и целых стран. Последствия могут быть ужасными. В апреле 2020 года хакеры нацелились на водоочистные сооружения Израиля через свою систему Интернета вещей, которая дала злоумышленникам возможность изменять давление, температуру и уровень хлора в воде. Если бы атака полностью увенчалась успехом, это могло бы привести к тому, что целые общины заболели от водоснабжения или сработали отказоустойчивые системы, в результате чего тысячи людей остались бы без воды.

Как хакеры используют системы Интернета вещей?

IoT-устройства и подключенные системы могут представлять большой риск для безопасности критически важных инфраструктурных сервисов, когда не реализованы передовые методы безопасности, поскольку они имеют несколько внутренних недостатков:

Отсутствие стандартизации практик кибербезопасности в цепочке поставок ведет к большей уязвимости.

Уязвимые протоколы и конструкции безопасности, включая слабые пароли и методы исправления.

Устаревшая и неподдерживаемая архитектура, прошивка и программное обеспечение.

Поверхность атаки, которая увеличивается с количеством подключенных устройств.

В результате у хакеров есть несколько способов использовать эти устройства и либо совершать атаки на более крупные цели, либо двигаться в сторону, чтобы нанести ущерб критически важным системам и украсть информацию клиентов и сотрудников, интеллектуальную собственность или другие конфиденциальные активы.

Новая «ботнет-атака» под названием Mozi была чрезвычайно активна в течение последних 18 месяцев, составляя 90% всех атак Интернета вещей в 2020 году и контролируя почти 500 000 подключенных устройств. Каждое взломанное устройство получает указание найти больше устройств для заражения, что позволяет киберпреступникам получить контроль над целыми сетями и их данными и удерживать их с целью получения выкупа.

В марте 2021 года стартап из Кремниевой долины Verkada подвергся массированной кибератаке в области Интернета вещей. Хакеры смогли получить административные привилегии для большого количества камер видеонаблюдения, что означает, что они могли выполнять свой собственный вредоносный код на устройствах.

Как только хакер может взломать сетевое устройство, он может использовать его в качестве отправной точки для боковых атак, обнажая критически важные для операций системы. По мере того, как отрасли продолжают интегрировать ИТ и сети ОТ для получения новых знаний, эти устройства представляют еще большую опасность для операций, которые зависят от промышленных систем управления. Если не будет усилена защита этих подключенных устройств, мы, вероятно, продолжим видеть больше атак, нацеленных на критически важные отрасли инфраструктуры.

Что делается в национальном и глобальном масштабе?

Критически важная инфраструктура остается в основном частной и потребует скоординированных усилий государственного и частного секторов для защиты от программ-вымогателей и угроз Интернета вещей. Чтобы устранить пробелы в протоколах и стандартах безопасности в критически важных отраслях, правительства берут на себя ответственность внедрять и расширять существующие политики кибербезопасности для устройств IoT.

Агентство Европейского Союза по кибербезопасности (ENISA) опубликовало руководство по безопасности цепочек поставок Интернета вещей в 2020 году и в настоящее время разрабатывает конкретные меры безопасности для операторов Интернета вещей и отраслей критической инфраструктуры. Между тем, в конце 2020 года был принят Закон о повышении кибербезопасности IoT, который требует от пользователей Интернета вещей в государственном секторе США, в том числе тех, которые используются в критически важной инфраструктуре, расширять надежную киберзащиту для своих развертываний IoT.

Стандарт для этого был разработан Национальным институтом стандартов в области технологий (NIST), который в течение нескольких лет играл центральную роль в разработке подходов к повышению кибербезопасности в США. NIST разработал ряд руководящих документов в консультации с заинтересованными сторонами в правительстве, промышленности и частном секторе, а также в координации с международными усилиями по стандартизации других стран. Учитывая размер правительства США как заказчика, стандарты NIST, принятые для государственного сектора, также могут выступать в качестве более широкого фактического отраслевого стандарта для всех типов устройств IoT в США и за их пределами.

Помимо Закона об улучшении кибербезопасности IoT, который ориентирован на рынок федерального правительства США, в Публичном законе 116-283, принятом в конце 2020 года, содержится призыв к Руководящему комитету IoT, состоящему из представителей частного сектора, для консультирования межведомственной группы федерального правительства США. Руководящему комитету и Федеральной рабочей группе поручено определить преимущества IoT, улучшить регулирование IoT и устранить препятствия для внедрения. Параллельно с этим в Указе президента о кибербезопасности от мая 2021 года содержится призыв к пилотному запуску программы маркировки потребительских продуктов IoT, которая определяет, насколько они соответствуют критериям кибербезопасности, которая будет введена в действие к февралю 2022 года.

Эти усилия по установлению требований безопасности для устройств IoT выходят за рамки федеральных агентств и подрядчиков, чтобы удовлетворить потребность в безопасности в критически важной инфраструктуре. Отрасли, которые больше всего подвержены этим атакам, стремятся к единообразию и эффективности и поэтому рассматривают эти законы и политики как руководящие принципы для принятия базовых требований безопасности.

Что могут сделать государственный и частный сектор?

По мере роста числа кибератак в важнейших отраслях, правительства и частный сектор несут общую ответственность за защиту этих систем. Сторонники IoT-устройств могут работать вместе с политиками и поставщиками кибербезопасности для достижения большего консенсуса в отношении стандартов безопасности IoT, одновременно укрепляя доверие к безопасности во всей критически важной инфраструктуре.

1) Разработать единый подход к безопасности Интернета вещей во всем мире путем:

Согласование общего глобального базового стандарта безопасности Интернета вещей (разграничение потребительских и промышленных устройств).

Продвижение общих принципов безопасности от отраслевых альянсов, таких как Cyber Tech Accord, Charter of Trust или Paris Call for Trust and Security.

Согласование правил и базовых механизмов сертификации безопасности устройств.

Разработка общих принципов цифровой безопасности и международных норм.

Ориентируйтесь не только на поставщиков, но и на потребителей технологий Интернета вещей.

2) Укрепление доверия за счет большей прозрачности и международного сотрудничества:

Уточнение модели ответственности в цепочке поставок и добавленной стоимости.

Содействие межотраслевому и международному сотрудничеству.

Содействие использованию международных структур обмена информацией и передового опыта в области гарантий».***(Jeremy Kaye, Mitch Muro, Katerina Megas. Protecting critical infrastructure from a cyber pandemic // World Economic Forum (https://www.weforum.org/agenda/2021/10/protecting-critical-infrastructure-from-cyber-pandemic/). 20.10.2021).***

***

«Новое исследование, проведенное фирмой Malwarebytes, занимающейся разработкой программного обеспечения для обеспечения безопасности, совместно с некоммерческой организацией Digitunity по обеспечению доступа к технологиям показывает, что расовые и гендерные предубеждения могут распространяться даже на мир киберпреступности. Исследование показало, что обездоленные группы не только чаще становятся объектами этих атак, но и страдают от них несоразмерно.

«Понимание того воздействия, которое киберпреступность оказывает на уязвимых людей или группы населения, особенно женщин и меньшинства, во всем мире имеет решающее значение, поскольку онлайн-доступ становится важным для современной жизни», - сказал Марцин Клечински, генеральный директор Malwarebytes. «Несоответствие между группами населения, которые чувствуют себя в безопасности в сети, и эмоциональное воздействие угроз на и без того уязвимые сообщества недопустимы. Трудно переоценить ту работу, которую Digitunity и Сеть поддержки киберпреступности проводят по обучению и расширению прав и возможностей сообществ. Как отрасль, мы должны работать вместе, чтобы сделать безопасный доступ в Интернет доступным для всех, независимо от дохода или их платежеспособности ».

Является ли киберпреступность жертвой с неравными возможностями?

Основываясь на идее о том, что многие аспекты повседневной жизни теперь неизбежно должны выполняться в Интернете, в опросе было опрошено около 5000 взрослых в трех странах (США, Великобритании и Германии).Исследование было сосредоточено на том, как результаты различаются между женщинами и мужчинами, а также между белыми респондентами и чернокожими и цветными коренными народами (BIPOC).

Первый вопрос опроса рисует четкую картину общего состояния Интернета: 50% всех респондентов считают, что у них нет адекватной конфиденциальности в Интернете, а 31% не чувствуют себя в безопасности, даже несмотря на то, что условия пандемии быстро увеличились и больше повседневных функций на компьютерах и мобильных устройствах.

Хотя можно вспомнить множество примеров, подтверждающих такое пессимистическое отношение к конфиденциальности и безопасному доступу в Интернет, респонденты сообщают о конкретных различиях в фактических результатах для уязвимых групп, когда их поражает киберпреступность. У людей BIPOC на 12% больше шансов получить какой-либо финансовый ущерб в результате киберпреступления и на 6% выше вероятность того, что их личные данные будут украдены.У женщин на 6% больше шансов, чем у мужчин, иметь учетные записи в социальных сетях, на которые направляются фишинговые сообщения, на 5% больше вероятность того, что злоумышленник отправит сообщения со взломанной учетной записи их друзьям и семье, и на 9% больше шансов, что в конечном итоге учетная запись будет взломана.У них также на 3% больше шансов столкнуться с какой-либо подозрительной онлайн-активностью и столкнуться с множеством подозрительных инцидентов за последние три месяца.

Женщины также сталкиваются с уникальной угрозой в цифровом мире: «порнография мести», распространяемая бывшими партнерами или людьми, взломавшими их личные учетные записи, что относительно редко встречается у мужчин. У них почти в три раза больше шансов стать жертвами преследований, чем у мужчин, и 26% из них считают киберпреследование элементом угрозы. Кроме того, они с большей вероятностью столкнутся с угрозой не только из-за публичного выпуска частных цифровых материалов, но и из-за создания «дипфейк» видео.

Неудивительно, что женщины с большей вероятностью будут чувствовать себя небезопасными в Интернете, чем мужчины (разница в 12%), а также реже будут считать, что их информация хранится в тайне (разница в 6%).Какие виды киберпреступности наиболее подвержены уязвимым группам? Самым распространенным на сегодняшний день является фишинг со ссылками на сайты атаки через текстовые сообщения с неизвестных номеров, которые 76% респондентов сообщили, что когда-то получали их. 43% заявили, что в какой-то момент переходили по подозрительной ссылке такого рода, 42% заявили, что испытали как минимум один взлом личной учетной записи в социальных сетях, а у 29% был украден номер кредитной карты. Ответы действительно подтверждают более широкую теорию о том, что программы-вымогатели переходят от широких атак на случайных лиц к целевым атакам на предприятия, однако только 16% респондентов заявили, что сталкивались с этим.

Обездоленные группы сообщают о несоразмерном ущербе

Респонденты BIPOC также сообщили о более высоком уровне риска и ущерба от киберпреступности. У них на 6% больше шансов получить кражу личных данных, на 5% больше шансов столкнуться с попытками финансового мошенничества и на 5% больше вероятность взлома учетной записи в социальных сетях. Это привело к тому, что они сообщили о том, что они менее безопасны и конфиденциальны в Интернете, чем белые респонденты.

Респонденты BIPOC также сталкиваются со своим собственным уникальным фактором стресса среди обездоленных групп: онлайн-домогательствами, при этом около 59% заявили, что когда-то сталкивались с ними в Интернете (примерно на 10-20 процентных пунктов выше, чем у представителей других

национальностей).Существует аналогичная разница в процентных пунктах в чувстве беспокойства по поводу одной из этих атак в Интернете.

Хотя это исследование было сосредоточено на конкретных уязвимых группах, оно также показало, что возраст является явным фактором риска киберпреступности в Интернете. Немногим более половины респондентов в возрастной группе 18–24 лет сообщают о взломе учетной записи в социальных сетях, и это число постоянно снижается до немногим более четверти от лиц в возрасте 65 лет и старше. Хотя известно, что конкретные виды мошенничества нацелены на пожилых людей, эти цифры указывают на то, что захват аккаунтов в социальных сетях представляет собой более высокий риск для демографических групп, наиболее активных на этих платформах.

Что касается решений по устранению этих рисков и диспропорций, связанных с киберпреступностью, в отчете отмечается широкая неосведомленность об инструментах защиты и безопасности в Интернете. 21% респондентов заявили, что совсем не знакомы с основными средствами защиты от вирусов и вредоносных программ. Только 42% знакомы с менеджерами паролей, 32% - с виртуальными частными сетями (VPN), 24% - со службами мониторинга личности и 8% - с цифровыми хранилищами.

Хизер Поне, старший вице-президент Untangle, дайте некоторое представление о том, почему женщины относятся к группам, находящимся в неблагоприятном положении, которые с наименьшей вероятностью будут использовать онлайн-инструменты безопасности: «Одна из возможных причин, по которой меньшее количество женщин знакомы с инструментами кибербезопасности, - это незаметность. Хотя компании могут следить за кибератаками, событиями и технологиями, для многих это не повседневная тема, и обмен сообщениями вряд ли поможет преодолеть беспорядок в рекламе... Хотя некоторые сообщения о кибербезопасности могут быть доступны женщинам, тот факт, что они не регистрируются, может быть побочный продукт меньшего числа женщин, которые получали образование и карьеру в области STEM, где технологии не находятся в их поле зрения. Откровенно говоря, отрасль может многому научиться из этого опроса.Многие решения безопасности кажутся нацеленными на крупный бизнес или ИТ-специалистами и недоступны для обычного пользователя». ***(SCOTT IKEDA. Disadvantaged Groups More Likely to Experience Cybercrime, Experience Disproportionately Damaging Results // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/disadvantaged-groups-more-likely-to-experience-cybercrime-experience-disproportionately-damaging-results/). 11.10.2021).***

***

По словам официальных лиц, израильская больница в среду подверглась атаке с использованием программ-вымогателей, а киберуправление штата назвало это первой такой атакой на больницу в стране.

Медицинский центр Хиллеля Яффе «в настоящее время использует альтернативные системы для лечения своих пациентов», говорится в заявлении, в котором атака описывается как «совершенно неожиданная».

«Лечение продолжается в обычном режиме, за исключением несрочных плановых процедур», - сказал Хиллель Яффе.

Игаль Унна, директор Национального управления киберпространства Израиля, назвал это «серьезной» атакой.

«Мы пытаемся решить эту проблему, это выглядит не очень хорошо», - сказал он на виртуальном саммите по атакам программ-вымогателей, организованном Советом национальной безопасности США.

По словам Унны, это была «первая в Израиле» кибератака с использованием программ-вымогателей, нацеленная на больницу, хотя медицинские центры в других странах подвергались аналогичным атакам.

Его агентство сообщило, что «министерство здравоохранения обновило больницы в профилактических целях».

Согласно данным, представленным Unna в июле, каждый пятый бизнес в Израиле подвергся кибератаке. В результате атак пятая часть атакованных заведений была повреждена». ***(Israeli hospital targeted in ransomware attack // Tech Xplore (https://techxplore.com/news/2021-10-israeli-hospital-ransomware.html). 13.10.2021).***

***

«Южнокорейская телекоммуникационная компания KT сообщила в понедельник, что временное отключение ее сети по всей стране было вызвано крупномасштабной распределенной атакой типа «отказ в обслуживании» (DDoS).

Клиенты, использующие сеть телекоммуникационной компании, не могли выйти в Интернет в течение 40 минут примерно в 11 часов утра в понедельник.

В течение этого периода пользователи не могли использовать кредитные карты, торговать акциями или получать доступ к онлайн-приложениям. Некоторые крупные коммерческие веб-сайты также были закрыты во время перебоев в работе.

С тех пор общий доступ к Интернету был восстановлен для пользователей KT в большинстве районов страны.

Представитель KT сообщил, что сеть телекоммуникационной компании была отключена из-за крупномасштабной DDoS-атаки. Они сказали, что во время сбоя команда антикризисного управления компании работала над быстрым восстановлением сети до нормального состояния.

Представитель KT добавил, что KT еще предстоит выяснить степень ущерба или кто стоял за DDoS-атакой.

Федеральная полиция и Министерство науки и информационных технологий заявили, что они также изучают этот вопрос в сотрудничестве с KT.В министерстве не подтвердили, что отказ сети был вызван DDoS-атакой, но заявили, что другие крупные телекоммуникационные компании SK Telecom и LG Uplusне пострадали.

Несмотря на то, что они не стали жертвами DDoS-атаки, пользователи сервисов SK Telecom и LG Uplus высказали в социальных сетях жалобы на сбои сети у этих операторов. Представители этих телекоммуникационных компаний заявили, что сбои в сети были вызваны внезапным всплеском трафика от пользователей KT, переключившихся на их услуги, из-за отключения KT в

Интернете…». ***(Cho Mu-Hyun. Large DDoS attack shuts down KT's nationwide network // ZDNet (https://www.zdnet.com/article/large-ddos-attack-shuts-down-south-korean-telcos-nationwide-network/). 24.10.2021).***

***

«Британский гигант супермаркетов Tesco восстановил доступ к своему веб-сайту и приложению после сбоя в работе службы в субботу, из-за чего клиенты не могли заказывать или отменять доставку до вечера воскресенья.

В заявлении для The GuardianTesco сообщила, что «была предпринята попытка вмешательства в наши системы, что вызвало проблемы с функцией поиска на сайте».

Розничный торговец, чьи 1,3 миллиона онлайн-заказов в неделю составляют почти 15% его продаж в Великобритании, заявил, что нет оснований полагать, что попытка вмешательства повлияла на данные о покупателях.

В воскресенье вечером Tesco подтвердила, что ее веб-сайт и приложение были восстановлены, но она использовала виртуальную комнату ожидания для обработки невыполненных заказов.

«Наш продуктовый веб-сайт и приложение снова работают. Чтобы помочь нам справиться с большими объемами заказов, мы временно используем виртуальную комнату ожидания. Приносим извинения за неудобства и благодарим вас за терпение», -сообщила Tesco в Twitter.

Tesco Bank был оштрафован Управлением финансового надзора Великобритании (FCA) на 16,4 миллиона фунтов стерлингов за инцидент 2016 года, когда кибератаки украли 2,26 миллиона фунтов стерлингов у 9000 клиентов. FCA обнаружило множество недостатков в конструкции своей системы дебетовых карт. Например, Tesco Bank случайно выпустил дебетовые карты с последовательными номерами основных счетов (PAN).Компанию также критиковали за медленную реакцию на мошеннические транзакции.

Покупатели продуктовых магазинов Tesco жаловались на обработку заказов и отмену заказов во время отключения веб-сайта. Некоторые клиенты сказали, что в субботу им сказали отменить свои заказы, но впоследствии они были проинформированы, что Tesco не может получить доступ или изменить какие-либо заказы.Другие клиенты сообщили в социальных сетях, что они пытались превысить установленное время в 23:45, чтобы отменить заказы после размещения заказов в конкурирующих супермаркетах.

В США ФБР недавно предупредило, что продовольственный и сельскохозяйственный сектор все чаще становится объектом атак программ-вымогателей, которые угрожают нарушить цепочку поставок продуктов питания. Это последовало за атакой на глобальный мясоперерабатывающий бизнес JBS, который заплатил злоумышленникам 11 миллионов долларов за восстановление доступа к зашифрованным данным.

Шведская продуктовая сеть Coop не могла принимать платежи по картам в своих магазинах в течение трех дней в начале этого года после того, как злоумышленники напали на поставщиков управляемых ИТ-услуг спомощью испорченного обновления программного обеспечения для продуктов Kaseya.

В прошлом году Tesco перевыпустила 600 000 карт Clubcardпосле обнаружения проблемы безопасности, которая позволила злоумышленникам использовать учетные данные с других платформ на своих веб-сайтах для погашения ваучеров.Все более распространенная атака известна как распыление паролей, когда списки часто используемых паролей используются для получения доступа к другим несвязанным учетным записям».***(Liam Tung. Tesco's website restored after suspected cyberattack // ZDNet (https://www.zdnet.com/article/tescos-website-restored-after-suspected-cyberattack/). 25.10.2021).***

***

«Многонациональная компания Atento, которая занимается аутсорсингом бизнес-процессов (BPO) и управлением взаимоотношениями с клиентами, подверглась кибератаке, причем наибольший эффект она имела в Бразилии, ее крупнейшем предприятии в Латинской Америке.

Фирма со штаб-квартирой в Мадриде проинформировала своих клиентов в воскресенье (17 октября) об атаке на ее системы в Бразилии, которая привела к прерыванию обслуживания, поскольку компания стремилась сдержать и оценить степень угрозы, сообщает местный новостной сайтNeofeed.

В записке Atento для клиентов добавлено, что его группа безопасности работает над его сдерживанием и обеспечением безопасности затронутых сред, прежде чем как можно скорее вернуть их в онлайн.

Компания ZDNet, с которой связались, подтвердила инцидент и сообщила в своем заявлении, что для предотвращения любого потенциального риска для клиентов компания «проактивно изолировала» затронутые системы.Это привело к приостановке связи с клиентами в Бразилии и прерыванию обслуживания.

«Расследование все еще продолжается, и компания продолжает тесно сотрудничать со своими консультантами и соответствующими органами, чтобы оценить влияние инцидента на бизнес и принять соответствующие меры», - отметили в компании.

Atento подчеркнула, что смогла сдержать угрозу в течение 24 часов и начать предоставлять ограниченное обслуживание некоторым клиентам. Операции центров обработки данных уже возобновлены, и компания начнет постепенно возобновлять больше услуг.

Бразилия - один из основных мировых рынков Atento.Более 45% глобальной рабочей силы компании, в которой работает более 150 000 человек, сосредоточено в бразильском подразделении, которое обслуживает крупные телекоммуникационные компании и банки, такие как Bradesco и Itaъ.

Фирма BPO является последней из ряда компаний, работающих в Бразилии, которые недавно подверглись кибератакам. На прошлой неделе одна из крупнейших страховых групп Бразилии, Porto Seguro, подверглась кибератаке, которая привела к нестабильности ее каналов обслуживания и некоторых ее систем.

Еще одна компания, которая также стала мишенью для киберпреступников, CVC, один из крупнейших туристических операторов страны, в начале этого

месяца подверглась атаке с использованием программ-вымогателей, в результате чего ее деятельность была остановлена.

Несмотря на рост угроз безопасности, 56% бразильских компаний в настоящее время инвестируют 10% или меньше своего ИТ-бюджета в кибербезопасность, согласноисследованию консалтинговой фирмы Marsh от имени Microsoft. Исследование показало, что 52% бразильских организаций заявили, что инвестиции в безопасность не изменились с начала пандемии.

Что касается практики сотрудников в области безопасности, только 23% бразильских организаций, принявших участие в исследовании, заявили, что их сотрудники используют для работы оборудование, предоставленное компанией.В исследовании отмечается, что такая практика значительно увеличивает подверженность некоторым типам киберинцидентов, но безопасность удаленного доступа является приоритетом только для 12% респондентов и вторым пунктом в списке для 7% респондентов». ***(Angelica Mari. Customer services firm Atento hit by cyberattack // ZDNet (https://www.zdnet.com/article/customer-services-firm-atento-hit-by-cyberattack/). 19.10.2021).***

***

«Согласно опросу, проведенному Cisco, в 51% малых и средних предприятий Азиатско-Тихоокеанского региона, пострадавших от киберинцидента в прошлом году, стоимость этого инцидента превысила 500 000 долларов.

Из 3750 компаний, в которых работает от 10 до 999 сотрудников в 14 странах региона, Cisco сообщила, что 83% сообщили об инцидентах на сумму более 100 000 долларов США, а 13% имели инциденты стоимостью более 1 миллиона долларов. Опрос проводился с апреля по июль.

В Австралии, куда ответили 306 подходящих компаний, цифры были более резкими: 64% сообщили об инциденте, который стоил более 500 000 долларов, а 33% заявили, что они понесли убытки более чем в 1 миллион долларов.

Что касается компаний, которые проводят симуляционные упражнения, Cisco сообщила, что 85% респондентов обнаружили проблемы в своей защите.

«Из тех, кто выявил слабые места, 95% заявили, что в ходе учений были выявлены проблемы, связанные с отсутствием правильных технологических решений для обнаружения кибератак или угроз. Столько же обнаружили, что у них слишком много технологий, и изо всех сил пытались объединить их вместе, а 96% обнаружили, что у них нет подходящих технологических решений для блокирования атаки », - заявили в компании.

Основным вектором атаки отобранных предприятий было вредоносное ПО, которое использовалось 85% времени и привело к 75% атак с получением информации о клиентах, 62% к обнаружению внутренней электронной почты и 61% атак на данные сотрудников, интеллектуальную собственность или финансовые ресурсы. данные.

В своем годовом отчете за 2020-2021 годы, опубликованном ранее на этой неделе, Австралийское управление сигналов (ASD) сообщило, что за последний год число атак программ-вымогателей увеличилось на 15%.

«ASD отреагировала на более чем 1630 инцидентов кибербезопасности в течение 2020–21 годов. По сравнению с предыдущим финансовым годом, общее количество инцидентов кибербезопасности в 2020–21 финансовом году снизилось на 28%», - говорится в сообщении.

«Более высокая доля инцидентов кибербезопасности в этом финансовом году была отнесена ACSC к категории« существенных »по влиянию. Это изменение частично связано с увеличением числа атак киберпреступников на более крупные организации и влиянием этих атак на жертв. включая кражу данных, вымогательство и / или оказание услуг в автономном режиме».

Благодаря пандемии ASD заявила, что переместила большую часть своей рабочей силы на гибкую и надомную работу и закрыла 7700 сайтов, на которых проводилась «киберпреступная деятельность», связанная с COVID-19». ***(Chris Duckett. Cyber incident impact sits at over $500,000 for half of small to medium APAC businesses // ZDNet (https://www.zdnet.com/article/cyber-incident-impact-sits-at-over-500000-for-half-of-small-to-medium-apac-businesses/). 19.10.2021).***

***

«Корпорация NTT, которая этим летом предоставляла широкий спектр телекоммуникационных услуг и сетевой безопасности для Олимпийских и Паралимпийских игр в Токио, заявила, что во время мероприятия в июле было совершено более 450 миллионов попыток кибератак.

Представители NTT заявили, что ни одна из атак не была успешной, и добавили, что игры прошли без сучка и задоринки. Но количество атак было в 2,5 раза больше, чем во время летних Олимпийских игр в Лондоне в 2012 году.

Андреа Маклин из NTT сравнила борьбу за кибербезопасность с последней битвой Гарри Поттера против Волдеморта, назвав усилия по защите события «титаническими».

«Киберпреступники, безусловно, рассматривали Игры - и связанную с ними цепочку поставок - как ценную цель с низким уровнем простоя. В конце концов, преступность следует за возможностью. И с подключенными стадионами, платформами для взаимодействия с болельщиками и полными цифровыми копиями спортивных объектов и «События сами по себе становятся нормой, существует множество ИТ-инфраструктуры и данных, на которые можно ориентироваться - и через множество компонентов», - сказал Маклин.

Она пояснила, что подход NTT к защите мероприятия включает «постоянный мониторинг и анализ информации об угрозах, услуги SOC, полный пакет решений безопасности и экспертную группу из более чем 200 специалистов по кибербезопасности».

Маклин сказал, что среди 450 миллионов атак NTT обнаружила вредоносное ПО Emotet, спуфинг электронной почты и фишинг, а также поддельные веб-сайты, которые выглядели так, как будто они были связаны с Олимпийскими играми.

«Спортивные мероприятия, такие как Олимпийские игры, Тур де Франс и Indy 500, например, являются определением среды реального времени», - сказал Маклин. «После начала простоя не остается. А с учетом сильно распределенной

команды и ограниченного физического присутствия гибкие технологии, которые могут реагировать на любые угрозы, имеют решающее значение».

NTT представила полный отчет об играх, отметив, что она предоставляла как услуги связи для управления Играми, так и сеть вещания, соединяющую места проведения Игр с Tokyo Big Sight, служившим международным центром вещания.

«NTT построила локальную сеть для объектов, включая 43 объекта Игр, IBC, Главный пресс-центр и Олимпийскую деревню, предоставляя различные коммуникационные услуги, включая распространение видео и стационарных телефонов для партнеров. Все объекты Игр были переведены на мобильные сети 5G, коммерческие услуги которых начали работу в 2020 году в Японии, чтобы предлагать услуги мобильной связи», - сказал NTT, добавив, что у них было в общей сложности 10 000 сотрудников, поддерживающих это мероприятие.

«Во время Игр наблюдались несанкционированные коммуникации, нацеленные на уязвимости в терминалах, но NTT ответила блокировкой коммуникации».

NTT заявила, что провела несколько учебных программ по кибербезопасности и провела моделирование перед мероприятием, чтобы подготовить свою команду по кибербезопасности.

В своем предварительном отчете, опубликованном перед Играми, NTT предсказывала, что столкнется с кибератаками со стороны государства, атаками программ-вымогателей и атаками дезинформации, некоторые из которых могут исходить от российских, северокорейских и китайских субъектов угроз, спонсируемых государством.

Они отметили, что киберпреступники могут использовать распределенные атаки типа «отказ в обслуживании» (DDoS), атаки программ-вымогателей или атаки на критически важную инфраструктуру.

Перед Играми ФБР выпустило частное отраслевое предупреждение, в котором призвало организации, работающие с летними Олимпийскими играми в Токио 2020, подготовиться к волне «DDoS-атак, программ-вымогателей, социальной инженерии, фишинговых кампаний или инсайдерских угроз, чтобы заблокировать или прервать прямые трансляции мероприятия., украсть и, возможно, взломать и утечь или удерживать в заложниках конфиденциальные данные, или повлиять на государственную или частную цифровую инфраструктуру, поддерживающую Олимпийские игры ».

В уведомлении говорилось о кибератаке в Пхенчхане, которая произошла во время предыдущих Олимпийских игр в феврале 2018 года, когда российские хакеры развернули вредоносное ПО OlympicDestroyer и повредили веб-серверы во время церемонии открытия.

Согласно уведомлению, хакеры «сокрыли истинный источник вредоносного ПО, имитируя код, используемый северокорейской группой, что создает возможность неправильной атрибуции», говорится в уведомлении. В октябре 2020 года Министерство юстиции предъявило шести сотрудникам российской разведки обвинение в нападении на Игры в Пхенчхане. ***(Jonathan Greig. 450 million cyberattacks attempted on Japan Olympics infrastructure: NTT // ZDNet***

(https://www.zdnet.com/article/nearly-450-million-cyberattacks-attempted-on-japan-olympics-infrastructure-ntt/). 21.10.2021).

***

Новое исследование показывает, что «ужасающее» состояние безопасности промышленных систем управления (АСУ ТП) подвергает критически важные службы серьезному риску.

Вам нужно только взглянуть на хаос, вызванный атакой программ-вымогателей, начатой против Colonial Pipeline вэтом году, что привело к паническим покупкам и нехватке топлива в некоторых частях США, чтобы увидеть, какие киберинциденты могут вызвать реальные нарушения в мире, и их последствия. может выйти далеко за рамки ущерба, который должна исправить одна компания.

Только в прошлом месяце порт Хьюстона отразил кибератаку, и нет оснований полагать, что кибератаки на операционные технологии (OT) не будут продолжаться или, возможно, станут более распространенными.

В пятницу SparshKulshrestha из CloudSEK опубликовал новый отчет, в котором исследуются АСУ ТП и их состояние безопасности в свете недавних кибератак против промышленных, коммунальных и производственных объектов. Основное внимание в исследовании уделяется АСУ ТП, доступным через Интернет.

«В то время как субъекты национального государства имеют множество инструментов, времени и ресурсов, другие субъекты угроз в первую очередь полагаются на Интернет для выбора целей и выявления своих уязвимостей», - отмечает команда.«Хотя в большинстве АСУ ТП применяются определенные меры кибербезопасности, человеческий фактор является одной из основных причин, из-за которой злоумышленники по-прежнему могут скомпрометировать их снова и снова».

Некоторые из наиболее распространенных проблем, обеспечивающих первоначальный доступ, упомянутые в отчете, включают слабые учетные данные или учетные данные по умолчанию, устаревшее или непропатченное программное обеспечение, уязвимое для эксплуатации ошибок, утечки учетных данных, вызванные третьими сторонами, теневые ИТ-службы и утечка исходного кода.

После проведения веб-сканирования уязвимых АСУ ТП команда сообщила, что были обнаружены «сотни» уязвимых конечных точек.

CloudSEK выделила четыре случая, которые, по словам компании, представляют собой текущие проблемы, связанные с кибербезопасностью промышленных и критически важных услуг сегодня:

Индийская компания по управлению водоснабжением: программное обеспечение, доступное с учетными данными производителя по умолчанию, позволило команде получить доступ к платформе управления водоснабжением. Злоумышленники могли вмешаться в калибровку системы водоснабжения, прекратить очистку воды и изменить химический состав водоснабжения.

Правительство Индии: на GitHub были найдены наборы учетных данных почтового сервера, принадлежащие правительству Индии.

Газотранспортная компания:веб-сервер этого важного поставщика услуг, отвечающий за управление и мониторинг газовых транспортных средств, был уязвим для атаки с использованием SQL-инъекции, а учетные данные администратора были доступны в виде открытого текста.

Центральная точка зрения: команда также нашла жестко запрограммированные учетные данные, принадлежащие правительству Индии, на веб-сервере, поддерживающем мониторы для видеонаблюдения в различных службах и штатах страны.

Агентство по кибербезопасности и безопасности инфраструктуры США (CISA) было проинформировано о результатах CloudSEK, а также связанных международных агентств.

«Из-за увеличения удаленной работы и онлайн-бизнеса большинство усилий по кибербезопасности было сосредоточено на ИТ-безопасности», - говорит Спарш Кулшреста, старший аналитик по безопасности в CloudSEK. «Однако недавние атаки OT стали своевременным напоминанием о том, почему традиционные отрасли и критическая инфраструктура требуют повышенного внимания, учитывая, что они составляют основу нашего общества и нашей экономики». ***(Charlie Osborne. Critical infrastructure security dubbed 'abysmal' by researchers // ZDNet (https://www.zdnet.com/article/critical-infrastructure-security-dubbed-abysmal-by-researchers/). 15.10.2021).***

***

Новая фишинговая кампания нацелена на сотрудников финансовых служб, использующих ссылки для загрузки того, что называется «вооруженным» документом Excel.

Фишинговая кампания, получившая название MirrorBlast, была обнаружена охранной фирмой ET Labs в начале сентября. Сотрудник компании по безопасности Morphisec проанализировал вредоносное ПО и отмечает, что вредоносные файлы Excel могут обходить системы обнаружения вредоносных программ, поскольку они содержат «чрезвычайно легкие» встроенные макросы, что делает его «особенно опасным» для организаций, которые зависят от безопасности на основе обнаружения и песочницы.

Макросы, скрипты для автоматизации задач, стали популярным инструментом кибератак. Хотя макросы в Excel по умолчанию отключены, злоумышленники используют социальную инженерию, чтобы обмануть потенциальных жертв и заставить их включить макросы.

Хотя макросы кажутся базовой техникой, они используются хакерами, спонсируемыми государством, потому что они часто работают.Ранее в этом году Microsoftрасширила свой интерфейс сканирования на вредоносное ПО (AMSI) для антивируса, чтобы справиться с ростом количества вредоносных макросови новой тенденцией злоумышленников использовать устаревшие макросы Excel 4.0 XLM (вместо более новых макросов VBA) для обхода систем защиты от вредоносных программ.

По словам Morphisec, цепочка атак в MirrorBlast напоминает методы, используемые хорошо зарекомендовавшей себя финансово мотивированной

киберпреступной группировкой из России, которую исследователи отслеживают как TA505. Группа действует по крайней мере с 2014 года и известна широким спектром инструментов, которые они используют.

«TA505 наиболее известен тем, что часто меняет используемые вредоносные программы, а также определяет глобальные тенденции распространения вредоносных программ», -отмечает в своем блоге исследователь Morphisec Арнольд Осипов.

Хотя атака MirrorBlast начинается с документа, прикрепленного к электронному письму, позже она использует URL-адрес Google feedproxy с приманкой SharePoint и OneDrive, которая выдает себя за запрос общего доступа к файлу. Щелчок по URL-адресу ведет к взломанному сайту SharePoint или поддельному сайту OneDrive. Обе версии приводят к вооруженному документу Excel.

Образец электронного письма MirrorBlast показывает, что злоумышленники используют тематику выпускаемой компанией информации об изменениях в рабочих условиях, связанных с COVID.

Morphisec отмечает, что код макроса может выполняться только в 32-разрядной версии Office из-за соображений совместимости с объектами ActiveX. Сам макрос выполняет сценарий JavaScript, предназначенный для обхода песочницы, проверяя, запущен ли компьютер в режиме администратора. Затем он запускает процесс msiexec.exe, который загружает и устанавливает пакет MSI.

Компания Morphisec обнаружила два варианта установщика MIS, в которых использовались допустимые инструменты создания сценариев под названием KiXtart и REBOL.

Сценарий KiXtart отправляет информацию о машине жертвы на сервер управления и контроля злоумышленника, такую как домен, имя компьютера, имя пользователя и список процессов. Затем он отвечает числом, указывающим, следует ли продолжить вариант Rebol.

Согласно Morphisec, сценарий Rebol ведет к инструменту удаленного доступа под названием FlawedGrace, который группа использовала в прошлом.

«TA505 - одна из многих финансово мотивированных групп угроз, действующих в настоящее время на рынке. Они также являются одной из самых творческих, поскольку имеют тенденцию постоянно менять атаки, которые они используют для достижения своих целей», - отмечает Осипов». ***(Liam Tung. This new phishing attack features a weaponized Excel file // ZDNet (https://www.zdnet.com/article/this-particularly-dangerous-phishing-attack-features-a-weaponized-excel-file/). 18.10.2021).***

***

«Ранее нераскрытая кампания кибершпионажа с использованием невиданных ранее вредоносных программ проникает в глобальные аэрокосмические и телекоммуникационные компании в рамках целенаправленной операции, которая была активна как минимум с 2018 года, но оставалась полностью незамеченной до июля этого года.

Кампания - это работа недавно раскрытой иранской хакерской группы под названием MalKamak, которая была подробно описана компанией Cybereason Nocturnus, занимающейся кибербезопасностью, которая обнаружила ее после того, как клиент позвонил ей для расследования инцидента безопасности.

Целью кампании кибер шпионажа, получившей название Operation GhostShell, является взлом сетей компаний аэрокосмической и телекоммуникационной отраслей с целью кражи конфиденциальной информации об активах, инфраструктуре и технологиях. Цели, которые не разглашаются, в основном находятся на Ближнем Востоке, но с дополнительными жертвами в США, Европе и России. Кажется, что каждая цель была выбрана нападающими.

«Это очень и очень целенаправленная атака», - сказал ZDNet Ассаф Дахан, руководитель отдела исследования угроз Cybereason. «Нам удалось идентифицировать только около 10 жертв по всему миру».

MalKamak распространяет ранее недокументированный троян удаленного доступа (RAT), известный как ShellClient, который разработан с расчетом на шпионаж - вот почему он оставался незамеченным в течение трех лет. Одна из причин, по которой вредоносное ПО остается настолько эффективным, заключается в том, что авторы приложили немало усилий, чтобы сделать его достаточно незаметным, чтобы избежать использования антивируса и других инструментов безопасности. Вредоносные программы получают регулярные обновления, так что это по-прежнему так.

«На каждой итерации они добавляют больше функциональности, они добавляют разные уровни скрытности», - сказал Дахан.

ShellClient даже начал внедрять клиента Dropbox для управления целевыми сетями, что затрудняет обнаружение, поскольку многие компании могут не заметить или не придать особого значения еще одному облачному инструменту совместной работы, выполняющему действия, если они вообще заметят это.

Это часть плана - использовать трояна для мониторинга систем, кражи учетных данных пользователей, тайного выполнения команд в сети и, в конечном итоге, кражи конфиденциальной информации. Каждой зараженной машине дается уникальный идентификатор, чтобы злоумышленники могли отслеживать свою работу в течение недель и месяцев, когда они шпионили за скомпрометированными сетями.

«Как только они окажутся внутри, они начинают проводить обширную разведку сети. Они определяют важные активы - драгоценности в короне, к которым они стремятся, ключевые серверы, такие как Active Directory, а также бизнес-серверы, которые содержат тип информации, который они после ", сказал Дахан.

Кампания успешно оставалась незамеченной до июля, когда для расследования инцидента были вызваны исследователи. Возможно, злоумышленники слишком уверены в своей тактике и переусердствовали, оставив доказательства, которые позволили исследователям идентифицировать кампанию и развертываемое вредоносное ПО.

«Судя по тому, что мы видим, в прошлом году они ускорились. Иногда, когда вы быстрее, вы можете быть немного небрежными или просто будет больше случаев, которые будут обнаружены», - объяснил Дахан.

Анализ инструментов и методов MalKamack привел исследователей к выводу, что атаки были результатом хакерской операции, разработанной в Иране, поскольку один из инструментов ShellClient RAT для атак с сбросом учетных данных является разновидностью SafetKatz, который был связан с предыдущими иранскими кампании. Атаки на телекоммуникационные и аэрокосмические компании, работающие на Ближнем Востоке, также соответствуют геополитическим целям Ирана.

Но хотя есть сходство с известными иранскими операциями кибершпионажа, поддерживаемыми государством, включая Chafer (APT39), который использует аналогичные методы для нацеливания на жертв на Ближнем Востоке, в США и Европе, а также APT Agrius, который имеет сходство в коде вредоносных программ, Исследователи полагают, что MalKamack - это новая иранская кибероперация, хотя, вероятно, она связана с другой деятельностью, спонсируемой государством.

Исследователи также считают, что операция GhostShell остается активной, и что MalKamack продолжит развивать методы проведения атак, чтобы продолжать кражу информации от целей. В настоящее время неизвестно, как злоумышленники получают первоначальный доступ к сети, но есть вероятность, что это происходит с помощьюфишинговых атакили использования незащищенных уязвимостей». ***(Danny Palmer. A company spotted a security breach. Then investigators found this new mysterious malware // ZDNet (https://www.zdnet.com/article/a-company-spotted-a-security-breach-then-investigators-found-this-new-mysterious-malware/). 06.10.2021).***

***

«Хакеры, ответственные за кибератаку на охрану окружающей среды Шотландии, пытались саботировать усилия по решению проблемы, говорится в новом отчете.

Вовремя инцидента Шотландское агентство по охране окружающей среды (Sepa) похитило более 4000 цифровых файлов.

В обзоре говорится, что атака в канун Рождества продемонстрировала «значительную скрытность и вредоносную изощренность».

Но также выяснилось, что план реагирования на киберинциденты Sepa был недоступен во время инцидента.

Это произошло потому, что, по словам независимых консультантов Азетс, отчет - вместе с планом аварийного восстановления наблюдателя - хранился на серверах, затронутых атакой, и не было доступной офлайн-версии или бумажной копии.

«Азетс» также обнаружил, что сотрудники первоначально отреагировали на нападение примерно в 00:01 24 декабря, но попытки передать проблему другим должностным лицам Sepa не увенчались успехом примерно до 08:00.

Хакеры предприняли попытки «взломать системы Sepa, поскольку команда пыталась восстановить и восстановить резервные копии», говорится в отдельном обзоре.

Но в обзоре полиции Шотландии говорится, что Сепа «не была и не является плохо защищенной организацией».

'Международно организованное преступление'

Сепа отклонил требование выкупа за атаку, на которое претендовала группа вымогателей Conti, после чего украденные файлы были размещены в Интернете.

Государственный орган заявил, что он стал «жертвой ужасного, организованного международным сообществом преступления», и добавил, что серия проведенных им проверок «ясно показывает, что мы хорошо защищены, но ни один режим кибербезопасности не может быть на 100% безопасным».

В одном из обзоров, проведенном Шотландским центром устойчивости бизнеса, говорится, что три копии данных Sepa хранятся в двух разных местах, а одна копия хранится в автономном режиме.

В отчете говорится, что «дизайн сети означал, что были затронуты оба сайта», но разделы этой части документа отредактированы, поэтому неясно, как это произошло.

"Бич киберпреступности"

После кибератаки Sepa восстановила большинство своих ключевых услуг, таких как прогнозирование наводнений, и сейчас строит новые ИТ-системы для их работы.

Исполнительный директор организации Терри А'Хирн сказал: «Большинство организаций, пострадавших от кибератак по всему миру, не афишируют эту атаку, и это их право.

«Мы знаем, что применили необычный подход, но убеждены, что мы поступаем правильно.

«Мы публикуем как можно больше обзоров, чтобы как можно больше организаций могли использовать наш опыт для лучшей защиты от этого растущего бедствия киберпреступности»…» ***(Hackers had second go at Sepa during cyber attack // BBC (https://www.bbc.com/news/uk-scotland-59054590). 27.10.2021).***

***

«По словам отраслевого органа, «беспрецедентная» и скоординированная кибератака поразила нескольких британских провайдеров услуг передачи голоса по интернет-протоколу (VoIP).

Промышленная организация Comms Council UK сообщила, что в последние недели несколько ее членов стали жертвами распределенных атак типа «отказ в обслуживании» (DDoS).

«Общая угроза возникла для всей отрасли», - добавил представитель.

Ofcom заявил, что осведомлен о ситуации.

DDoS-атаки работают путем наводнения веб-сайта или онлайн-сервиса интернет-трафиком в попытке отключить его или иным образом сделать недоступным.

В прошлом они часто отключали веб-сайты и иногда использовались для политических заявлений.

Но последняя волна атак была нацелена на VoIP якобы с целью вымогательства у этих компаний.

Провайдеры VoIP предлагают звонки через Интернет ряду клиентов, включая предприятия, а также государственные службы, включая полицию и NHS.

В заявлении Comms Council UK говорится, что DDoS-атаки на британские VoIP-компании произошли в течение последних четырех недель и «являются частью скоординированной международной кампании профессиональных киберпреступников, ориентированной на вымогательство».

Орган заявил, что поддерживает связь с правительством Великобритании, Ofcom и Национальным центром кибербезопасности (NCSC) по этому поводу.

Представитель Comms Council UK сообщил BBC, что он не может указать, сколько фирм пострадало, и добавил, что назвал бы масштаб атаки «беспрецедентным».

«Мы никогда не видели ничего подобного с момента основания в 2004 году», - сказал он.

«Угрозы выкупа исходили от многих поставщиков услуг, и в целом возникла угроза для всей отрасли».

«Злоумышленники пошли по этому пути, и атаки продолжаются».

Представитель Ofcom сказал: «Нам известно, что в последнее время в некоторых сетях возникают проблемы.

«Мы связываемся с ними, чтобы установить масштаб и причину проблемы, а также поддерживаем тесные связи с правительством Великобритании и Национальным центром кибербезопасности»…» ***(Cyber-attack hits UK internet phone providers // BBC (https://www.bbc.com/news/technology-59053876). 26.10.2021).***

***

«Электронные письма Craigslist, злоупотребляющие Microsoft OneDrive, предупреждают пользователей о том, что их объявления содержат «неприемлемый контент».

Музыкальные инструменты, запчасти для мотоциклов, а теперь и вредоносные программы - все это действительно есть на Craigslist.

В этом месяце злоумышленники взломали внутреннюю систему электронной почты Craigslist для доставки убедительных сообщений, в конечном итоге направленных на то, чтобы избежать контроля безопасности Microsoft Office для доставки вредоносного ПО.

Электронные письма, отправленные с подлинного IP-адреса Craigslist, информировали пользователей о том, что их опубликованная реклама содержала неприемлемый контент и нарушала условия и положения Craigslist, давая ложные инструкции о том, как избежать удаления их учетных записей.

Исследователи INKY обнаружили, что злоумышленники преобразовали HTML-код электронного письма в настраиваемый документ со ссылкой для

загрузки вредоносного ПО, загруженной на страницу Microsoft OneDrive. Эта страница олицетворяла такие крупные бренды, как DocuSign, Norton и Microsoft.

Это также позволило кампании обойти стандартную аутентификацию по электронной почте.

«Поскольку в URL-адресе для решения проблемы был размещен настроенный документ, размещенный в Microsoft OneDrive, он не появлялся ни в одном канале аналитики угроз, что позволяло ему обходить стороной большинство поставщиков средств обеспечения безопасности», - отмечают исследователи в публикации на этой неделе.

Злоупотребление анонимностью

Craigslist - это не одна гигантская распродажа. Его внутренняя система электронной почты также позволяет заинтересованным покупателям и продавцам связываться анонимно. Согласно отчету INKY, злоумышленники могли злоупотреблять этой почтовой системой Craigslist и доставлять аутентичные фишинговые электронные письма пользователям, которые активно пытались что-то продать на сайте.

Это означает, что жертвы, скорее всего, уже отправляли случайные запросы из системы Craigslist, поэтому вредоносные электронные письма просто смешивались.

«Craigslist знает личности всех, но если корреспондент не раскрывает подробностей, они совершенно анонимны для других пользователей системы», - говорится в отчете INKY. «Эта ситуация отлично подходит фишерам. Они могут стрелять своими отравленными стрелами из-за местного почтового прокси. И они стреляли - несколько раз в начале октября».

Фишинговые письма выглядели как уведомление от Craigslist о том, что реклама пользователя содержит неприемлемый контент. Затем в письме содержалась угроза забанить пользователя на платформе, если он не заполнит форму, доступную по злонамеренной ссылке.

Craigslist Фишинговые письма помечают "неприемлемое содержание"

«Политика публикации контента нашей платформы прямо запрещает неприемлемый контент, ваше объявление получило множество красных флажков», - говорится в письме. «Более подробное описание проблемы доступно в этой форме. Он будет доступен круглосуточно».

По словам INKY, щелкнув «форму», пользователи перейдут к документу Microsoft OneDrive.

«Похоже, что злоумышленники смогли манипулировать HTML-кодом электронного письма, чтобы создать эту кнопку и связать ее с OneDrive», - пишут исследователи. «При наведении указателя мыши на ссылку обнаружен русский домен (myjino [.] Ru)».

Щелчок по ссылке инициировал загрузку файла.ZIP, содержащего электронную таблицу с поддержкой макросов, которая доставляла вредоносное ПО. Чтобы обойти меры безопасности Microsoft Office и запустить макросы, вредоносные документы предлагали жертвам нажать кнопку «Включить редактирование» или «Включить контент», - сказал INKY.

«Электронная таблица олицетворяла DocuSign, а также использовала логотипы Norton и Microsoft, чтобы обозначить безопасность файла», - говорится в отчете. «На самом деле DocuSign не имеет службы под названием «Служба защиты DocuSign».

Когда команда INKY попыталась заставить вредоносное ПО работать, это привело к сообщению об ошибке 404, которое, по предположениям команды, было ошибкой злоумышленников или они уже были обнаружены и устранены хостом.

Тем не менее, команда INKY заявила, что эту атаку, размещенную на Craigslist, можно было использовать для установки инструмента удаленного доступа (RAT), запуска атаки вымогателя, внедрения имплантата первого уровня, такого как TrickBot, эксфильтрации конфиденциальных данных или развертывания кейлоггера.

INKY посоветовал пользователям Craigslist внимательно следить за такими атаками и добавил, что любые сообщения электронной почты, которые кажутся необычными, следует рассматривать как потенциально вредоносные.

«Еще один тревожный сигнал - это смешение платформ», - добавили аналитики. «Нет смысла решать проблему с Craigslist с помощью документа, загруженного в OneDrive». ***(Becky Bracken. Attackers Hijack Craigslist Emails to Bypass Security, Deliver Malware // Threatpost (https://threatpost.com/attackers-hijack-craigslist-email-malware/175754/). 26.10.2021).***

***

«В недавнем отчете было обнаружено, что 98 процентов компаний испытали хотя бы одну утечку облачных данных за последние 18 месяцев, по сравнению с 79 процентами в прошлом году. В том же отчете говорится, что почти 60 процентов из 200 опрошенных руководителей по информационной безопасности и лиц, ответственных за безопасность, считают отсутствие прозрачности и неадекватное управление идентификацией и доступом серьезной угрозой для своей облачной инфраструктуры.

От угроз программ-вымогателей до атак вредоносного ПО - компании по всему миру сталкиваются с огромным увеличением нарушений кибербезопасности, которые являются разрушительными и хорошо скоординированными. Независимо от того, предназначены ли они для того, чтобы люди нажимали на компрометирующие веб-страницы или открывали зараженные вложения электронной почты, большинство кибератак сегодня нацелены на человеческую ошибку. Помимо доступных технологий, обеспечивающих нашу безопасность, ваша организация также сильно зависит от своих сотрудников в принятии правильных решений в области безопасности.

Поэтому сейчас, более чем когда-либо, организациям необходимо укрепить свою защиту от настойчивых злоумышленников, которые, например, умело овладели искусством злоупотребления слабыми учетными данными (один из многих рисков, возникающих из-за того, что люди выбирают удобные, легко запоминающиеся пароли или повторно используют их. учетные записи).

Контрольный список плана реагирования на инциденты

Чтобы избежать перехода в режим аварийного восстановления во время атаки, корпорации должны методично планировать и готовиться к киберинцидентам, используя следующий контрольный список реагирования на инциденты, для минимизации ущерба и быстрого восстановления.

Тщательный план реагирования на инциденты может помочь компании быстро восстановиться и снизить затраты на инциденты. Также очень важно не только иметь план реагирования на инциденты, но и быть «готовым к реагированию на инциденты», что означает, что план периодически проверяется, подобно учению о пожаре.

Право собственности и ответственность. Первым шагом в разработке плана реагирования на инциденты является определение ролей в организации, которые будут нести ответственность за обеспечение выполнения программы. Это включает в себя членов команды, обученных шагам, инструментам и технологиям, включенным в план, и обеспечение того, чтобы план обновлялся с учетом изменений или обновлений внутри организации. Для старшего персонала и руководителей разумно взять на себя ответственность за план реагирования на инциденты, чтобы обеспечить его полную и успешную интеграцию на всех уровнях и ролях бизнеса.

Роли и контакты. В случае инцидента обычно затрагиваются все внешние и внутренние бизнес-стороны, в том числе группы высшего руководства, юристы, человеческие ресурсы, финансы, маркетинг и продажи. Все они должны знать, как их роли будут затронуты во время кибератаки и что от них ожидается для восстановления бизнеса.

Способы связи и список контактов -во время инцидента традиционные средства связи, такие как электронная почта или V0IP, могут быть недоступны. Чтобы обеспечить надлежащую и своевременную связь с клиентами и сотрудниками, организациям необходимо подготовить контактные данные и альтернативные методы связи. Это также включает в себя четкий план того, что будет сообщено кому и в какое время.

Запись и идентификация- после того, как инцидент произошел, все аспекты и детали инцидента должны быть зарегистрированы и задокументированы. Когда произошел инцидент? Кто это открыл? В какой момент вмешались службы безопасности и ИТ-специалисты? Наряду с этими шагами крайне важно определить тип и характер инцидента и подтвердить, что это действительно реальный инцидент.

Сдерживание - возможно, одним из самых важных шагов в плане является сдерживание угрозы и прекращение атаки. На этом этапе службы безопасности и ИТ-службы должны решить, безопасно ли наблюдать и изучать, или они должны немедленно сдерживать угрозу (отключая операции, что, конечно, очень разрушительно).Кроме того, службы безопасности и ИТ-службы должны определить масштаб атаки и раскрыть конфиденциальные данные. Используйте индикаторы компрометации (IoC), чтобы определить степень уязвимости систем, и обновите все брандмауэры и сетевую безопасность, чтобы собрать ценные доказательства для криминалистической экспертизы.

На этом этапе организациям необходимо предвидеть возможные юридические последствия и любое влияние на нормативные акты. Предприятиям необходимо спросить, следует ли продолжать оказание услуг их компании во время инцидента или необходимо участие правоохранительных органов, в зависимости от серьезности и чувствительности инцидента.

Искоренение и восстановление- одним из последних шагов контрольного списка является восстановление систем и программного обеспечения до их исходного состояния. Во время этого процесса службы безопасности и ИТ-службы должны собирать доказательства для надлежащих целей цифровой криминалистики и устранять любые существующие риски, чтобы злоумышленники не могли восстановить доступ. Этот шаг будет включать инвентаризацию журналов, памяти, аудита, сетевого трафика и образов дисков, а также исправление систем, закрытие доступа к сети, сброс паролей скомпрометированных учетных записей и определение основной причины инцидента для предотвращения подобных атак в будущем. Когда восстановление начнется, вы должны обеспечить целостность, доступность и конфиденциальность системы, чтобы вернуться к работе.

Извлеченные уроки- важно осмыслить киберинцидент и извлечь у него урок. Что сработало эффективно, а что нужно улучшить? Потратьте время на то, чтобы обдумать и составить ответный отчет, это поможет вашему бизнесу лучше подготовиться к другому инциденту. Извлечение уроков из инцидента также приведет к изменениям и дальнейшим инвестициям в людей, обучение и технологии, чтобы повысить уровень безопасности вашей организации в целом.

Создание плана инцидентов - трудоемкая и непростая задача, особенно когда кажется, что ваша компания непобедима против атак. Но факт в том, что с постоянно увеличивающимся размером ландшафта киберугроз и возможностью человеческих ошибок возрастает вероятность того, что ваша организация станет жертвой киберпреступности.

От вашей подготовки будет зависеть общее влияние на ваш бизнес? Разумно иметь четкий и твердый план реагирования на инциденты, чтобы помочь вашей организации сделать все возможное для снижения потенциального воздействия и рисков кибератаки. Будьте готовы к реагированию на инциденты и имейте надежный план реагирования на инциденты, который поможет вашей организации быстро восстановиться». ***(Joseph Carson. How to Build an Incident-Response Plan, Before Security Disaster Strikes // Threatpost (https://threatpost.com/incident-response-plan-security-disaster/175335/). 05.10.2021).***

***

«Новый злоумышленник, получивший название DEV-0343, был замечен в атаке на компании оборонных технологий США и Израиля, порты въезда в Персидский залив и глобальные морские транспортные компании, связанные с Ближним Востоком. Цель злоумышленника - захват учетной записи Microsoft Office 365.

Microsoft, которая начала отслеживать активность в конце июля 2021 года, подробно описала атаки в предупреждении, опубликованном в понедельник,

добавив, что виновные, похоже, склонны к шпионажу и имеют связи с Ираном. В нем говорится, что кибератаки «проводят масштабное распыление паролей» на учетные записи Office 365.

Распыление паролей - это процесс проверки списка имен пользователей и ряда различных паролей для учетных записей в Интернете в надежде найти совпадение и получить доступ к учетным записям, защищенным паролем. В этом случае злоумышленники обычно проводят атаки на «десятки или сотни учетных записей» в каждой целевой организации, сообщает Microsoft, и были замечены попытки использовать тысячи комбинаций учетных данных для каждой учетной записи.

На данный момент кампания охватила около 250 конкретных организаций, использующих облачный пакет Office от Microsoft, при этом менее 20 из них пострадали от компрометации, по данным компании. Однако «DEV-0343 продолжает совершенствовать свои методы для совершенствования своих атак», - предупредил компьютерный гигант.

Согласно анализу, атаки на данный момент проводятся с использованием эмулированного браузера Firefox или Chrome и ротации IP-адресов, размещенных в прокси-сети Tor. По словам Microsoft, в среднем каждая атака использует от 150 до 1000+ уникальных адресов, чтобы запутать операционную инфраструктуру.

«Изменение IP-адреса при каждой попытке ввода пароля становится все более распространенным методом среди изощренных групп угроз», - говорится в отчете. «Часто группы угроз рандомизируют пользовательский агент, который они используют, а также IP-адрес. Этот метод стал возможен благодаря появлению сервисов, предоставляющих огромное количество домашних IP-адресов. Эти службы часто включаются через вредоносные плагины браузера».

Такое использование прокси-адресов затрудняет разработку индикаторов или компрометации (IoC), но шаблоны, которые Microsoft наблюдала в атаках, включают:

Обширный входящий трафик с IP-адресов Tor для кампаний по рассылке паролей.

Эмуляция браузеров FireFox (наиболее распространенных) или Chrome в кампаниях со спреем паролей

Перечисление конечных точек Exchange ActiveSync (наиболее часто) или автообнаружения

Использование инструмента для перечисления /вводапароля, аналогичного инструменту «o365spray».

Использование автообнаружения для проверки учетных записей и паролей

«Операторы обычно нацелены на две конечные точки Exchange - Autodiscover и ActiveSync - в качестве функции используемого ими инструмента для перечисления / разбрызгивания паролей», - сообщает Microsoft. «Это позволяет DEV-0343 проверять активные учетные записи и пароли, а также дополнительно уточнить их действия по спрею паролей».

Предполагаемые связи с Ираном

Название группы, основанное на «DEV», - это просто временное обозначение Microsoft, обозначающее кластер развивающейся деятельности. Как только о злоумышленниках станет известно больше, Microsoft даст ему постоянное имя.

Однако на данный момент есть свидетельства, указывающие на то, что субъекты угрозы являются иранскими. Например, атаки были специально направлены на компании, которые производят радары военного уровня, технологии беспилотных летательных аппаратов, спутниковые системы, системы связи для реагирования на чрезвычайные ситуации, географические информационные системы (ГИС) и пространственную аналитику, заявила Microsoft, а также на порты и транспортные компании. По данным Microsoft, это согласуется с прошлыми атаками Ирана на судоходные и морские цели, а также с общими целями.

Компания принято к сведению. «Microsoft оценивает, что этот таргетинг поддерживает отслеживание иранским правительством служб безопасности и морских перевозок на Ближнем Востоке с целью улучшения их планов действий в чрезвычайных ситуациях... Получение доступа к коммерческим спутниковым изображениям, а также собственным планам и журналам доставки может помочь Ирану компенсировать его развивающуюся спутниковую программу».

Кроме того, группа наиболее активна с воскресенья по четверг с 7:30 до 20:30 по местному иранскому времени, а пиковая активность спрея паролей в Microsoft наблюдается с 7:30 до 14:30.

Как защититься от поглощения Office 365

Чтобы защититься от атак с использованием паролей, Microsoft предложила пользователям в первую очередь включить многофакторную аутентификацию.

В противном случае компания заявила, что другая защитная тактика включает использование беспарольных решений, таких как Microsoft Authenticator, для защиты учетных записей; обзор политик доступа к Exchange Online; заблокировать клиентам ActiveSync возможность обхода политик условного доступа; и блокировать весь входящий трафик от анонимных сервисов, где это возможно». ***(Tara Seals. Office 365 Spy Campaign Targets US Military Defense // Threatpost (https://threatpost.com/military-defense-spy-campaign/175425/). 12.10.2021).***

***

«Заправочные станции Национальной иранской компании по распределению нефтепродуктов (NIOPDC) сегодня прекратили работу из-за кибератаки, которая затронула всю распределительную сеть.

Инцидент привел к появлению ряда взломов электронных дорожных рекламных щитов, на которых показывались сообщения с требованием объяснений или просьбой о топливе.

Сеть NIOPDC насчитывает более 3500 станций по всей стране и поставляет нефтепродукты более 80 лет.

Хакеры повторяют предыдущую атаку

Расследование изучает причину сбоя, и в данный момент нет публичной информации о том, кто это сделал, но Иран обвиняет враждебную страну.

Подсказкой, которая также может быть ложной наводкой, является отображаемое на машинах сообщение «cyberattack 64411».

В записке упоминается кибератака в июле, в результате которой было нарушено движение поездов Ирана. Злоумышленники также модифицировали железнодорожные доски объявлений, чтобы указать, что хакеры вызвали задержку или отмену поездов, и показали номер телефона офиса верховного лидера Али Хаменеи.

Исследование, проведенное компанией SentinelOne, занимающейся кибербезопасностью, показало, что система железнодорожных вокзалов Ирана была атакована вредоносным ПО, специально созданным для удаления данных (очиститель файлов) под названием Meteor, которого раньше не было.

В результате сегодняшнего нападения некоторые иранцы часами ждали открытия заправочных станций и остались без топлива.

По сообщениям СМИ, сообщение «кибератака 64411» появилось у клиентов, которые пытались получить субсидированное топливо по цене 5 центов за литр или 20 центов за галлон с использованием государственных карт.

По мере распространения новостей о том, что распределительная сеть NIOPDC подверглась атаке, на цифровых рекламных щитах во многих городах Ирана стали появляться сообщения «Хаменеи! Где наше топливо?» и «Бесплатное топливо на станции Джамаран».

В некоторых местных СМИ сначала говорилось, что нарушение работы АЗС было вызвано технической неисправностью, а позже отмечалось, что проблема возникла из-за кибератаки.

По словам журналистов BBC Шаяна Сардаризадеи Киан Шарифи, государственное телевидение Ирана подтвердило сообщения о кибератаке на заправочные станции, а Высший совет киберпространства Ирана считает, что инцидент спонсируется государством, хотя пока рано говорить, какая страна за этим стоит». ***(Ionut Ilascu. Iranian gas stations out of service after distribution network hacked // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/iranian-gas-stations-out-of-service-after-distribution-network-hacked/). 26.10.2021).***

***

«В настоящее время злоумышленники используют математические символы на вымышленных логотипах компаний, чтобы избежать обнаружения антифишинговыми системами.

Один примечательный случай, обнаруженный аналитиками INKY, связан с подделкой Verizon, крупного американского поставщика телекоммуникационных услуг.

В этом случае субъекты используют символ квадратного корня, логический оператор NOR или сам символ галочки, что помогает создать небольшую оптическую дифференциацию, которая может обмануть детекторы спама на основе ИИ.

Однако для многих людей, которые не успевают за последними изменениями логотипов, эти слегка измененные логотипы выглядят достаточно хорошо, поэтому

у успешной доставки и уровня вовлеченности пользователей больше шансов остаться на высоком уровне.

У вас фальшивая голосовая почта

Все три типа спуфинга маскируются под уведомления голосовой почты, содержащие встроенную кнопку «Воспроизвести», при нажатии которой пользователь попадает на фишинговый портал, созданный так, чтобы выглядеть как веб-сайт Verizon.

Целевой домен явно не является частью официального веб-пространства Verizon, в одном из примеров, приведенных в отчете, является sd9-08 [.] Click.

Актеры сделали ставку на невнимательность цели, иначе подделанный сайт выглядит довольно убедительно. Кроме того, Inky обнаружил, что эта фишинговая кампания основывалась на недавно зарегистрированных доменах, о которых не было зарегистрировано.

Логотип на клонированном сайте является подлинным, поскольку злоумышленники украли большую часть элементов HTML и CSS с настоящего сайта Verizon.

Прокручивая поддельную страницу вниз, посетитель найдет предполагаемую голосовую почту, но ему разрешен доступ к ней только в том случае, если они предоставят учетные данные своей учетной записи Office365 в форме входа.

Первая попытка приведет к получению сообщения «неправильный пароль», тогда как вторая попытка приведет к фиктивной ошибке, завершающей процедуру входа в систему.

Это делается для злоумышленников, чтобы гарантировать, что жертва не ошиблась при вводе пароля с первой попытки, так что это, по сути, шаг «гарантии качества».

Когда вы получаете такое электронное письмо, тщательная проверка является важным фактором, чтобы не стать жертвой такого мошенничества. Никогда не нажимайте на встроенные кнопки, всегда проверяйте URL-адрес сайта, на котором вы собираетесь ввести какие-либо учетные данные, и, наконец, учитывайте реалистичность ситуации.

В этом случае сообщение от Verizon призывает получателей ввести свои учетные данные Office365, что в данной ситуации не имеет смысла. Если содержимое электронного письма по какой-либо причине не имеет смысла, обычно это фишинг, и письмо следует удалить». ***(Bill Toulas. Phishing campaign uses math symbols to evade detection // Bleeping Computer® (https://www.bleepingcomputer.com/review/security/phishing-campaign-uses-math-symbols-to-evade-detection/). 12.10.2021).***

***

«Рекордный по количеству кибератак 2020 год принёс потери данных в результате взлома IT-систем компаний, правительственных организаций и частных лиц на сумму $2,5 трлн. Росту количества и качества кибератак способствовало появление новых технологий — глубокого обучения ИИ и 5G.

Из-за отсутствия должного уровня информирования и привлечения внимания к проблеме, повсеместно нарушается «кибергигиена» (надежные пароли,

соответствующее программное обеспечение, многофакторная аутентификация и прочее). Возможно, вся IT-индустрия опасается, что широкое и повсеместное обсуждение проблем кибербезопасности отпугнёт большую часть пользователей высоких технологий и клиентов IT-гигантов из-за ощущения финансовой беспомощности перед нарастающей угрозой.

Если бы в новостях ежедневно сообщали о том, в каком объеме утекают медицинские данные из организаций здравоохранения, общественность выступила бы категорически против хранения такой информации в электронном виде. В США медицинские данные утекли из 90% всех медицинских организаций за последние три года. В России, согласно отчёту InfoWatch, из 404 случаев (на 100 млн записей) на медицинскую информацию пришлось 10% утечки всех данных.

По прогнозам аналитиков, если население планеты будет и дальше расширять использование информационных технологий и не изобретет совершенные методы защиты от хакерских атак, то к 2025 году киберпреступность будет стоить миру $10,5 трлн в год. Новые атаки будут происходить каждые 2 секунды, поскольку злоумышленники постепенно улучшают свои вредоносные программы.

Тревогу нужно бить прямо сейчас: каждую минуту из-за киберпреступности теряются $2,9 млн в результате взлома криптовалютных бирж, потерь от фишинговых атак, скомпрометированных записей идентификаторов, вредоносных программ и т. д.

Еще одним лакомым куском для киберпреступников является интернет вещей (IoT). Именно в этих системах будет сосредоточен основной объем передачи и обработки информации. Уже сегодня устройства IoT подвергаются 5200 кибератакам каждый месяц. Наиболее уязвимыми устройствами являются ноутбуки, компьютеры, смартфоны и планшеты, сетевые камеры и устройства хранения данных, а также устройства для потоковой передачи видео.

Критической для национальной безопасности является ситуация, когда кибератакам подвергаются автоматизированные системы управления (АСУ) на промышленных предприятиях. В первом полугодии 2021 года такие атаки были заблокированы на 33,8% компьютеров АСУ во всём мире, что на 1,2% больше по сравнению с аналогичным периодом 2020 года. В России доля атакованных компьютеров АСУ составила 39,4% и показала рост на 7,2%. Наиболее часто атаковались АСУ машиностроения, энергетики и нефтегазовой отрасли.

Особого внимания к защите информационных систем от кибератак требуют такие жизненно важные сферы, как водоочистные сооружения, водопроводные системы и электросети. При этом в России четыре из пяти объектов электроэнергетики могут быть уязвимы для кибератак из-за рубежа в том числе и из-за использования иностранных операционных систем и компьютерного оборудования.

Что касается энергетики в целом, то примеры последних 7 лет заставляют крепко задуматься о том, стоит ли удобство в управлении и экономия от использования информационных технологий потенциальных потерь для общества и экономики.

В 2020 году жертвой кибератаки стала Европейская сеть операторов систем передачи электроэнергии (ENTSO-E).

В июне 2019 года The New York Times сообщила, что США начали кибератаки на российскую энергосистему.

В декабре 2016 года произошла кибератака на Украину — хакеры оставили потребителей в некоторых районах Киева без электричества на час, после отключения электроподстанции.

В декабре 2014 года была взломана Южнокорейская ядерно-гидроэнергетическая компания Korea Hydro and Nuclear Power: хакеры похитили и выложили в сеть планы и инструкции по эксплуатации двух ядерных реакторов, а также данные 10 тысяч сотрудников.

Причиной кибератак является не только нажива отдельных групп хакеров, но и технологические войны. С развитием IT-индустрии и обслуживающей её науки технологическое неравенство постепенно становится инструментом политического давления.

По прогнозам, к 2027 году рынок кибербезопасности будет стоить $403 млрд. Это сулит очень хорошие перспективы для IT-компаний, которые в предвкушении этого солидного куска пирога будут выступать за то, чтобы знания о реальных объемах киберпреступности были доступны ровно в том объеме, чтобы поддерживать спрос на их продукты на достаточно высоком уровне». ***(Ангелина Потеряйко. Кибербезопасности в мире не будет? //Regnum (https://regnum.ru/news/polit/3406877.html). 25.10.2021).***

***

«Компания HP представила отчет Wolf Security Threat Insights Report с анализом кибератак за третий квартал. Данные для него были собраны с виртуальных машин пользователей HP Wolf Security в период с июля по сентябрь. В отчете эксперты описывают выявленные методы и инструменты злоумышленников для обхода средств защиты от взлома.

В частности, специалисты HP Wolf Security изучили участившиеся случаи использования уязвимостей нулевого дня. Эксплойты CVE-2021-40444i построены на удаленном исполнении вредоносного кода на компьютере жертвы. Эта уязвимость позволяет использовать движок браузера MSHTML в пакете программ Microsoft Office– впервые она была выявлена специалистами по безопасности 8 сентября, за неделю до выпуска очередного обновления.

Уже 10 сентября – всего через тридня после публикации первого бюллетеня об угрозе– группа исследователей HP обнаружила на GitHub информацию, предназначенную для автоматизации создания этого эксплойта. В отсутствие обновлений системы данная уязвимость позволяла злоумышленникам взламывать конечные устройства при минимальном взаимодействии с пользователями. Эксплойт использует вредоносный архивный файл, который разворачивает вредоносное ПО через документ Office. При этом пользователям ненужно открывать файл или включать какие-либо макросы для его предварительного просмотра. Открытия проводника достаточно, чтобы инициировать атаку, о которой владелец устройства зачастую даже не будет подозревать. После взлома устройства злоумышленники могут установить в системы бэкдоры, которые могут

быть проданы, например, другим преступным группам, использующим вредоносные программы с требованием выкупа.

Среди других угроз можно отметить рост числа киберпреступников, использующих сервисы поставщиков облачного ПО и ресурсы веб-провайдеров для размещения вредоносного ПО. Кпримпру, входе недавней кампании GuLoader был обнаружен вредоносный код Remcos Remote Access Trojan (RAT) – этот вирус использует удаленный доступ для обхода систем обнаружения угроз, скрываясь под видом обычных файлов на крупнейших платформах, таких как OneDrive. Специалисты HPWolf Security также обнаружили несколько семейств подобных вредоносных программ, размещенных в социальных сетях и на игровых платформах, таких как Discord.

Кроме того, эксперты выделяют вредоносные программы наJavaScript, способные обойти средства обнаружения: речь идет о распространении зараженных RAT-программ, написанных на языке JavaScript, через вложения электронной почты. Скрипты на JavaScript сложнее распознать и обнаружить среди всех данных, чем в документах с расширениями Office или в двоичных файлах. Вредоносное ПО RAT становится популярнее всреде злоумышленников, стремящихся украсть учетные данные бизнес-пользователей или получить доступ крипто кошелькам. Также опасен переход на файлы HTA, который позволяет распространять вредоносный код водин клик: троян Trickbot теперь оказывается накомпьютерах жертв после получения файлов HTA (приложение HTML), распространяющих вредоносное ПО посистеме сразу после открытия вложенного документа или архива, содержащего вредоносный код. Поскольку этот типфайлов еще неполучил широкого распространения, вредоносный код, скрытый вHTA-файлах, сменьшей долей вероятности будет замечен средствами обнаружения.

«Среднее время, которое требуется компаниям для применения, тестов и внедрения патчей безопасности ссоответствующими проверками, составляет 97 дней, что дает киберпреступникам возможность использовать это «окно уязвимости». Поначалу использовать подобные уязвимости могли только высококвалифицированные хакеры, но появление скриптов для автоматизации написания кода снизило порог вхождения, сделав этот тип атак доступным для менее опытных и технически подготовленных злоумышленников. Это существенно увеличивает риск для бизнеса, поскольку эксплойты нулевого дня превращаются в товар и становятся доступнее для массового рынка, например, в даркнете,– объясняет Алекс Холланд (Alex Holland), старший аналитик вредоносного ПО из группы исследования угроз безопасности HP Wolf Security.– Подобные новые уязвимости, как правило, не отслеживаются средствами обнаружения, поскольку исходные сигнатуры могут быть несовершенными и быстро устаревать по мере оценки масштабов эксплойта. Мы ожидаем, что эксплуатация кода CVE-2021-40444 станет новым орудием киберпреступников, возможно, даже заменит собой распространенные вредоносные программы, используемые сегодня для первоначального получения доступа к системам, например, те, которые задействуют уязвимость вEquation Editor».

Среди ключевых выводов исследования, основанных на данных, полученных с миллионов устройств, на которых работает HP Wolf Security, можно отметить то,

что 12% выявленных вредоносных программ для электронной почты сумели обойти хотя бы один шлюз сетевого сканирования, 89% обнаруженных вредоносных программ были доставлены по электронной почте, в то время как на долю веб-загрузок пришлось 11%, а на другие способы доставки, такие как заражение через внешние устройства хранения– менее 1% зараженного ПО. Наиболее распространенными типами вложений, используемых для доставки вредоносного ПО, были архивные файлы (38%– по сравнению с 17,26% в прошлом квартале), документы Word (23%), электронные таблицы (17%) ифайлы.EXE(16%), сообщают эксперты. Пять самых распространенных фишинговых атак были связаны с такими бизнес-операциями, как «оформление» и«оплата» заказа, «реклама новых товаров», «предложение» и«спрос».

«В современных условиях организациям необходим многоуровневый подход кбезопасности конечных точек, который бы следовал принципам Zero Trust для сдерживания и предотвращения наиболее распространенных направлений атак, в том числе атак через электронную почту, браузеры и загрузки. Это позволит свести к минимуму вероятность атак для целых классов угроз, предоставив организациям необходимый временной зазор для своевременного устранения уязвимостей без вреда для бизнес-процессов»,– считает Йэн Пратт (Ian Pratt), руководитель отдела безопасности персональных систем в HP». ***(Евгений Куликов. Средства автоматизации упрощают киберпреступникам эксплуатацию уязвимостей нулевого дня // Компьютерное Обозрение (https://ko.com.ua/sredstva_avtomatizacii_uproshhayut_kiberprestupnikam_jekspluataciyu_uyazvimostej_nulevogo_dnya_139131). 25.10.2021).***

***

«Исследователи Check Point Research выпустили очередной отчет о брендах, которые чаще всего использовались злоумышленниками в фишинговых атаках в третьем квартале. В нем представлены компании, чьи ресурсы киберпреступники имитировали для кражи персональных данных и платежной информации пользователей.

Пальму первенства в третьей четверти года снова получила компания Microsoft– несмотря на то, что общее число упоминаний бренда в фишинговых письмах снизилось по сравнению со вторым кварталом. Злоумышленники использовали бренд ИТ-гиганта в 29% всех попыток фишинговых атак. В предыдущей четверти этот показатель составлял 45%. Amazon опередила компанию DHL, заняв второе место. В третьем квартале бренд Amazon использовался в 13% фишинговых атак, во втором данный показатель составлял 11%. Это свидетельствует о том, что мошенники учитывают рост популярности онлайн-шопинга в преддверии праздничного сезона.

Эксперты Check Point Research предупреждают о появлении нового тренда: втретьем квартале злоумышленники стали чаще использовать бренды социальных сетей. Представители данного сегмента впервые в этом году вошли в десятку лидеров по количеству попыток фишинга.

Топ брендов, которые злоумышленники чаще всего использовали в фишинговых атаках в третьем квартале:

Microsoft (29% проанализированных фишинговых атак вмире);
Amazon (13%);
DHL (9%);
BestBuy (8%);
Google (6%);
WhatsApp (3%);
Netflix (2.6%);
LinkedIn (2.5%);
PayPal (2.3%);
Facebook (2.2%).

В фишинговых атаках злоумышленники стремятся имитировать официальный сайт известного бренда, выбирая похожее доменное имя или URL-адрес и копируя дизайн страницы. Ссылку на поддельный сайт потенциальным жертвам отправляют по электронной почте или посредством SMS. Также на фишинговый сайт можно попасть случайно, просматривая страницы в Интернете, или через вредоносное мобильное приложение. Очень часто на таких сайтах содержится специальная форма для сбора учетных данных, платежной и другой конфиденциальной информации пользователей.

Для защиты от фишинговых атак с использованием брендов, эксперты Check Point Software Technologies рекомендуют не доверять электронным письмам, запрашивающим конфиденциальную информацию, проверять такие сообщения идомены н наличие орфографических и грамматических ошибок. Также не стоит моментально реагировать на тревожные уведомления, требующие срочных действий, например письма о компрометации учетных записей– чаще всего это попытки фишинга. Помните, что ни в коем случае нельзя открывать вложения из подозрительных писем, особенно в форматах Word, Excel, PowerPoint иPDF». ***(Социальные сети впервые вошли в топ брендов, используемых мошенниками в фишинговых атаках //Компьютерное Обозрение(https://ko.com.ua/socialnye_seti_vpervye_voshli_v_top_brendov_ispolzuemyh_moshennikami_v_fishingovyh_atakah_139096). 20.10.2021).***

***

«СМИ сообщают, что начиная с прошлой недели как минимум семь email-провайдеров пострадали от мощных DDoS-атак, что привело к длительным перебоям в их работе.

По данным издания The Record, все эти атаки были организованы одним и тем же злоумышленником, который вымогал выкупы у своих жертв. DDoS начался в минувший четверг, 21 октября и продолжается до сих пор. Атаки в основном нацелены на небольшие компании, которые предоставляют email-сервисы, ориентированные на безопасность и конфиденциальность: Runbox, Posteo, Fastmail, TheXYZ, Guerilla Mail, Kolab Now и RiseUp.

Журналисты пишут, что вскоре после атак компании получают электронные письма с требованием выкупа в размере 0,06 BTC (около 4000 долларов США). Хакер, подписавшийся как Cursed Patriarch, отводит пострадавшим три дня на оплату, а в противном случае угрожает увести сервисы жертв в офлайн надолго.

Компания Posteo так же подтверждает в своем блоге, что получила угрозы, и злоумышленники вымогают у нее деньги, однако платить в Posteo отказались. Аналогичные заявления можно увидеть в блогахRunboxиTheXYZ.

Пиковые значения атак, по словам пострадавших, достигали 50 и 256 Гбит/сек.

The Record отмечает, что эти инциденты не связаны с недавними вымогательскими DDoS-атаками на VoIP-провайдера Voipfoneи провайдера игровых серверов Sparked. По словам собственных источников издания, эти атаки осуществлены разными злоумышленниками». ***(Мария Нефёдова. Несколько email-провайдеров подверглись DDoS-атакам // xakep (https://xakep.ru/2021/10/26/email-ddos/). 26.10.2021).***

***

«Хакери продавали на чорному ринку або використовували викрадені ютуб-канали для махінацій з криптвалютою. Вартість одного акаунта становила 3-4 тисячі доларів.

Компанія Google 20 жовтня повідомила, що запобігла масованій атаці «російськомовних» хакерів на понад чотири тисячі блогерів YouTube.

«З кінця 2019 року наша команда припиняє фішингові кампанії, організовані з метою отримання фінансової вигоди, націлені на користувачів YouTube із застосуванням шкідливого програмного забезпечення з отримання доступу до cookie-файлів», – йдеться в повідомленні.

Група аналізу загроз Google виявила, що хакерів набирали на російськомовному форумі. Вони розсилали блогерам фішингові листи з пропозиціями співпраці. Хакери «заманювали [блогерів] фальшивими можливостями співпраці (рекламою антивірусного програмного забезпечення, VPN, музичних програвачів, редагування фотографій або онлайн-ігор)». Після того, як блогери натискали на фішингові посилання, хакери отримували доступ до їхніх cookie-файлів та даних, зокрема, доступ до акаунтів на YouTube.

Ці ютуб-канали хакери продавали на чорному ринку або використовували для махінацій з криптвалютою. Вартість одного акаунта становила 3-4 тисячі доларів.

Google повідомив, що йому вдалося заблокувати 1,6 мільйона фішингових повідомлень і відновити 99% вкрадених акаунтів. Через цю ситуацію компанія звернулася до Федерального бюро розслідувань США». ***(Google повідомив про атаку «російськомовних» хакерів на блогерів YouTube // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/28336/2021-10-21-google-povidomyv-pro-ataku-rosiyskomovnykh-khakeriv-na-blogeriv-youtube/). 21.10.2021).***

***

«Соцсеть экс-президента США Дональда Трампа Truth Social, о создании которой он объявил накануне, подверглась хакерской атаке. Об этом пишет The New York Times (NYT).

Злоумышленники утверждают, что через несколько часов после объявления о создании TRUTH Social они смогли получить доступ к бета-версии платформы.

Киберпреступники создали фейковые учетные записи от имени Трампа и его бывшего помощника Стива Бэннона. На фальшивой странице экс-президента США они разместили фотографию испражняющейся свиньи и нецензурные высказывания в адрес основателя Twitter Джека Дорси.

Разработчикам пришлось удалить эти учетные записи и закрыть доступ к сайту. Его официальный релиз был запланирован на 2022 год.

Хакеры предпочли скрыть свои личности, однако утверждают, что связаны с группировкой Anonymous. По их словам, взлом соцсети был частью их "войны против ненависти". Кроме того, они хотели развлечься». ***(Хакеры взломали соцсеть Трампа до ее запуска // SecurityLab.ru (https://www.securitylab.ru/news/525879.php). 27.10.2021).***

***

Діяльність хакерів та хакерські угруповування

«Компанія Microsoft опублікувала звіт Digital Defense Report, у якому викриває російських хакерів, розповідає агентство CNN. У звіті згадані кіберзлочинці також інших країн.

Російські хакери підтримуються на державному рівні, стверджує Microsoft. Їхні атаки у більшості випадків порушують роботу урядів та інститутів США, України, Великобританії та, меншою мірою, інших країн світу. За рік рівень успішних вторгнень зріс у півтора раза – з 21% до 32%. Це зауважує адміністрація США, яка намагається зміцнити оборону проти кібершпигунства Росії. А минулого місяця Європейський Союз викрив операції російських хакерів і зупинив витік інформації, спрямований на «втручання у демократію». В Україні кількість клієнтів Microsoft, які постраждали від атак, зросла до 1200. Паралельно з нарощуванням військової присутності на кордоні з Україною, Росія активізує хакерські групи, відомі своїм проривом через програмне забезпечення компанії SolarWinds. У 2020 році вони порушили діяльність щонайменше дев’яти федеральних агентств США і вони ж останні три місяці намагаються зламати безпеку урядових організацій Сполучних Штатів та Європи. У розпорядженні Москви є цілий ряд хакерських команд, які виконують різні місії проти цілей у США та союзних країнах, кажуть аналітики. Деякі з цих груп спеціалізуються на проникненні для простого збору інформацію. Експертів Microsoft непокоїть очевидна підготовка до нападів на критичну інфраструктуру США, України та країн Західної Європи. Одну з таких груп, відому як Berserk Bear, пов’язують із порушеннями промислового програмного забезпечення в електромережах США у 2018 році. Хакери, яких деякі аналітики пов’язують із розвідувальним агентством ФСБ Росії, у 2019 та 2020 роках зламала вебсайт однієї з найбільших українських енергетичних компаній та міжнародного аеропорту Сан-Франциско, свідчить у звіті Джо Словік, колишній спеціаліст з кібербезпеки ВМС США. У звіті наведено комплексні дані щодо атак з липня 2020 року по червень 2021.

Розглядались хакерські групи з Росії, Китаю, Ірану, Північної Кореї, В'єтнаму, Туреччини. Країни, які піддавалась наймасштабнішим нападам: - США

— 46%, - Україна — 19%, - Великобританія — 9%. Сектори, які піддавались найактивнішим атакам: - уряди – 48%, - неурядові організації та аналітичні центри – 31%, - освіта та міжурядові організації – по 3% Експерти Microsoft поділили хакерські групи за країнами походження та особливістю нападів. Найбільш активними хакерськими групами були: Nobelium (59%) – Росія – атаки на уряди, аналітичні центри, дипломатичні установи, IT-компанії, телекомунікаційні мережі, Thallium (16%) – Північна Корея – атаки на аналітичні центри, дипломатичні установи, наукові центри, Phosphorus (9%) – Іран – дипломатичні установи, ядерні інституції, наукові установи, журналісти. Крістін Гудвін, заступник генерального радника та керівник підрозділу цифрової безпеки Microsoft, зауважує: США та їхні союзники засуджують Росію та Китай, але це держави – лідери у кібершпигунстві – не зупиняє». ***(Елена Бурдейная. Microsoft викриває російських хакерів, які готують напад на Україну // Comments.ua (https://it.comments.ua/ua/news/technology/microsoft-vikrivae-rosiyskih-hakeriv-yaki-gotuyut-napad-na-ukrainu-685691.html). 07.10.2021).***

***

«Twitter заблокировал аккаунты северокорейской хакерской группы, нацеленной на исследователей безопасности.

Аккаунты социальных сетей, @ lagal1990 и @ shiftrows13, были заблокированы в этом месяце после того, как «выдавали себя за исследователей безопасности», по словам аналитика Google Threat Analysis Group (TAG) Адама Вейдерманна, который добавил, что профили «опирались на ажиотаж 0-days чтобы получить последователей и завоевать доверие ".

Как отмечает Threatpost, еще один аккаунт, @ lagal1990, был закрыт по той же причине в августе.

Кампания, предположительно созданная кибератаками из Северной Кореи при поддержке государства, отслеживалась командой Google TAG в течение последнего года.

Кампания, впервые задокументированная в январе 2021 года, включает создание сети поддельных профилей на разных платформах, включая Twitter, LinkedIn, Keybase и GitHub.

Поддельные профили основаны на интересе к эксплойтам и ошибкам нулевого дня, чтобы создать ауру доверия и публиковать контент, такой как код подтверждения концепции (PoC) и методы эксплойтов.

По словам Вейдерманна, фальшивые аккаунты обнаружили исследователи Франсиско Алонсо и Хавьер Маркос.

«Мы (TAG) подтвердили, что они напрямую связаны с группой учетных записей, о которых мы писали ранее в этом году», - прокомментировал Вейдерманн.«В случае @ lagal1990 они переименовали учетную запись GitHub, ранее принадлежавшую другому из их профилей Twitter, которая была закрыта в августе, @ mavillon1».

Кластер учетных записей используется для достижения намеченных целей, включая хорошо известных и заслуживающих доверия исследователей безопасности. В Интернете также был опубликован исследовательский блог, и в

Интернете были загружены видеоролики, которые утверждали, что они являются доказательством эксплойтов и ошибок.

«Они использовали эти профили Twitter для размещения ссылок на свой блог, публикации видео с заявленными ими эксплойтами, а также для усиления и ретвита сообщений из других учетных записей, которые они контролируют», - сообщает Google TAG.

Однако, как только связь установлена, северокорейская группа затем спрашивает своих целей, заинтересованы ли они в сотрудничестве в исследованиях безопасности.

Затем ссылки отправляются исследователям в блог, содержащий эксплойты браузера, включая Internet Explorer нулевого дня, разоблаченного в январе.В качестве альтернативы им также может быть отправлен вредоносный файл проекта Visual Studio, содержащий бэкдор, предоставляющий злоумышленникам доступ на машину их жертвы - и содержащуюся в нем информацию.

В марте группа создала фальшивую турецкую компанию по обеспечению безопасности под названием SecuriElite с партией профилей, связанных с этой фирмой, якобы состоящей из исследователей кибербезопасности и рекрутеров.

На прошлой неделе Google TAG задокументировал усилия по противодействию атакам APT35, иранской группы, специализирующейся на фишинговых кампаниях против пользователей Google с высоким уровнем риска, включая сотрудников кампании во время выборов в США 2020 года».***(Charlie Osborne. Twitter accounts linked to cyberattacks against security researchers suspended // ZDNet (https://www.zdnet.com/article/twitter-accounts-linked-to-cyberattacks-against-researchers-suspended/). 19.10.2021).***

***

«Спонсируемая Северной Кореей хакерская группа Lazarus переключила свое внимание на новые цели, и исследователи Kaspersky по безопасности наблюдали, как расширяют свои возможности атак на цепочку поставок.

Lazarus использовал новый вариант бэкдора BLINDINGCAN для нападения на южнокорейский аналитический центр в июне после его развертывания для взлома латвийского ИТ-поставщика в мае.

«В первом случае, обнаруженном исследователями «Лаборатории Касперского», Lazarus разработал цепочку заражения, которая возникла из-за того, что законное южнокорейское программное обеспечение безопасности развертывало вредоносную нагрузку», - заявили исследователи.

«Во втором случае целью была компания, разрабатывающая решения для мониторинга активов в Латвии, нетипичная жертва для Lazarus».

Бэкдор, использованный в этих атаках, был впервые идентифицирован CISA и ФБР. Они обнаружили, что он может удалить себя из скомпрометированных систем, чтобы избежать обнаружения, эксфильтровать данные, порождать и уничтожать процессы, а также изменять временные метки файлов и папок.

Согласно отчету Kaspersky о тенденциях APT в третьем квартале 2021 года, Lazarus также доставил троян удаленного доступа (RAT) COPPERHEDGE, используя бэкдор BLINDINGCAN.

Тот же RAT также использовался Lazarus при нацеливании на криптовалютные биржи и связанные с ними объекты в прошлом.

Эта вредоносная программа известна тем, что помогает операторам выполнять задачи по разведке системы, запускать произвольные команды на зараженных устройствах и извлекать украденные данные.

Старое вредоносное ПО, перепрофилированное для кибершпионажа

Lazarus Group(также отслеживаются как СКРЫТОМ COBRAс помощью разведывательного сообщества США) является военным хакерство группа при поддержке Корейской Народно-Демократической Республики и действует с 2009 года, покрайней мере.

Они известны тем, что нацелены на крупные организации, такие как Sony Films in Operation Blockbusterи несколько банков по всему миру,а также за координацию глобальной кампании по вымогательству WannaCryв 2017 году.

Совсем недавно Google обнаружил Lazarus в январе во время атак социальной инженерии, нацеленных на исследователей безопасности с использованием тщательно продуманных псевдонимов «исследователей безопасности» в социальных сетях и в аналогичной кампании в марте.

В том же месяце они также использовали ранее недокументированный бэкдор под названием ThreatNeedle в крупномасштабной кампании кибершпионажа, нацеленной на оборонную промышленность более чем десятка стран.

В июне исследователи «Лаборатории Касперского» также увидели, как Lazarus развернул свою вредоносную среду MATA для целей кибершпионажа.

MATA может нацеливаться на Windows, Linux и macOS, и Lazarus ранее использовал его в 2020 году для кражи данных при атаках программ-вымогателей.

«Эти недавние события подчеркивают две вещи: Lazarus по-прежнему интересуется оборонной промышленностью и также стремится расширить свои возможности с помощью атак на цепочки поставок», -сказал Ариэль Юнгейт, старший исследователь безопасности в Kaspersky.

«При успешном проведении атаки на цепочки поставок могут привести к разрушительным результатам, затрагивая гораздо больше, чем одну организацию - что мы ясно видели при атаке SolarWinds в прошлом году».

Министерство финансов США санкция три КНДР спонсируемый хакерских групп (Lazarus, Bluenoroff и Andariel) в сентябре 2019 года.

Правительство США также предлагает вознаграждение в размере до 5 миллионов долларов за информацию о кибер-активности хакеров в КНДР, чтобы помешать их деятельности или выявить северокорейских террористов». ***(Sergiu Gatlan. North Korean state hackers start targeting the IT supply chain// Bleeping Computer® (https://www.bleepingcomputer.com/news/security/north-korean-state-hackers-start-targeting-the-it-supply-chain/). 26.10.2021).***

***

«Анализ 500 хакерских инцидентов в широком спектре отраслей выявил тенденции, характеризующие зрелость того, как хакерские группы действуют сегодня.

Исследователи «Лаборатории Касперского» сосредоточили свое внимание на российском подполье киберпреступлений, которое в настоящее время является одной из самых плодовитых экосистем, но многие элементы в их выводах являются общими знаменателями для всех групп хакеров по всему миру.

В поисках новых возможностей

Одним из ключевых выводов исследования является то, что уровень безопасности офисного программного обеспечения, веб-сервисов, почтовых платформ и т. Д. Повышается.

Как объясняет Касперский, количество уязвимостей браузеров уменьшилось, и сегодня веб-сайты не так легко взломать и использовать, как векторы заражения.

Это привело к тому, что веб-инфекции стали слишком сложными для преследования несложных групп угроз.

То же самое и с уязвимостями, обнаружение которых обходится реже и требует больших затрат.

Вместо этого хакерские группы ждут выпуска PoC или патча, а затем используют эту информацию для создания своих собственных эксплойтов.

Стать более эффективным

В настоящее время хакерские группы оптимизируют свою членскую структуру и предоставляют каждому человеку определенные функциональные роли.

В современных операциях по борьбе с киберпреступностью больше нет необходимости в авторах и тестерах вредоносных программ, потому что участники получают свои инструменты из центральных точек продаж в темной сети.

Более того, поскольку большая часть украденных денег переводится в криптовалюту, участникам нужны только денежные мулы или кто-то, кто будет управлять операциями по снятию наличных при обналичивании в фиатной валюте.

То же самое касается учетных данных, доступа через веб-интерфейс к различным организациям и даже DDoS-атак. Все это покупается у провайдеров, а не «нанимает» эксперта в команду.

Еще один способ оптимизации для киберпреступников сегодня - обратиться к поставщикам облачных услуг вместо того, чтобы выбирать более дорогостоящий и рискованный вариант аренды или создания собственной инфраструктуры физических серверов.

Обратной стороной этого является то, что облачные серверы регулируются, а поставщики услуг реагируют на отчеты, но злоумышленники всегда могут переключиться на другие платформы или создать новые учетные записи, когда они обнаружены.

Одно из самых ярких различий, которое мы видим сегодня, по сравнению с практикой киберпреступности пятилетней давности заключается в том, что крупные банки больше не являются объектом решительных атак.

Вместо этого хакеры поняли, что было бы намного проще и зачастую выгоднее атаковать компании с помощью программ-вымогателей, RAT и воров, перенаправляя платежи с помощью атак BEC или заставляя жертв платить выкуп.

«Еще в 2016 году мы в первую очередь сосредоточили внимание на крупных кибергангах, нацеленных на финансовые учреждения, особенно банки, -сказал Руслан Сабитов, эксперт по безопасности в «Лаборатории Касперского».

«В наши дни атакованные отрасли не ограничиваются финансовыми учреждениями, и крупные атаки, подобные тем, которые мы расследовали в прошлом, к счастью, больше невозможны. Но вряд ли можно сказать, что киберпреступности стало меньше. В прошлом году общее количество расследованных нами инцидентов составило около 200. Этот год еще не завершился, но подсчет уже составляет около 300 и продолжается».

По мере увеличения числа атак группы участников становятся более нестабильными и склонными к расформированию, поскольку сотрудничество теперь ограничивается финансовой выгодой и не более того.

Наконец, по мере того, как участники разбегаются и перемешиваются, то же самое происходит и с их методами, и с большим количеством групп, использующих аналогичные наборы инструментов, разделительные линии, которые помогали идентифицировать каждого действующего лица, стали размытыми». ***(Bill Toulas. Cybercrime matures as hackers are forced to work smarter // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/cybercrime-matures-as-hackers-are-forced-to-work-smarter/). 21.10.2021).***

***

«Группа хакеров, которую исследователи безопасности называют LightBasin, взламывает системы мобильной связи по всему миру в течение последних пяти лет.

С 2019 года группа взломала более десятка телекоммуникационных компаний и сохраняла настойчивость с помощью специального вредоносного ПО, чтобы украсть данные, которые будут использоваться разведывательными организациями.

Переход через сети GPRS

LightBasin активен по крайней мере с 2016 года и нацелен, в частности, на серверы Linux и Solaris, хотя он действительно взаимодействовал с системами Windows, где это необходимо, в их миссии по краже информации о подписчиках и метаданных вызовов.

В сегодняшнем отчете компания CrowdStrike, занимающаяся кибербезопасностью, сообщает, что злоумышленник представляет собой сложную группу со стратегией строгой операционной безопасности (OPSEC).

Исследователи собрали вместе активность LightBasin, начиная с инцидента, который они расследовали в одной телекоммуникационной компании. Они узнали, что злоумышленник будет перепрыгивать из одной взломанной сети в другую через SSH-соединение и «ранее установленные имплантаты».

Среди телекоммуникационных систем, на которые нацелен LightBasin, - серверы External DNS (eDNS), системы Service Delivery Platform (SDP) и

обеспечение SIM / IMEI, все из которых являются частью сети General Packet Radio Service (GPRS), которая обеспечивает роуминг между операторами мобильной связи.

В ходе расследования CrowdStrike обнаружил, что злоумышленник сначала получил доступ к серверу eDNS через SSH-соединение из сети другой скомпрометированной компании.

Исследователи обнаружили доказательства того, что LightBasin взламывает систему, пытаясь использовать учетные данные по умолчанию для целевой системы.

После успешного взлома злоумышленник установил и запустил специальное вредоносное ПО, которое в настоящее время отслеживается как SLAPSTICK - бэкдор для модуля аутентификации Solaris Pluggable Authentication Module (PAM), который предоставляет доступ к системе на основе жестко запрограммированного пароля.

Обладая бэкдорным доступом к целевой системе Solaris, LightBasin мог красть пароли для перехода к другим системам и обеспечивать постоянство с помощью того же метода.

Позже хакеры получили доступ к нескольким серверам eDNS от взломанной телефонной компании через имплант, который CrowdStrike назвал PingPong.

PingPong будет получать команды через запрос ICMP, чтобы установить обратную оболочку TCP на IP-адрес и порт, указанные в пакете…

Исследователи говорят, что они заметили обратные оболочки, созданные имплантатом PingPong, который через TCP-порт 53 (по умолчанию для DNS) общался с серверами других телекоммуникационных компаний в других частях мира.

Чтобы сохранить низкий профиль, LightBasin также добавил правила iptables к серверу eDNS, которые разрешили соединение SSH от пяти скомпрометированных компаний.

Кроме того, злоумышленник использовал троянизированную версию утилиты iptables, которая удаляла выходные данные, содержащие первые два октета, с IP-адресов, принадлежащих другим взломанным компаниям, что затрудняло администраторам поиск измененных правил.

Новый метод перемещения данных между сетями

CrowdStrikes отмечает, что LightBasin использует новую технику для перемещения трафика через телекоммуникационную сеть, которая включает специальную программную эмуляцию и использование TinyShell, распространенного бэкдора Unix с открытым исходным кодом.

Актер создал сценарий bash, который объединил бэкдор TinyShell и общедоступное программное обеспечение (sgsnemu2), которое имитирует точки доступа к сети GPRS - так называемые обслуживающие узлы поддержки GPRS (SGSN) - для перемещения трафика между сетями через определенные мобильные станции.

Хотя сценарий выполнялся в системе все время, он выполнял только определенные шаги в течение получасового окна каждый день, аналогично запланированной задаче.

Роль эмулятора SGSN заключалась в том, чтобы установить альтернативный маршрут связи, если TinyShell не удалось подключиться к IP-адресу управления и контроля (C2) через маршрут, добавленный в интерфейс tun0…

После успешного завершения этого шага TinyShell может использовать интерфейс tun0 для связи с сервером C2 актера. Если в конце 30-минутного окна не происходит успешного подключения, сценарий bash убивает и эмулятор SGSN, и имплант TinyShell.

В своем сегодняшнем отчете CrowdStrike также перечисляет набор утилит и вредоносных программ, которые LightBasin использует в своих операциях:

CordScan - утилита сетевого сканирования и захвата пакетов, которая может сканировать и извлекать информацию, специфичную для телекоммуникационных протоколов.

SIGTRANslator - двоичный файл ELF, который может отправлять и получать данные через протоколы связи (SIGTRAN).

Fast Reverse Proxy - инструмент обратного прокси с открытым исходным кодом

Microsocks Proxy - легкий прокси-сервер SOCKS5 с открытым исходным кодом

ProxyChains - инструмент с открытым исходным кодом, который связывает прокси и направляет сетевой трафик через цепочку.

LightBasin также известен как UNC1945 ив ноябре 2020 года был представлен компанией Mandiant, занимающейся кибербезопасностью, как субъект, скомпрометировавший поставщиков управляемых услуг (MSP) для достижения целей в области финансового и профессионального консалтинга.

Mandiant отмечает, что злоумышленник нацелился на системы Oracle Solaris и в своей деятельности полагался на эксплойты уязвимостей, инструменты и вредоносное ПО для нескольких операционных систем.

Исследователи заявили, что UNC1945 проявил «дисциплинированный интерес к прикрытию или манипулированию своей деятельностью, а также продемонстрировал передовые технические способности во время интерактивных операций».

Несмотря на то, что ни от Mandiant, ни от CrowdStrike нет никакой информации, последний нашел подсказку, предполагающую, что разработчик SIGTRANslator имеет некоторое знание китайского языка». ***(Ionut Ilascu. LightBasin hacking group breaches 13 global telecoms in two years // Bleeping Computer®(https://www.bleepingcomputer.com/news/security/lightbasin-hacking-group-breaches-13-global-telecoms-in-two-years/). 19.10.2021).***

***

Вірусне та інше шкідливе програмне забезпечення

«Специалисты предупредили о распространении инструмента для удаленного доступа (RAT) под видом обновления официального приложения SafeMoon.

При помощи вредоносной программы злоумышленники получают контроль над устройствами пользователей и могут похищать их пароли и деньги, сообщают специалисты международного разработчика антивирусного программного обеспечения - компании ESET.

С момента своего создания SafeMoon стал достаточно популярным, что вызвано продвижением инфлюенсерамы в социальных сетях. Не остались в стороне и киберпреступники, которые начали нацеливаться на пользователей криптовалюты.

В частности, мошенники присылают пользователям Discord сообщение от имени официального аккаунта SafeMoon, в котором сообщают якобы о новой версии приложения.

После перехода по ссылке в письме жертва попадает на ресурс, подобный официальному сайту SafeMoon. Домен, о котором впервые сообщил пользователь Reddit в августе 2021 года, также похож на легитимный, однако содержит дополнительную букву в конце. Таким образом злоумышленники пытались остаться незамеченными для большинства пользователей, которые спешат получить необходимое «обновление».

Все внешние ссылки на сайте являются легитимными, за исключением адреса для загрузки якобы официального приложения SafeMoon из магазина Google Play. Вместо SafeMoon для устройств Android загружается компонент с распространенным стандартным программным обеспечением Windows, которое можно использовать как в легитимных, так и в злонамеренных целях.

После выполнения инсталлятор загружает несколько файлов в систему, включая инструмент RAT под названием Remcos. Несмотря на то, что этот RAT позиционируется как легитимный инструмент, он также продается на подпольных форумах.

Стоит отметить, что Remcos был задействован во вредоносных кампаниях различных групп киберпреступников. В частности, только несколько месяцев назад исследователи ESET обнаружили его использование во время операции Spalax, целями которой были колумбийские организации.

Remcos позволяет злоумышленникам собирать конфиденциальные данные жертвы. Он может похищать учетные данные из разных браузеров, считывать нажатия клавиш, получать контроль над вебкамерой и звуком с микрофона жертвы. Также у инструмента есть возможность загружать и разворачивать дополнительные вредоносные программы на устройстве. Управление этим инструментом осуществляется через командный сервер (C&C), IP-адрес которого добавляется к загруженным файлам…». ***(Григорий Бондарь. Фейковое приложение для криптовалюты шпионит за пользователями // UNIAN.NET (https://www.unian.net/science/feykovoe-prilozhenie-dlya-kriptovalyuty-shpionit-za-polzovatelyami-novosti-11569552.html). 07.10.2021).***

***

«Эксперты обнаружили ранее неизвестное семейство вредоносных программ, которое использует модули, нацеленные на операционные системы Linux.

Об этом сообщают специалисты международного разработчика антивирусного программного обеспечения - компании ESET.

Сообщается, что модули, которые получили название FontOnLake, находятся в стадии разработки и обеспечивают удаленный доступ злоумышленникам, а также собирают учетные данные и выполняют роль прокси-сервера.

«Коварство инструментов FontOnLake в сочетании с усовершенствованным дизайном и низким уровнем распространения свидетельствует о том, что их применяли в целенаправленных атаках», - объясняет исследователь ESET Владислав Хрчка.

Семейство вредоносных программ для сбора данных или осуществления других вредоносных действий использует измененные легитимные бинарные файлы, которые настроены для загрузки других компонентов. Для избегания обнаружения FontOnLake всегда используется в сочетании с руткитом. Эти бинарные файлы, как правило, применяются в системах Linux и могут помогать оставаться незамеченными.

Исследователи ESET считают, что операторы FontOnLake очень осторожны, так как почти все выявленные образцы имели уникальные командные серверы(C&C) с различными нестандартными портами. Кроме этого, злоумышленники используют преимущественно C/C++ и различные сторонние библиотеки, такие как Boost, Poco и Protobuf.

Первый файл этого семейства вредоносных программ появился на VirusTotal (служба, осуществляющая анализ подозрительных файлов и ссылок, - УНИАН) в мае 2020 года, тогда как другие образцы загружались в течение года. Ни один из командных серверов из образцов, загруженных в VirusTotal, не был активным на момент написания новости. Это свидетельствует о том, что они могли быть отключены в связи с загрузкой. Расположение командного сервера и стран, из которых были загружены образцы в VirusTotal, могут свидетельствовать о том, что целью угрозы является Юго-Восточная Азия.

«Компании или отдельные пользователи, которые хотят защитить свои рабочие станции или серверы Linux от этой угрозы, должны применять мощные многоуровневые решения, а также актуальную версию дистрибутива Linux, поскольку некоторые из обнаруженных образцов вредоносного программного обеспечения были разработаны специально для CentOS и Debian», - сказал Владислав Хрчка…». ***(Григорий Бондарь. Новое семейство вредоносных программ атакует пользователей Linux – исследование // UNIAN.NET (https://www.unian.net/science/novoe-semeystvo-vredonosnyh-programm-atakuet-polzovateley-linux-issledovanie-novosti-11569594.html). 07.10.2021).***

***

«Microsoft подробно описала необычную фишинговую кампанию, направленную на кражу паролей, в которой используется набор для фишинга, созданный с использованием фрагментов кода, скопированных из работы других хакеров.

«Фишинговый комплект» - это различное программное обеспечение или услуги, предназначенные для облегчения фишинговых атак. В этом случае набор

был назван Microsoft ZooToday после некоторого текста, используемого набором. Microsoft также назвала его «Franken-Phish», потому что он состоит из различных элементов, некоторые из которых доступны для продажи через публично доступных продавцов мошенничества или повторно используются и переупаковываются другими торговыми посредниками.

Microsoft сообщила, что TodayZoo использует домен WorkMail AwsApps [.] Com для перекачки электронной почты со ссылками на фишинговые страницы, имитирующие страницу входа в Microsoft 365.

Microsoft заявляет, что злоумышленники создают вредоносные учетные записи AWS WorkMail «в масштабе», но просто используют случайно сгенерированные доменные имена вместо имен, которые будут представлять законную компанию. Другими словами, это грубый фишинговый продукт, который, вероятно, имеет ограниченный бюджет, но достаточно большой, чтобы его можно было заметить.

Он привлек внимание Microsoft, потому что выдавал себя за бренд Microsoft и использовал технику, называемую «обфускация шрифта с нулевой точкой» - HTML-текст с нулевым размером шрифта в электронном письме - чтобы избежать обнаружения человеком. В июле Microsoft обнаружилавсплеск атак с нулевым шрифтом.

Кампании TodayZoo в апреле и мае этого года обычно выдавали себя за страницы входа в Microsoft 365 и запрос на сброс пароля.Тем не мение. Microsoft обнаружила, что в августовских кампаниях использовались уведомления о факсах и сканерах под брендом Xerox, чтобы заставить рабочих отказаться от учетных данных.

Исследователи угроз Microsoft обнаружили, что большинство фишинговых целевых страниц размещались внутри облачного провайдера DigitalOcean. Эти страницы были идентичны странице входа в Microsoft 365.

Еще одна необычная особенность заключалась в том, что после сбора учетных данных украденная информация не пересылалась на другие учетные записи электронной почты, а сохранялась на самом сайте. Такое поведение было характерно для фишингового набора TodayZoo, который ранее был ориентирован на фишинговые учетные данные из учетных записей видеовстреч Zoom.

Но исследователи Microsoft считают, что эта фишинговая группа представляет собой единичную операцию, а не сеть агентов.

«Хотя многие фишинговые комплекты связаны с широким спектром шаблонов почтовых кампаний, и, наоборот, многие шаблоны почтовых кампаний связаны со многими фишинговыми наборами, на страницах TodayZoo использовались исключительно те же шаблоны почтовых кампаний, а в любых из этих последующих почтовых кампаний - только появились наборы TodayZoo. Это наводит нас на мысль, что лица, стоящие за этой конкретной реализацией TodayZoo, действуют сами по себе », - заявила Microsoft.

Microsoft заявляет, что проинформировала Amazon о фишинговой кампании TodayZoo и что AWS «незамедлительно приняла меры».***(Liam Tung. This monster of a phishing campaign is after your passwords // ZDNet***

(https://www.zdnet.com/article/this-frankensteins-monster-of-a-phishing-campaign-is-after-your-passwords/). 22.10.2021).

***

«По данным поставщика сети безопасности и доставки контента Akamai, более 25% вредоносного кода JavaScript запутывается так называемыми «упаковщиками» - методом упаковки программного обеспечения, который дает злоумышленникам возможность избежать обнаружения на основе сигнатур.

Упаковщики работают, сжимая или шифруя код, чтобы сделать этот код нечитаемым и не поддающимся отладке, в результате чего получается «запутанный» код, который трудно обнаружить антивирусу.

Упаковщики JavaScript - не новая угроза.Как отмечалось в Secureworks еще в 2008 году, упаковщики JavaScript стали популярной альтернативой библиотекам JavaScript, поскольку они хорошо уменьшали количество байтов, загружаемых на каждую страницу, чтобы поддерживать более богатые веб-приложения того времени.

«Компьютерные хакеры воспользовались признанием этих упаковщиков как неоптимальной тактики оптимизации сети и используют их как способ обойти меры безопасности на шлюзе и на хосте», -отметила тогда SecureWorks.

Akamai отмечает, что некоторые из самых популярных веб-сайтов в мире содержат обфусцированный JavaScript по бизнес-причинам.

Компания подчеркивает, что упаковщики по-прежнему представляют собой крупномасштабную проблему, способствуя распространению фишинговых страниц, вредоносных программ-дропперов и мошенничества, такогокак атаки Magecart на системы онлайн-платежей. На конференции SecTor 2021 в ноябре исследователи представят новую «технику, которая профилирует уникальную функциональность упаковщиков для обнаружения JavaScript до того, как он будет запутан, независимо от исходного кода».

По словам Акамая, вместо подписи или хэша код JavaScript обнаруживается методами, которые использует упаковщик.

Чтобы показать, как он профилирует упаковщики, Akamai рассмотрел четыре фрагмента кода JavaScript из четырех несвязанных вредоносных файлов.Два фрагмента были предназначены для фишинга, один был вредоносным ПО, а четвертый - мошенником Magecart.

«Эти четыре примера являются результатом той же уникальной функции упаковщика, которая используется для обфускации любого заданного кода JavaScript», - объясняет Акамай.

«Путем профилирования упаковщиков и их функций мы оценили 30 000 доброкачественных и вредоносных файлов JavaScript и смогли увидеть, что по крайней мере 25% вредоносных файлов использовали одну из пяти функций профилированного упаковщика».

Исследование также показало, что 0,5% безопасных файлов с 20 000 самых популярных веб-сайтов на Alexa.com использовали методы обфускации упаковщика.Затем Акамай утверждает, что обфускация не является достаточно

сильным сигналом для вредоносного кода, и предполагает, что для обнаружения потребуется машинное обучение, чтобы различать вредоносный и доброкачественный запутанный код JavaScript».***(Liam Tung. Hackers are disguising their malicious JavaScript code with a hard-to-beat trick // ZDNet (https://www.zdnet.com/article/hackers-are-disguising-their-malicious-javascript-code-with-hard-to-beat-trick/). 20.10.2021).***

***

«Киберпреступная группа TA505 возобновляет работу своего финансового оборудования для грабежа, распространяя вредоносное ПО в ряде отраслей, что изначально было маломасштабным волнами, которые, по наблюдениям исследователей, резко усилились в конце прошлого месяца.

«Они делают плохие вещи, но они настолько сложны, что отслеживать их - очень весело», - сказал Шеррод Де Гриппо, вице-президент по исследованию и обнаружению угроз в Proofpoint.

«Отслеживание TA505 - одно из маленьких удовольствий жизни, - признала она. «Они первопроходцы в мире киберпреступности, регулярно меняя [тактику, методы и процедуры, или ТТП]».

TA505, также известная как Hive0065, - это банда киберпреступников, причастная как к финансовым махинациям, так и к действиям, спонсируемым государством. Исследователи Proofpoint описывают эту группу как «одного из наиболее плодовитых участников», за которыми они следят.

Он стоит за крупнейшими спам-кампаниями, которые когда-либо видела фирма, а именно за распространением банковского трояна Dridex. Proofpoint также отслеживает банду, распространяющую программы-вымогатели Locky и Jaff, банковский троян Tricki другие «в очень больших объемах», - сообщает Proofpoint.

TA505, активно нацеленная на множество отраслей, включая финансы, розничную торговлю и рестораны, действует по крайней мере с 2014 года. Она известна частой сменой вредоносных программ и движущей силой глобальных тенденций в распространении криминального вредоносного ПО.

Самая последняя серия кампаний напоминает активность TA505 в 2019 и 2020 годах, но «в ней нет недостатка в некоторых интригующих новых элементах», - сказал Де Гриппо, включая усовершенствованные инструменты и экзотические языки. «Помимо обновления [трояна удаленного доступа FlawedGrace, или RAT], они также переработали свои промежуточные этапы загрузки, заменив надежный Get2 несколькими новыми загрузчиками, написанными на необычных языках сценариев», - отметила она.

Переоборудование для повторной атаки

Как и следовало ожидать, последние кампании банды охватывают широкий спектр отраслей. Они также показ новой передачи, втом числе модернизированной KiXtart погрузчика, погрузчика MirrorBlast что загружает Rebol скрипт stagers, тем переоборудовано FlawedGraceRAT и обновленные вредоносные вложения Excel.

В анализе, опубликованном во вторник, Proofpoint сказал, что его исследователи отслеживают возобновленные кампании вредоносных программ с TA505, которые медленно начинались в начале сентября - всего с несколькими

тысячами электронных писем на волну, распространяя вредоносные вложения Excel - а затем увеличили объем позже. в месяц, что привело к появлению от десятков до сотен тысяч писем к концу сентября.

Многие из кампаний, особенно более масштабные, «сильно напоминают» то, чем занималась банда в период с 2019 по 2020 год, включая аналогичные соглашения об именах доменов, приманки для электронной почты, приманки для файлов Excel и доставку FlawedGrace RAT, согласно рецензии. Во время волны атак по электронной почте в начале сентября TA505 использовал более специфические приманки, которые не затронули столько же отраслей, как недавние кампании октября 2021 года, заявленные исследователями Proofpoint.

«Примеры приманок включали юридические темы, публикации в СМИ, отчеты о ситуации и заявления о вреде для здоровья», - говорится в анализе.

К тому времени, когда кампании набрали обороты в конце сентября - начале октября, TA505 нацелилась на большее количество отраслей, и банда начала использовать кампании электронной почты как на основе URL-адресов, так и на основе вложений.

TA505 также начал разветвляться: изначально мошенники нацеливались преимущественно на цели в Северной Америке, такие как США и Канада, но в конечном итоге начали преследовать немецкоязычные страны, включая Германию и Австрию, по мере того, как кампании набирали обороты.

Среди заслуживающих внимания новых разработок - обновленная версия FlawedGrace RAT, а также переработанные промежуточные этапы загрузчика, написанные в Rebol и KiXtart, которые. По словам исследователей, банда использует вместо популярного ранее загрузчика Get2. «Новые загрузчики выполняют аналогичные функции разведки и вытягивания на следующих этапах», - отметили исследователи Proofpoint.

Фирма предоставила снимок экрана, показанный ниже, одного из электронных писем от недавней кампании (28 сентября).

«Электронные письма содержали вложение Excel, которое при открытии и включении макросов приводило к загрузке и запуску файла MSI», - сказал Proofpoint. Файлы MSI используются для установки программного обеспечения в системе Windows. «Файл MSI, в свою очередь, будет запускать встроенный загрузчик Rebol, дублированный Proofpoint как MirrorBlast».

Proofpoint также предоставил снимок экрана приложения Excel со страховым возмещением, показанный ниже, который также был частью кампании от 28 сентября.

В более поздней кампании - от 13 октября - банда начала злоупотреблять брендингом Microsoft и OneDrive на своей целевой странице.

Новый TTP: промежуточные загрузчики на экзотических языках

Исследователи отметили, что TA505 теперь использует несколько промежуточных загрузчиков до доставки FlawedGrace RAT, и они написаны на необычных языках сценариев - Rebol и KiXtart.

Однако чем больше вещей меняется, тем больше они остаются прежними: промежуточные загрузчики, по-видимому, служат той же цели, что и Get2 -

загрузчик, который TA505 использует с 2019 года для доставки множества вторичных полезных нагрузок, говорят исследователи.

«Загрузчики выполняют минимальную разведку зараженной машины, такую как сбор информации о пользовательском домене и имени пользователя, и загружают дополнительные полезные данные», - говорится в описании.

Вредоносные программы видоизменяются, но следы остаются

Proofpoint обнаружил сходство между текущими и более ранними кампаниями TA505. Во-первых, поддельные логотипы Microsoft в виде листов Excel оставались идентичными со времени кампании 2 сентября 2020 г. той, которая использовалась в кампании 6 октября 2021 г., как показано на рисунке ниже.

Другие параллели включают соглашения об именах доменов и повторное использование кода, которые исследователи Proofpoint обнаружили в некоторых частях цепочки доставки, например, в нескольких частях целевой страницы.

Макросы на победу

Невидимые жертвы должны включить макросы после открытия вредоносных файлов Excel, чтобы создатели вредоносных программ выиграли дело.«Код, ответственный за загрузку MSI-файла следующего этапа, обычно слегка запутывался с помощью символов-заполнителей, реверсирования строк или аналогичных простых функций и спрятан в комментариях документа, заголовке, в ячейке или других местах», - отмечается в анализе.

Ожидайте большего

Учитывая, что TA505 изменяет TTP и что они «считаются законодателями мод в мире киберпреступности», Proofpoint не ожидает, что они исчезнут в ближайшее время. «Этот злоумышленник не ограничивает свой набор целей и, по сути, является равным оппортунистом с географическими и вертикальными направлениями, которые он выбирает для атаки», - отмечают аналитики. «Это в сочетании со способностью TA505 быть гибким, сосредотачиваясь на том, что является наиболее прибыльным, и при необходимости меняя свои ДТС, делают актора постоянной угрозой».

Они предсказали, что будущее, вероятно, будет содержать еще больше новинок от постоянно меняющихся обманщиков, говорят исследователи Proofpoint: «[Мы] ожидаем, что TA505 будет продолжать корректировать свои операции и методы всегда с прицелом на финансовую выгоду. Использование промежуточных загрузчиков в цепочке атак также может стать более долгосрочной техникой, которую использует злоумышленник». ***(Lisa Vaas. TA505 Gang Is Back With Newly Polished FlawedGrace RAT// Threatpost (https://threatpost.com/ta505-retooled-flawedgrace-rat/175559/). 19.10.2021).***

***

«Исследователи предупреждают, что было обнаружено редкое вредоносное ПО для буткитов Windows UEFI, предлагающее злоумышленникам путь к кибершпионажу.

Согласно ESET, цель буткита - установить на целевой компьютер полнофункциональный бэкдор, который «поддерживает богатый набор команд и

содержит различные возможности автоматической кражи данных, включая кражу документов, ведение кейлоггеров и мониторинг экрана жертвы путем периодического создания снимков экрана.»

Безопасность при запуске начинает работать

UEFI (Unified Extensible Firmware Interface) - это встроенный компонент микропрограмм в вычислительных микросхемах, отвечающий за безопасность вычислительной среды при запуске и загрузке операционной системы. Таким образом, это идеальное место для размещения вредоносных программ, чтобы обеспечить их постоянство, поскольку UEFI загружается независимо от того, какие изменения или перезапускает ОС.

Новый вредоносный буткит, который исследователи ESET назвали ESPecter, базируется на части встроенной технологии EFI System Partition (ESP). ESP содержит загрузчики или образы ядра, которые UEFI использует для запуска установленных ОС и различных утилит во время загрузки.

«Злоумышленники [таким образом] достигают выполнения на ранних стадиях процесса загрузки системы, до того, как операционная система будет полностью загружена», - говорится в анализе ESETESPecter, опубликованном во вторник. «Это позволяет ESPecter обходить принудительное использование подписи драйверов Windows (DSE) для выполнения собственного неподписанного драйвера при запуске системы».

Исследователи отметили, что затем этот драйвер внедряет другие компоненты пользовательского режима в определенные системные процессы; а те, в свою очередь, используются для подключения к серверу управления и контроля (C2). После того, как это соединение установлено, злоумышленники могут начать загрузку и запуск дополнительных вредоносных программ или выполнение различных команд, чтобы получить полный контроль над машиной.

Интересно, что технический анализ ESPecter, проведенный ESET, показывает, что его начало восходит к 2012 году и использует модификацию основной загрузочной записи (MBR) в качестве метода сохранения. Но разработка в значительной степени бездействовала: с тех пор, по словам исследователей, до прошлого года в код вносились лишь «незначительные изменения». Именно тогда его операторы переместили вредоносное ПО с устаревших систем BIOS на современные системы UEFI.

Взгляд на реализацию ESPecter

Исследователи еще не уверены, как он распространяется, но как только ESPecter попадает на ПК, он начинает заражение UEFI, изменяя законный двоичный файл Windows Boot Manager. Согласно ESET, этот двоичный файл (bootmgfw.efi) находится на ESP.

«Чтобы успешно отбросить вредоносную полезную нагрузку, ESPecter необходимо изменить диспетчер загрузки, чтобы обойти проверки целостности [которые предотвращают выполнение мошеннических элементов буткита]», - отмечают исследователи.

Диспетчер загрузки отвечает за поиск установленной ОС в ESP и передачу задачи выполнения для этой ОС загрузчику ядра. Затем этот загрузчик ядра ОС загружает и выполняет следующий компонент в цепочке загрузки - само ядро

Windows, которое содержит упомянутую ранее проверку безопасности Linchpin DSE.

Чтобы обойти проверки целостности и обеспечить постоянство во время процесса запуска, ESPecter ищет байтовые шаблоны, которые идентифицируют различные процессы проверки, а затем просто исправляет их. Например, «ESPecter ищет в памяти BmFwVerifySelfIntegrity с использованием различных байтовых шаблонов и изменяет эту функцию таким образом, что она всегда возвращает ноль, указывая на то, что проверка прошла успешно», - пояснили исследователи.

ESPecter также вставляет обход для функции, ответственной за вышеупомянутую передачу выполнения ядру ОС.Это позволяет ему «исправлять ядро Windows в памяти после его загрузки, но до его выполнения», согласно записи. «Последний этап загрузочного кода буткита отвечает за отключение DSE путем исправления функции ядра SepInitializeCodeIntegrity».

Затем он может легко запустить драйвер, который запускает остальную часть процесса ESPecter.

ESPecter: склонный к шпионажу

Согласно ESET, основная цель драйвера - загрузить две разные полезные нагрузки пользовательского режима (WinSys.dll и Client.dll) и настроить кейлоггер, который перехватывает все действия с клавиатуры. После этого он удаляется.

Полезная нагрузка WinSys.dll периодически опрашивает сервер C2 (он находит его адрес в файле конфигурации вредоносной программы) для загрузки дополнительных вредоносных программ или выполнения простых команд. C2 может попросить его загрузить системную информацию (имя процессора, версия ОС, размер памяти, MAC-адрес Ethernet, список установленного программного обеспечения и т.д.). Получить и выполнить новые файлы, перезагрузить компьютер или загрузить новую конфигурацию.

Client.dll - это более полнофункциональная полезная нагрузка, которая, по словам ESET, действует как многофункциональный бэкдор. Он устанавливает свой собственный зашифрованный канал связи с C2, после чего ожидает одной из следующих команд:

Остановите бэкдор.

Выполнить командную строку, полученную от C2, и захватить вывод с помощью каналов.

Выполнение команд питания: выход из системы, выключение, перезагрузка или выключение.

Сделайте снимок экрана переднего плана, полный снимок экрана или измените параметры автоматического снимка экрана, в зависимости от значения параметра.

Выполнять различные операции с файловой системой.

Загрузите собранные данные и файлы.

Выполнять различные служебные команды.

Выполнять различные команды, связанные с процессом.

Измените значения конфигурации.

Остановить / запустить кейлоггер.

Отмена защиты безопасной загрузки

Исследователи ESET заявили, что не знают, как конкретно распространяется ESPecter, но для первоначального компромисса вполне вероятно, что он использует одну из различных уязвимостей прошивки UEFI, которые позволяют отключить или обойти безопасную загрузку.

Безопасная загрузка - это стандарт безопасности для ПК, использующий UEFI, который гарантирует, что устройства загружаются с использованием только надежного программного обеспечения. Исследователи ESET отметили, что для большинства компьютеров это основной барьер для взлома на уровне запуска, и для успешной загрузки с модифицированным диспетчером загрузки его необходимо отключить.

«Хотя безопасная загрузка стоит на пути выполнения ненадежных двоичных файлов UEFI из ESP, за последние несколько лет мы стали свидетелями различных [способов решения этой проблемы]», - говорится в анализе. «Это показывает, что защита прошивки UEFI - сложная задача, и то, как различные поставщики применяют политики безопасности и используют сервисы UEFI, не всегда идеально».

Согласно анализу, помимо использования уязвимости, другие возможные сценарии обхода безопасной загрузки включают следующие:

Злоумышленник имеет физический доступ к устройству (исторически известный как атака «злая горничная») и вручную отключает безопасную загрузку в меню настройки BIOS.ESET отмечает, что часто меню конфигурации микропрограмм по-прежнему обозначается и называется «меню настройки BIOS», даже в системах с UEFI.

Безопасная загрузка уже была отключена на скомпрометированной машине (например, пользователь может выполнить двойную загрузку Windows и других ОС, не поддерживающих безопасную загрузку).

Первой версией Windows, поддерживающей безопасную загрузку, была Windows 8, поэтому машины, на которых были запущены все предыдущие версии, уязвимы для атаки.

Таким образом, своевременное обновление и правильная настройка компьютеров может помочь предотвратить атаку ESPecter.

Буткиты: редкая находка

Вредоносные буткиты редко можно найти в природе, отмечает ESET: «до ESPecter было обнаружено только три реальных случая вредоносного ПО UEFI».

Первым был LoJax, обнаруженный ESET в 2018 году. Предполагается, что он использовался российской расширенной постоянной угрозой (APT), известной как APT28 (также известной как Fancy Bear или Sofacy), LoJax представляет собой модифицированную версию программного обеспечения для восстановления LoJack от Absolute Software для ноутбуков. LoJack скрывается за системным UEFI и незаметно сообщает владельцу о его местонахождении для возможного физического восстановления ноутбука. К сожалению, уязвимая версия 2009 года содержала несколько ключевых ошибок, главная из которых - модуль конфигурации, который был плохо защищен с помощью слабого шифрования, которым злоумышленники воспользовались, чтобы превратить его в оружие.

Затем был MosaicRegressor, обнаруженный «Лабораторией Касперского» в 2019 году. Он был замечен в дикой природе, нацелен на дипломатов и членов неправительственных организаций (НПО) из Африки, Азии и Европы по электронной почте. Все цели были связаны с Северной Кореей. MosaicRegressor основана на специальной версии просочилась исходного кода VectorEDK буткитом HackingTeam, согласно анализу в то время.

Третий - это новая версия набора для наблюдения FinSpy, обнаруженная «Касперским» на прошлой неделе, в которой есть модуль, который также компрометирует диспетчер загрузки Windows UEFI.

Несмотря на то, что полноценных буткитов очень мало, «в последние несколько лет мы видели контрольные примеры буткитов UEFI (DreamBoot, EfiGuard), утечку документов (DerStarke, QuarkMatter) и даже утечку исходного кода (Hacking Team Vector EDK)», - утверждают исследователи ESET.

Они добавили, что обязательно появятся новые буткиты: «Неудивительно, что такая широко распространенная технология [как UEFI] также стала заманчивой целью для злоумышленников в их стремлении к максимальной устойчивости», - заявили они.

Threatpost обратился в ESET за подробностями о жертвах кампании и другими подробностями об атаках». ***(Tara Seals. ESPecter Bootkit Malware Haunts Victims with Persistent Espionage// Threatpost(https://threatpost.com/especter-bootkit-malware-espionage/175366/). 06.10.2021).***

***

«Новая вредоносная угроза под названием Squirrelwaffle появилась в дикой природе, помогая субъектам получить начальную точку опоры и способ перенести вредоносное ПО на скомпрометированные системы и сети.

Новый вредоносный инструмент распространяется через спам-кампании, отбрасывая Qakbot и Cobalt Strike в последних кампаниях.

Обнаруженный исследователями Cisco Talos, Squirrelwaffle является одним из инструментов, который появился на замену Emotet вскоре после нарушения правоохранительными органами широко используемого ботнета.

Эта новая угроза впервые появилась в сентябре 2021 года, а пик объемов распространения пришелся на конец того же месяца. В то время как спам-кампания в основном использует рассылку украденных электронных писем с цепочкой ответов на английском языке, злоумышленники также используют французские, немецкие, голландские и польские электронные письма.

Эти электронные письма содержат гиперссылки на вредоносные ZIP-архивы, размещенные на веб-серверах, контролируемых злоумышленниками, и обычно включают вредоносный.doc или.xls-вложение, которое запускает вредоносный код при открытии.

В нескольких документах, отобранных и проанализированных исследователями Talos, участники используют платформу для подписи DocuSign в качестве приманки, чтобы обманом заставить получателей включить макросы в их пакете MS Office.

Содержащийся код использует реверс строки для обфускации, записывает сценарий VBS в% PROGRAMDATA% и выполняет его.

Это действие извлекает Squirrelwaffle из одного из пяти жестко заданных URL-адресов, доставляя его в виде файла DLL в скомпрометированную систему.

Затем загрузчик Squirrelwaffle развертывает вредоносное ПО, такое как Qakbot или широко используемый инструмент тестирования на проникновение Cobalt Strike.

Cobalt Strike - это законный инструмент для тестирования на проникновение, разработанный как инфраструктура атаки для тестирования инфраструктуры организации с целью обнаружения пробелов и уязвимостей в системе безопасности.

Однако взломанные версии Cobalt Strike также используются злоумышленниками (обычно используются во время атак программ-вымогателей) для задач после эксплуатации после развертывания маяков, которые обеспечивают им постоянный удаленный доступ к скомпрометированным устройствам.

Squirrelwaffle также имеет черный список IP-адресов, который заполняется известными исследовательскими фирмами в области безопасности, чтобы избежать обнаружения и анализа.

Все коммуникации между Squirrelwaffle и инфраструктурой C2 зашифрованы (XOR + Base64) и отправляются через запросы HTTP POST.

Злоумышленники используют ранее скомпрометированные веб-серверы для поддержки аспекта распространения файлов в своих операциях, причем большинство из этих сайтов работают под управлением WordPress 5.8.1.

На этих серверах злоумышленники развертывают сценарии «антибот», которые помогают предотвратить обнаружение и анализ «белой шляпы».

Другие авторитетные участники использовали несколько методов, описанных в отчете Cisco Talos в прошлом.

Таким образом, Squirrelwaffle может быть перезагрузкой Emotet участниками, которые уклонились от правоохранительных органов или других злоумышленников, пытающихся заполнить пустоту, оставленную печально известным вредоносным ПО…». ***(Bill Toulas. Spammers use Squirrelwaffle malware to drop Cobalt Strike // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/spammers-use-squirrelwaffle-malware-to-drop-cobalt-strike/). 26.10.2021).***

***

«Ботнет PurpleFox обновил свой арсенал новыми эксплойтами уязвимостей и сбросил полезную нагрузку, теперь также используя WebSockets для двунаправленной связи C2.

Хотя ботнет PurpleFoxв основном базируется в Китае, он все еще присутствует во всем мире через сотни взломанных серверов.

го действие начинается с выполнения команды PowerShell, которая загружает вредоносные полезные данные с указанного URL-адреса, указывая на доступный сервер C2.

Полезная нагрузка, используемая в недавних кампаниях, отслеживаемых исследователями Trend Micro, представляет собой длинный сценарий, состоящий из трех компонентов повышения привилегий.

Они нацелены на системы от Windows 7 до Windows 10, но ограничены только 64-битными системами.

Последние версии PurpleFox используют следующие недостатки:

Windows 7 / Windows Server 2008 - CVE-2020-1054, CVE-2019-0808

Windows 8 / Windows Server 2012 - CVE-2019-1458

Windows 10 / Windows Server 2019 - CVE-2021-1732

PurpleFox обнаруживает хост-систему, выбирает соответствующий эксплойт, а затем использует модуль PowerSploit для его загрузки.

Пакет MSI также запускается процессом на уровне администратора без какого-либо взаимодействия с пользователем, проверяя наличие старых установок PurpleFox и заменяя их компоненты новыми.

Бэкдор, установленный в хост-системе, представляет собой файл DLL, запутанный с помощью утилиты сжатия файлов VMProtect.

Вредоносная программа также использует драйвер руткита, который скрывает свои файлы, ключи реестра и процессы, снижая вероятность обнаружения на взломанном сервере.

Открытие канала WebSocket и поддержание его активности

Новый бэкдор.NET, полученный из недавних кампаний, отключается через несколько дней после первоначального вторжения, чтобы использовать WebSockets для связи C2.

Этот компонент отвечает за настройку конфигурации связи, а также за инициализацию криптографических функций.

Использование WebSockets для связи является чем-то необычным в сфере вредоносных программ, но PurpleFox показывает, что, тем не менее, это может быть очень эффективным.

Обмен сообщениями между зараженной машиной и выбранным сервером C2 начинается с согласования сеансового ключа шифрования RSA, но даже этот первый обмен шифруется AES с использованием ключа по умолчанию.

Отправляя «keepalive» сообщения, TCP-соединение поддерживается столько, сколько необходимо.

Список команд WebSocket, наблюдаемых TrendMicro, обширен, и, хотя между различными вариантами есть некоторые расхождения...

В настоящее время PurpleFox все еще активен, и существует значительное количество серверов C&C, управляющих клиентами WebSocket.

Проведя профилирование целей, TrendMicro сообщает, что наиболее заметные очаги активности находятся в США, Турции, ОАЭ, Ираке и Саудовской Аравии». ***(Bill Toulas. New PurpleFox botnet variant uses WebSockets for C2 communication // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-purplefox-botnet-variant-uses-websockets-for-c2-communication/). 20.10.2021).***

***

«Исследование, в ходе которого было проанализировано более 10 000 образцов разнообразного вредоносного ПО, написанного на JavaScript, показало, что примерно 26% из них зашифрованы, чтобы избежать обнаружения и анализа.

Обфускация - это когда простой для понимания исходный код преобразуется в трудный для понимания и запутанный код, который по-прежнему работает так, как задумано.

Злоумышленники обычно используют обфускацию, чтобы затруднить анализ вредоносных сценариев и обход программного обеспечения безопасности.

Обфускация может быть достигнута с помощью различных средств, таких как внедрение неиспользуемого кода в сценарий, разделение и объединение кода (разбиение его на несвязанные фрагменты) или использование шестнадцатеричных шаблонов и сложных совпадений с именами функций и переменных.

Обфускация на подъеме

Исследователи Akamai проанализировали 10000 образцов JavaScript, включая вредоносные программы, фишинговые страницы, инструменты мошенничества, фрагменты Magecart, криптомайнеры и т.д.

По крайней мере, 26% из них используют ту или иную форму обфускации, чтобы избежать обнаружения, что указывает на рост использования этого базового, но эффективного метода.

Большинство этих обфусцированных образцов имеют похожий код, потому что они были объединены одними и теми же упаковщиками, поэтому их структура кода выглядит похожей, даже если функция отличается.

Akamai планирует представить более подробную информацию о том, как они фокусируют свои усилия по обнаружению на методах упаковки, а не на самом коде файла, на предстоящей конференции SecTor.

Доброкачественные сайты также используют его

Но не всякая обфускация злонамеренна или коварна. Как поясняется в отчете, около 0,5% из 20 000 веб-сайтов с самым высоким рейтингом (по данным Alexa) также используют методы обфускации.

Эти случаи можно отнести к следующим:

Веб-сайты пытаются скрыть от конкурентов некоторые функции своего клиентского кода.

Фрагменты JavaScript, которые они используют, были запутаны сторонним провайдером.

Конфиденциальная информация, такая как адреса электронной почты, должна быть скрыта от всеобщего обозрения.

Таким образом, обнаружения вредоносного кода на основе того факта, что он запутан, недостаточно, и необходимо провести дальнейшую корреляцию с вредоносными функциями.

Именно это смешение с легитимным развертыванием затрудняет обнаружение рискованного кода и является причиной того, что обфускация становится настолько распространенной в среде угроз». ***(Bill Toulas. About 26% of all malicious JavaScript threats are obfuscated // Bleeping Computer®***

(https://www.bleepingcomputer.com/news/security/about-26-percent-of-all-malicious-javascript-threats-are-obfuscated/). 19.10.2021).

***

«Ранее неизвестный спонсируемый государством субъект развертывает новый набор инструментов для атак, направленных на поставщиков телекоммуникационных услуг и ИТ-компании в Южной Азии.

Цель группы, которую исследователи Symantec называют Harvester, - это сбор разведданных в рамках целенаправленных шпионских кампаний с упором на ИТ, телекоммуникации и государственные учреждения.

Вредоносные инструменты Harvester ранее не встречались в дикой природе, что указывает на то, что это злоумышленник, не связанный с известными противниками.

«Группа Harvester использует как пользовательские вредоносные программы, так и общедоступные инструменты в своих атаках, которые начались в июне 2021 года, а самая последняя активность наблюдалась в октябре 2021 года. Целевые секторы включают телекоммуникации, правительство и информационные технологии (ИТ)», -заявили исследователи Symantec.

«Возможности инструментов, их индивидуальная разработка и жертвы предполагают, что Harvester является актером, поддерживаемым государством».

Вот краткое изложение инструментов, используемых операторами комбайнов в своих атаках:

Backdoor.Graphon - настраиваемый бэкдор, использующий инфраструктуру Microsoft для своей C&C деятельности.

Custom Downloader - использует инфраструктуру Microsoft для своей деятельности C&C.

Custom Screenshotter - периодически записывает скриншоты в файл.

Cobalt Strike Beacon - использует инфраструктуру CloudFront для своей деятельности C&C (Cobalt Strike - это готовый инструмент, который можно использовать для выполнения команд, внедрения других процессов, повышения уровня текущих процессов или имитации других процессов, а также загрузки и скачивания файлов)

Metasploit - готовая модульная структура, которую можно использовать для различных злонамеренных целей на машинах-жертвах, включая повышение привилегий, захват экрана, настройку постоянного бэкдора и многое другое.

Умные трюки и безопасные соединения

Хотя аналитики Symantec не смогли определить первоначальный вектор заражения, есть некоторые свидетельства того, что для этой цели использовался вредоносный URL-адрес.

Graphon предоставляет участникам удаленный доступ к сети и маскирует свое присутствие, смешивая коммуникационную активность командного управления (C2) с легитимным сетевым трафиком из CloudFront и инфраструктуры Microsoft.

Интересный момент обнаружен в том, как работает пользовательский загрузчик, создавая необходимые файлы в системе, добавляя значение реестра для

новой точки загрузки и, в конечном итоге, открывая встроенный веб-браузер по адресу hxxps: // usedust [.] Com.

Хотя это выглядит как точка, откуда берется Backdoor. Graphon, субъекты просто используют URL-адрес как приманку, чтобы ввести в заблуждение.

Пользовательский инструмент для создания снимков экрана снимает фотографии с рабочего стола и сохраняет их в защищенном паролем ZIP-архиве, который пересылается через Graphon. Каждый ZIP-файл хранится в течение недели, поэтому все, что старше этого, автоматически удаляется.

Symantec предупреждает, что Harvester по-прежнему активен, в настоящее время в основном нацелившись на организации в Афганистане.

Несмотря на то, что исследователи смогли опробовать инструменты новой группы, у них пока нет достаточных доказательств, чтобы приписать эту деятельность конкретной стране». ***(Bill Toulas. State-backed hackers breach telcos with custom malware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/state-backed-hackers-breach-telcos-with-custom-malware/). 18.10.2021).***

***

«В отчете Amnesty International индийская компания, занимающаяся кибербезопасностью, связывает со шпионской программой Android, которая используется для нацеливания на известных активистов.

Расследование проводится командой Amnesty International, которая подтвердила случай шпионажа против тоголезского активиста, а также заметила признаки развертывания шпионского ПО в нескольких ключевых регионах Азии.

Ссылка на индийскую фирму по кибербезопасности

Согласно Amnesty International, шпионское ПО для Android было связано с индийской компанией Innefu Labs, занимающейся кибербезопасностью, после того, как IP-адрес, принадлежащий компании, неоднократно использовался для распространения полезной нагрузки шпионского ПО.

Однако фактическое развертывание может быть результатом работы «Donot Team» (APT-C-35), коллектива индийских хакеров, которые атакуют правительства в Юго-Восточной Азии как минимум с 2018 года.

Amnesty отмечает, что, возможно, Innefu не знает, как ее клиенты или третьи стороны используют ее инструменты. Однако внешний аудит может выявить все теперь, когда стали известны все технические подробности.

В письменном письме в Amnesty International, Innefu Labs отрицает свою причастность к команде Donot и преследованиям активистов.

«Вначале мы категорически отрицаем существование какой-либо связи между Innefu Labs и шпионскими инструментами, связанными с группой« Donot Team »и атаками на Защитника прав человека в Того. Как мы уже заявили в нашем предыдущем письме, мы не знаем о каких-либо «Донот-командах» и не имеем с ними никаких отношений.

В вашем письме от 20.09.2021 упоминается телефон Xiaomi Redmi 5A, который якобы получил доступ к IP-адресу Innefu Labs, а также какой-то другой частный VPN-сервер для доступа к украинской хостинговой компании под

названием Deltahost.Мы считаем, что этот телефон не принадлежит никому, связанному с Innefu Labs. Просто потому, что к нашему IP-адресу был осуществлен доступ с помощью этого телефона, ipso facto не делает вывод об участии Innefu Labs в какой-либо из предполагаемых действий », - Innefu Labs.

BleepingComputer несколько раз связывался с Innefu Labs со вчерашнего утра, но не получил ответа.

Ориентация на активистов Того

Атака на активистов началась с незапрашиваемого сообщения в WhatsApp, в котором предлагалось установить якобы защищенное приложение для чата под названием ChatLite.

Провалившись там, злоумышленники отправили электронное письмо из учетной записи Gmail, содержащее зашнурованный файл MS Word, который использует старую уязвимость для удаления шпионского ПО.

В случае ChatLite шпионское ПО представляло собой специально разработанное приложение для Android, которое позволяло злоумышленнику собирать конфиденциальные данные с устройства и получать дополнительные вредоносные инструменты.

Для шпионского ПО, распространяемого через вредоносный документ Word, оно обладало следующими возможностями:

Записывать нажатия клавиш

Регулярно делайте скриншоты

Украсть файлы с локальных и съемных носителей

Загрузите дополнительные модули шпионского ПО

Анализируя образец шпионского ПО для Android, следователи Amnesty обнаружили несколько сходств с «Kashmir_Voice_v4.8.apk» и «SafeShareV67.apk», двумя вредоносными программами, связанными с прошлыми операциями Donot Team.

Ошибка opsec злоумышленника позволила исследователям обнаружить «тестовый» сервер в США, где злоумышленники хранили скриншоты и данные кейлоггеров со скомпрометированных телефонов Android.

Именно здесь Amnesty впервые увидела IP-адрес Innefu Labs, поскольку в остальном реальный источник скрывался за VPN.

Того нанимает иностранных хакеров?

Это первый случай, когда команда Donot была замечена нацеленной на организации в африканских странах, и это может указывать на то, что группа предлагает правительствам услуги «по найму».

Freedom House присваивает Тогорейтинг «частично свободный», поскольку управление страной находится в руках семьи Гнасингбе с 1963 года. Главный оппозиционный кандидат Агбейоме Коджо был арестован в апреле 2020 года.

К сожалению, нарушения прав человека, нападения на активистов и защитников гражданских свобод, а также подрывающий политический плюрализм - обычное дело в Того, и, согласно докладу Amnesty, дела в африканской стране только ухудшаются». ***(Bill Toulas. Amnesty International links cybersecurity firm to spyware operation // Bleeping Computer®***

(https://www.bleepingcomputer.com/news/security/amnesty-international-links-cybersecurity-firm-to-spyware-operation/). 10.10.2021).

***

«Компанія ESET повідомила, що її спеціалісти виявили унікального завантажувача для бінарних файлів Windows, який працює як сервер.

Відповідно до даних телеметрії ESET, за останні два роки було зафіксовано кілька зразків Wslink у Центральній Європі, Північній Америці та на Близькому Сході.

Варто зазначити, що завантажувач - це шкідливий код (програма), який використовується для завантаження інших виконуваних файлів на інфікований пристрій, у цьому випадку - безпосередньо у пам’ять.

«Wslink - це простий, але цікавий завантажувач, який на відміну від інших, працює як сервер та виконує отримані модулі в пам'яті, Ї коментує Владислав Грчка, дослідник ESET. Ї Це нове шкідливе програмне забезпечення отримало назву Wslink через одну зі своїх DLL».

Дослідники ESET розкрили можливості Wslink та інформували спеціалістів з кібербезпеки.

Відсутність подібностей коду, функціоналу або поведінки не дозволяють пов’язати інструмент із відомими групами кіберзлочинців. Крім того, його модулі повторно використовують функції завантажувача для з'єднання, ключів та сокетів, тому їм не потрібно створювати нові вихідні з'єднання. Wslink також має якісно розроблений криптографічний протокол для захисту даних для обміну.

«Ми реалізували власну версію клієнта Wslink, яка показує можливість повторного використання існуючих функцій завантажувача та взаємодії з ними. Наш аналіз є корисним тим, що інформує про цю загрозу спеціалістів з кібербезпеки», – пояснює дослідник ESET.

Повний вихідний код клієнта доступний у репозиторії WslinkClient на GitHub». ***(Wslink — новий шкідливий завантажувач, який працює як сервер // Компьютерное Обозрение (https://ko.com.ua/wslink_-_novij_shkidlivij_zavantazhuvach_yakij_pracyuye_yak_server_139185). 28.10.2021).***

***

«Антивірусні продукти Dr.Web для Android у вересні на захищуваних пристроях найчастіше виявляли рекламні троянські, атакож шкідливі програми, що завантажували інше програмне забезпечення та виконували довільний код. Окрім того, серед найактивніших загроз знову виявилися різні небажані рекламні модулі, які розробники вбудовують у програми з метою монетизації.

Протягом попереднього місяця вірусні аналітики компанії «ДокторВеб» виявили вкаталозі Google Play десятки нових програм-підробок сімейства Android.FakeApp, використовуваних зловмисниками в різних шахрайських схемах.

За даними антивірусних продуктів Dr.Web для Android

Android.HiddenAds.1994– Троян, призначений для показу нав'язливої реклами. Трояни цього сімейства часто поширюються під виглядом нешкідливих

програм і в деяких випадках встановлюються в системний каталог іншими шкідливими програмами.

Android.Triada.4567, Android.Triada.510.origin – Багатофункціональні трояни, що виконують різні шкідливі дії. Відносяться до сімейства троянських програм, що проникають у процеси всіх працюючих програм. Різні представники цього сімейства можуть зустрічатися в прошивках Android-пристроїв, куди зловмисники впроваджують їх на етапі виробництва. Окрім того, деякі їх модифікації можуть експлуатувати уразливості, щоб отримати доступ доз ахищених системних файлів і каталогів.

Android.RemoteCode.284.origin – Шкідлива програма, що завантажує та виконує довільний код. Залежно від модифікації трояни цього сімейства також можуть завантажувати різні веб-сайти, переходити за посиланнями, натискати на рекламні банери, підписувати користувачів на платні послуги та виконувати інші дії.

Android.DownLoader.1007.origin – Троян, що завантажує інші шкідливі програми та непотрібне ПЗ. Подібні трояни можуть ховатися у зовнішньо нешкідливих програмах, що поширюються з каталогу Google Play або завантажуються зі шкідливих сайтів.

Program.FakeAntiVirus.1 – Детектування рекламних програм, що імітують роботу антивірусного ПЗ. Такі програми можуть повідомляти про неіснуючі загрози та вводити користувачів у оману, вимагаючи оплатити купівлю повної версії.

Program.WapSniff.1.origin – Програма для перехоплення повідомлень в месенджері WhatsApp.

Program.FreeAndroidSpy.1.origin, Program.Reptilicus.7.origin – Програми, що стежать за власниками Android-пристроїв і можуть використовуватися для кібершпигунства. Вони здатні контролювати місцезнаходження пристроїв, збирати дані про SMS-листування, бесіди в соціальних мережах, копіювати документи, фотографії тавідео, прослуховувати телефонні дзвінки та оточення тощо.

Program.SecretVideoRecorder.1.origin – Програма, призначена для фонової фото- та відеозйомки за допомогою вбудованої камери Android-пристроїв. Вона може працювати непомітно, відключаючи повідомлення про запис, а також змінювати значок і опис програми на фальшиві. Така функціональність робить дану програму потенційно небезпечною.

Tool.SilentInstaller.14.origin, Tool.SilentInstaller.6.origin, Tool.SilentInstaller.13.origin – Потенційно небезпечні програмні платформи, які дозволяють програмам запускати apk-файли без їх встановлення. Вони створюють віртуальне середовище виконання, яке не впливає на основну операційну систему.

Tool.Packer.1.origin – Спеціалізована утиліта-пакувальник, призначена для захисту Android-програм від модифікації та зворотного інжинірингу. Вона не є шкідливою, але може використовуватися для захисту як нешкідливих, так і троянських програм.

Tool.Obfuscapk.1– Детектування програм, захищених утилітою-обфускатором Obfuscapk. Ця утиліта використовується дляавтоматичної модифікації та заплутування вихідного коду Android-програм, щоб ускладнити їх зворотний

інжиніринг. Зловмисники застосовують її для захисту шкідливих та інших небезпечних програм відвиявлення антивірусами.

Програмні модулі, що вбудовуються в Android-програми, призначені для показу нав'язливої реклами на мобільних пристроях. Залежно від сімейства та модифікації вони можуть демонструвати рекламу в повноекранному режимі, блокуючи вікна інших програм, виводити різні повідомлення, створювати ярлики та завантажувати веб-сайти. Adware.SspSdk.1.origin, Adware.AdPush.36.origin, Adware.Adpush.16510, Adware.Adpush.6547, Adware.Myteam.2.origin.

Загрози вGoogle Play

У вересні фахівці компанії «Доктор Веб» виявили в Google Play декілька десятків нових програм-підробок, які допомагали зловмисникам реалізовувати різні шахрайські схеми. В їх числі був троян Android.FakeApp.344, декілька модифікацій якого поширювалися під виглядом найрізноманітніших програм – графічних оболонок (лончерів), збірок зображень, самовчителя гри на піаніно, програм для контролю пульсу та ін.

Його основна функція – завантаження веб-сайтів за командою авторів вірусів. При цьому троян може використовуватися в різних шкідливих сценаріях: виконувати фішинг-атаки, підписувати жертв на платні послуги мобільного зв'язку, просувати сайти, які цікавлять зловмисників, або ж завантажувати сайти зрекламою.

Android.FakeApp.344 керується з одного з облікових записів GitHub, репозиторії яких містять конфігураційні файли. При запуску троян отримує необхідні налаштування. Якщо в них є відповідне завдання, він завантажує цільовий сайт. Якщо ж завдання немає або трояну невдалося отримати конфігурацію, він працює у звичайному режимі, а користувачі можуть навіть не підозрювати, що з програмою щось не так.

Інші виявлені шкідливі програми-підробки отримали імена Android.FakeApp.347, Android.FakeApp.364 іAndroid.FakeApp.385. Вони також поширювалися як нешкідливі та корисні програми – програми для безкоштовних дзвінків, фоторедактор, програми на релігійну тематику та ПЗ для захисту встановлених програм від несанкціонованого використання.

Проте заявлених функцій вони не виконували – трояни лише завантажували різні сайти, утому числі такі, на яких у користувачів запитували номер мобільного телефону. Після його введення власники Android-пристроїв переспрямовувалися на сторінку пошукової системи, й на цьому робота підробок завершувалася». ***(У вересні спостерігалась висока активність програм-підробок, які поширюються з каталогу Google Play // Компьютерное Обозрение (https://ko.com.ua/u_veresni_sposterigalas_visoka_aktivnist_program-pidrobok_yaki_poshiryuyutsya_z_katalogu_google_play_139152). 26.10.2021).***

***

«Как быстро атакующие программы-вымогатели могут нанести удар? В одном случае три часа - это все, что потребовалось одному или нескольким злоумышленникам, использующим программы-вымогатели, чтобы получить первоначальный доступ к цели, развернуть атаку и развернуть вредоносное ПО для криптоблокировки.

Так заявляет компания по безопасности Sophos в новом отчете, в котором подробно описывается вспышка программ-вымогателей, поразившая установку VMware ESXi, которая представляет собой гипервизор корпоративного класса, который представляет собой гипервизор корпоративного класса для разделения серверов на несколько виртуальных машин.

«Это одна из самых быстрых атак программ-вымогателей, которые когда-либо исследовала компания Sophos, и она, по всей видимости, была нацелена на платформу ESXi», - говорит Эндрю Брандт, главный исследователь Sophos.

Атака примечательна не только своей скоростью, но и списком защитных ошибок, допущенных жертвой, которая в противном случае могла бы отразить атаку, включая оставление ненужных функций активными и отказ от использования многофакторной аутентификации для блокировки инструментов удаленного доступа. особенно для пользователей с доступом уровня администратора к основным системам.

Удар по гипервизору дает злоумышленникам возможность принудительно зашифровать сразу несколько различных систем. Кроме того, если гипервизор должен поддерживать многопользовательскую среду, злоумышленники могут иметь возможность криптоблокировки систем, используемых несколькими организациями, что дает им больше жертв для вымогательства.

«Серверы ESXi представляют собой привлекательную цель для злоумышленников-вымогателей, поскольку они могут атаковать сразу несколько виртуальных машин, где на каждой из виртуальных машин могут быть запущены критически важные для бизнеса приложения или службы», - говорит Брандт.«Атаки на гипервизоры могут быть быстрыми и разрушительными. Операторы программ-вымогателей, включая DarkSide и REvil, атакуют серверы ESXi».

Группы таргетинга ESXi

Sophos не приписывает рассмотренную им атаку какой-либо конкретной группе вымогателей.

Но, как отмечается, несколько групп были замечены нацеленными на ESXi.К ним относятся REvil, также известный как Sodinokibi, который был доминирующим штаммом вымогателей, замеченных во втором квартале, прежде чем летом он замолчал. Но недавно группа вымогателей возобновила свою деятельность.

Также исчезнув летом, DarkSide, похоже, возродился как BlackMatter. В августе группа исследования безопасности Malware Hunter Team предупредила, что BlackMatter продолжает использовать версию вредоносного ПО DarkSide для Linux, разработанную для сред ESXi, которая включает в себя возможность запускать команды оболочки ESXi и, таким образом, принудительно выключать

виртуальные машины, чтобы они могли быть зашифрованными и требовать выкупа.

Тем временем в июле Доэль Сантос и Ручна Нигам из группы исследования угроз Unit 42 в Пало-Альто предупредили, что они заметили «Linux-вариант HelloKitty, нацеленный на гипервизор VMware ESXi, который широко используется в облачных и локальных центрах обработки данных».

Злоумышленники владеют Python

В своем отчете Sophos сообщает, что в этом инциденте злоумышленники успешно внедрили скрипт Python на сервер, работающий под управлением ESXi, на котором по умолчанию установлен Python.

Что не ясно, так это то, сколько других организаций пытались атаковать, прежде чем успешно поразить эту.

Sophos не сразу ответила на запрос о дополнительной информации о жертве, например об отрасли и географии, в которой она работает.

Но многие аспекты МО злоумышленников не являются чем-то новым, включая их нанесение ударов по жертве в выходные дни, когда ИТ-специалисты с меньшей вероятностью обнаружат или смогут быстро остановить вторжение.

К счастью для злоумышленников, Sophos заявляет, что они, похоже, нашли активную оболочку для доступа к ESXi, которую администраторы используют для повседневного обслуживания, включая обновления, но которую они обычно деактивируют впоследствии из соображений безопасности…

Основы безопасности

Вывод для любой организации, использующей гипервизор, заключается в том, что у злоумышленников есть история попыток их использования, а это означает, что им следует применять соответствующие меры защиты.

«Это включает в себя использование уникальных паролей, которые сложно подобрать перебором, и принудительное использование многофакторной аутентификации везде, где это возможно», - говорит Брандт, особенно для учетных записей удаленного доступа, включая протокол удаленного рабочего стола и TeamViewer.

Чтобы помочь организациям, использующим ESXi, VMware опубликовала руководство по защите гипервизора.

Помимо минимизации доступа, не в последнюю очередь для администраторов, включая регулярный аудит уровней доступа Active Directory, Sophos также рекомендует использовать виртуальные локальные сети или VLAN для сегментации критически важных серверов, включая платформы ESXi, чтобы затруднить их атаку.

«Оболочка ESXi может и должна быть отключена всякий раз, когда она не используется персоналом для текущего обслуживания, например, во время установки исправлений», - говорит Брандт.«ИТ-группа может сделать это либо с помощью элементов управления на консоли сервера, либо с помощью инструментов управления программным обеспечением, предоставляемых поставщиком». ***(Mathew J. Schwartz. How Ransomware Attackers Hit Virtual Machine Hypervisors // Information Security Media Group, Corp.***

(https://www.govinfosecurity.com/how-ransomware-attackers-hit-virtual-machine-hypervisors-a-17675). 05.10.2021).

***

«Агрессивная, финансово мотивированная группа русскоязычных злоумышленников, которая развертывает вариант программы-вымогателя Ryuk, использует брокеров первоначального доступа Trickbot и обычно пропускает попытки двойного вымогательства в пользу быстрых и более высоких выкупов, в основном нацелена на сектор здравоохранения, предупреждает отчет от охранной фирмы Mandiant.

По словам Mandiant, группа злоумышленников, получившая название FIN12, стояла за «многочисленными атаками программ-вымогателей», начиная как минимум с октября 2018 года.

«Операции FIN12 демонстрируют, что ни одна цель не является закрытой, когда дело доходит до атак программ-вымогателей, в том числе тех, которые обеспечивают функции критической помощи», - говорится в отчете.

Около 20% жертв FIN12, непосредственно наблюдаемых Mandiant, работали в сфере здравоохранения. Это включает в себя атаки FIN12 на медицинские организации как до, так и после того, как в октябре 2020 года было опубликовано совместное предупреждение несколькими правительственными организациями США, включая CISA, ФБР и Министерство здравоохранения и социальных служб, с предупреждением об «увеличивающихся и неизбежных» угрозах больницам и больницам. в медицинских учреждениях с участием Рюка, отмечает Mandiant (см.Больницы США, предупрежденные о новой волне атак программ-вымогателей).

«Эта схема нацеливания отличается от некоторых других злоумышленников, которые, по крайней мере, заявили о намерении проявлять сдержанность при нацеливании на больницы, особенно во время пандемии COVID-19», - отмечает Mandiant.

Например, в недавних предупреждениях HHS для сектора здравоохранения об угрозах, связанных с группами программ-вымогателей LockBit 2.0 и BlackMatter, отмечалось, что, вопреки свидетельствам таких атак, группы заявляют, что не нацелены на больницы и другие медицинские учреждения.

Верхняя цель

Медицинские учреждения по-прежнему являются главной целью атак программ-вымогателей, поскольку они предоставляют своим пациентам услуги по спасению жизни, «что означает, что они не могут позволить себе отключать свои учреждения из-за кибератаки - и могут быть более гибкими, чтобы платить выкуп быстрее и быстрее. «обеспечить безопасность человеческой жизни», - говорит вышедший на пенсию агент ФБР Джейсон Г. Вайс, поверенный юридической фирмы Faegre Drinker Biddle & Reath LLP.

«Эти атаки со стороны FIN12, а также других банд вымогателей, а теперь и новые банды,« сдающие в аренду »вымогатели другим бандам, будут продолжаться до тех пор, пока они будут успешными и есть деньги, которые можно заработать. Период», - говорит он.

Бретт Кэллоу, аналитик угроз компании Emsisoft, предлагает аналогичную оценку.

«Операторы программ-вымогателей непредсказуемы», - говорит он.«Если определенная тактика работает для них или конкретный сектор оказывается особенно прибыльным, это будет случай« промыть и повторить ».Зачем связываться с формулой победы?»

Независимо от того, является ли бизнес-предприятие законным или преступным, «они сосредотачиваются на стратегиях, которые, по их мнению, работают хорошо, а в случае FIN12, похоже, это включает в себя атаки на сектор здравоохранения», - добавляет он.

Другие жертвы

По словам Mandiant, другие жертвы FIN12 были в различных секторах, включая бизнес-услуги, образование, финансы, правительство, производство, розничную торговлю и технологии.

«Большинство наблюдаемых жертв FIN12 базировались в Северной Америке, но их региональное нацеливание расширилось в 2021 году на другие регионы, включая Европу и Азиатско-Тихоокеанский регион», - отмечает Mandiant.

«Мы также стали свидетелями взрыва атак программ-вымогателей на организации, не относящиеся к сфере здравоохранения, такие как правительственные веб-сайты, школы, университеты и даже местные муниципалитеты».- Джейсон Г. Вайс, Faegre Drinker Biddle & Reath LLP.

Mandiant заявляет, что подозревает, что FIN12, вероятно, состоит из русскоязычных участников, которые могут находиться в странах Содружества Независимых Государств, которые являются бывшими членами Советского Союза. «FIN12 не нацелился на организации из стран СНГ и не выявил партнеров, и все идентифицированные в настоящее время пользователи Ryuk говорят по-русски», - сообщает компания.

Особенности атаки

По словам Mandiant, почти при каждом вторжении FIN12 с февраля 2020 года FIN12 использовала полезные нагрузки Cobalt Strike Beacon для взаимодействия с сетями-жертвами, продвигаясь через свои атаки от внутренней разведки до развертывания вымогателей.

Ранее, однако, FIN12 использовал более широкий набор инструментов для выполнения тех же функций, включая платформу Empire на основе PowerShell и, в своих самых ранних вторжениях, использование банковского трояна Trickbot в качестве пост эксплуатационной структуры наряду с Empire, говорится в отчете.

В отчете говорится, что FIN12 полагается на партнеров для получения первоначального доступа к среде жертв.«Примечательно, что вместо многостороннего вымогательства - тактики, широко используемой другими злоумышленниками-вымогателями, - FIN12, по-видимому, уделяет приоритетное внимание скорости и более высоким доходам жертв», - говорится в отчете.

«Отсутствие крупномасштабной кражи данных в инцидентах FIN12 почти наверняка способствовало их высокой частоте операций, при этом вторжения FIN12 составляют почти 20% наших действий по реагированию на инциденты с программами-вымогателями с сентября 2020 года».

Mandiant заявляет, что проанализировал ограниченный набор транзакций биткойн-кошельков, связанных с платежами, совершенными жертвами FIN12.

«Мы с высокой степенью уверенности оцениваем, что выплаты жертвам распределяются между различными участниками угроз, что согласуется с нашим убеждением, что FIN12 использует поставщиков первичного доступа и, вероятно, других партнеров для завершения всех аспектов жизненного цикла атаки».

Как отмечает Mandiant, годовой доход жертв обычно превышает 300 миллионов долларов.«Мы считаем, что партнеры FIN12 используют более широкую сеть и позволяют участникам FIN12 выбирать из списка жертв после того, как доступ уже получен»

Рабочие отношения

По словам Mandiant, FIN12, похоже, поддерживает тесные рабочие отношения с участниками, связанными с разработкой троянских программ Trickbot и связанных семейств, в том числе Bazarloader, Bazarbackdoor и Anchor.

«В некоторых случаях оказывается, что эти отношения могут привести к совместному использованию ресурсов, включая использование вредоносных программ, которые нетипичны для вторжений FIN12», - говорит Mandiant.

«Помимо использования доступа, полученного с помощью этих семейств, как FIN12, так и деятельность, связанная с Trickbot, обычно используют перекрывающиеся наборы инструментов и сервисов, включая бэкдоры, дропперы и сертификаты для подписи кода».

Несмотря на эти совпадения, Mandiant отслеживает FIN12 «как отдельный субъект угрозы, учитывая особую роль в развертывании программ-вымогателей и их продемонстрированную способность работать независимо».

Другие тенденции атак

Маркус Гидри, старший аналитик по киберугрозам в охранной компании Pondurance, отмечает, что FIN12 использует многие из тех же инструментов, что и другие группы программ-вымогателей для запуска своих атак. Например, «очень хорошо известно использование Cobalt Strike для горизонтального перемещения по взломанным сетям», - говорит он.

«К сожалению, после пандемии COVID-19 тенденции атак программ-вымогателей на сектор здравоохранения только продолжали расти», - говорит он.

Гидри говорит, что на данный момент в этом году ему известно о почти 90 атаках программ-вымогателей по всему миру на здравоохранение, и большинство из них было в США.

«Другие группы программ-вымогателей, такие как Conti, Revil и PYSA, также нацелены на здравоохранение таким же образом», - говорит он.

Вайс считает, что использование программ-вымогателей как услуги является опасной тенденцией в войнах программ-вымогателей и, вероятно, приведет к увеличению частоты и количества атак программ-вымогателей.

«Мы также стали свидетелями взрыва атак программ-вымогателей на организации, не относящиеся к сфере здравоохранения, такие как правительственные веб-сайты, школы, университеты и даже местные муниципалитеты», - говорит он.

«Короче говоря, войны с программами-вымогателями вступают в новое и опасное расширение, которое будет продолжаться только до тех пор, пока эти киберугрозы будут продолжать выкупать значительные суммы».

Защита от атак

По словам Гуидри, основной проблемой для многих медицинских организаций является нехватка ресурсов для адекватной защиты от атак программ-вымогателей.

«Лучший способ не дать группам вымогателей атаковать вашу среду - это реализовать многоуровневый защитный подход», - говорит он. Установка последних исправлений безопасности для критически важных приложений, таких как Citrix и Exchange, является обязательной ».

По его словам, еще одним важным шагом для организаций является немедленная изоляция и восстановление любых машин в их сетях, на которых было обнаружено вредоносное ПО, являющееся предшественником программ-вымогателей, например Trickbot, BazarLoader, Qbot или IcedID». ***(Marianne Kolbasuk McGee. FIN12 Ransomware Attacks Aggressively Targeting Healthcare // Information Security Media Group, Corp. (https://www.govinfosecurity.com/fin12-ransomware-attacks-aggressively-targeting-healthcare-a-17717). 11.10.2021).***

***

«Виплати хакерам-здирникам, які здійснювали кібератаки за допомогою вірусів в США, за перші шість місяців 2021 року досягли 590 мільйонів доларів - це на 42 відсотки більше, ніж за весь 2020 рік (416 мільйонів). Про це повідомляється в доповіді Міністерства фінансів США, опублікованому в п'ятницю, 15 жовтня…

Цитата

«Програми-вимагачі та кібератаки становлять пряму загрозу нашій економіці, їх жертвами стають великі і малі підприємства зі всієї Америки»,— сказано взвіті.

Контекст

Вашингтон 13-14 жовтня проводив конференцію по боротьбі з хакерами-вимагачами, в якій брали участь близько 30 країн. Серед іншого вони обговорили опір спробам вимагання та роль криптовалюта у відмиванні коштів, одержуваних кіберзлочинцями в якості викупу. Примітно, що Росія небула запрошена на конференцію…». ***(Ілля Нежигай. Майже 600 млн доларів виплатили хакерам-здирникам в США в 2021 році // Українські Національні Новини (https://www.unn.com.ua/uk/news/1948366-mayzhe-600-mln-dolariv-viplatili-khakeram-zdirnikam-v-ssha-v-2021-rotsi). 16.10.2021).***

***

«Тільки в першому кварталі цього хакери виманили 81 мільйон доларів.

Жертви кібератак, що проводилися за допомогою вірусів-вимагачів, заплатили хакерам по всьому світу понад 400 мільйонів доларів у 2020 році, підрахували в США.

«Глобальні економічні втрати від програмного забезпечення вимагачів є значними. Виплати (хакерам) в результаті нападів з використанням вірусів-

вимагачів досягли у 2020 році понад $400 млн по всьому світу», - йдеться в заяві Білого дому.

Такі кібератаки вчиняються проти організацій будь-яких розмірів і незалежно від того, де вони розташовані.

США неодноразово звинувачували в кібератаки хакерів з Китаю, Росії, Північної Кореї та Ірану». ***(Александр Хребет. Скільки заробляють хакери-вимагачі: У США порахували суму // Дзеркало тижня. Україна (https://zn.ua/ukr/WORLD/skilki-zarobljajut-khakeri-vimahachi-u-ssha-porakhuvali-sumu.html). 13.10.2021).***

***

«У середу і четвер Вашингтон зібрав близько 30 країн для активізації міжнародної боротьби з програмами-вимагачами, сказав високопосадовець Білого дому, зазначивши, що Росія запрошення не отримала.

Велика Британія, Австралія, Індія, Японія, Франція, Німеччина, Південна Корея, Європейський Союз, Ізраїль, Кенія і Мексика - серед тих, хто має приєднатися до віртуального саміту.

За словами високопосадовця, обговорення будуть обертатися навколо чотирьох тем: підвищення стійкості до спроб вимагання, роль криптовалюти у відмиванні викупу, правоохоронні та судові дії, а також дипломатія.

«Коли ми почали розсилати запрошення... прагнення до участі, прагнення вчитися, прагнення допомагати іншим країнам в нарощуванні потенціалу... було просто величезним», - сказав високопосадовець, передає AFP.

Відповідаючи на питання про відсутність Москви, джерело відповіло, що «ми не запрошували росіян до участі з низки причин», додавши, що Вашингтон встановив «окремий канал» для зв'язку з Москвою з цього питання…». ***(Оксана Лебедина. США проведуть глобальний саміт щодо кібербезпеки без Росії // Дзеркало тижня. Україна (https://zn.ua/ukr/WORLD/ssha-provedut-samit-z-kiberzlochinnosti-bez-rosiji.html). 13.10.2021).***

***

«Фирма кибербезопасности VirusTotal по поручению Google проанализировала 80 миллионов образцов программ-вымогателей из более чем 140 стран, полученных ею с 2020 года.

В предоставленном отчёте десятью наиболее пострадавшими государствами по количеству образцов, рассмотренных VirusTotal, в порядке убывания названы Израиль, Южная Корея, Вьетнам, Китай, Сингапур, Индия, Казахстан, Филиппины, Иран и Великобритания. При этом, Израиль лидирует почти с 5-кратным отрывом от следующей за ним Южной Кореи.

Главный пик активности ransomware, наблюдавшийся впервые два квартала 2020 г., VirusTotal связывает с деятельностью группы GandCrab, предлагающей программы-вымогатели как услугу. Второй по величине пик приходится на июль 2021 г., его виновником является преступная группировка Babuk, впервые заявившая о себе вначале 2021 г.

Среди самых активных банд вымогателей сначала 2020 года GandCrab лидирует с 78,5 процентами образцов. На Babuk и Cerber приходятся доли 7,6% и 3,1% соответственно.

Масштабы действий GandCrab и Babuk, делают остальные семейства ransomware почти невидимыми на диаграмме. Тем не менее, VirusTotal подчёркивает, что эта фоновая активность более, чем 100 других семейств программ-вымогателей никогда не останавливалась и не должна игнорироваться.

Согласно отчету, 95% обнаруженных файлов-ransomware были исполняемыми файлами или динамическими библиотеками (DLL) Windows, и лишь 2% — ориентированы на Android.

Также обнаружено, что с эксплойтами (чаще всего, повышения привилегий и удалённого выполнения) непосредственно связано очень мало образцов— около 5%. Это легко объяснимо, если вспомнить, что ransomware, как правило, распространяется с помощью методов социальной инженерии и/или дропперов (небольших программ, предназначенных для установки вредоносного ПО).

Только две из 10 наиболее часто эксплуатируемых уязвимостей были обнародованы в 2020 году и ни одной — в 2021 году.

Почти все из 10 главных семейств программ-вымогателей использовали для распространения одну из пяти разновидностей вредоносных программ: Emotet, Zbot, Dridex, Gozi, Danabot.

Для других этапов, таких как латеральное продвижение вкорпоративных сетях, VirusTotal выявила применение Mimikatz иCobaltstrike, нескольких языков сценариев, таких как AutoIT и Powershell и десятков троянских программ удалённого доступа (RAT), включая Phorpiex, Smokeloader, Nanocore иPonystealer». ***(Google опубликовала итоги анализа 80 млн образцов ransomware //Компьютерное Обозрение (https://ko.com.ua/google_opublikovala_itogi_analiza_80_mln_obrazcov_ransomware_139063). 18.10.2021).***

***

«Отключения пресловутого Revil - ака Sodinokibi - вымогателей операция была из-за координации усилий правоохранительных органов с участием США и иностранных партнеров, направленных на срыв возможности атаки на группы.

«ФБР вместе с Киберкомандованием, Секретной службой и странами-единомышленниками действительно предприняли серьезные подрывные действия против этих групп», -сказал Том Келлерманн, глава стратегии кибербезопасности VMWare, а также советник Секретной службы США по расследованию киберпреступлений. Служба, сообщает Reuters. «REvil был первым в списке».

На прошлой неделе Белый дом сообщил, что известные выплаты злоумышленникам-вымогателям достигли более 400 миллионов долларов во всем мире в 2020 году и превысили 81 миллион долларов в первом квартале 2021 года.

REvil считается одной из самых больших таких угроз. После первого появления в апреле 2019 года как ответвление программы-вымогателя GandCrab, REvil быстро стал одним из самых доминирующих и разрушительных штаммов

программ-вымогателей. Но сайт утечки данных Happy Blog, где он называет имена жертв и позорит их, а также платежный портал, где жертвы могут договориться и заплатить выкуп, закрылись в июле, вскоре после двух крупных атак.

30 мая злоумышленники с REvil зашифровали системы на американских предприятиях бразильского мясоперерабатывающего гиганта JBS, который заплатил злоумышленникам выкуп в размере 11 миллионов долларов в обмен на ключ дешифрования и обещание не утечки украденных данных. 2 июля REvil организовал атаку с помощью программного обеспечения для удаленного управления ИТ, разработанного Kaseya и используемого поставщиками управляемых услуг. В общей сложности он поразил около 1500 организаций - в совокупности клиентов 50 различных поставщиков услуг - и заблокировал многие из их систем.

Президент США Джо Байден мобилизует дополнительные ресурсы на борьбу с угрозой, исходящей от программ-вымогателей, после ряда таких атак, в результате которых не только REvil, но и многие другие группы серьезно нарушили критически важную инфраструктуру не только в Соединенных Штатах, но и в соседних странах. страны.

Эксперты говорят, что усилиям по прямому разрушению групп программ-вымогателей помогла Генеральная прокуратура США, которая подняла усилия по борьбе с программами-вымогателями до уровня, в котором они теперь привлекают внимание и ресурсы, равные тем, которые выделяются на борьбу с терроризмом. С юридической точки зрения это дало правоохранительным органам и правительственным группам взломщиков большую свободу действий.

«Раньше на эти форумы нельзя было взломать, и военные не хотели иметь с этим ничего общего», - сказал Келлерманн. «С тех пор перчатки оторвались».

В то же время Министерство финансов также пытается ограничить поток криптовалютных средств группам программ-вымогателей, чтобы еще больше подорвать эффективность этой незаконной бизнес-модели.

Хиты критического сектора

Не только REvil, но и другие группы вызывают разрушение. В мае национальная служба здравоохранения Ирландии пострадала от Конти, вызвав многомесячный удар, который нарушил медицинское обслуживание по всей стране. В том же месяце DarkSide ударил по компании Colonial Pipeline Co., которая поставляет 45% топлива на Восточное побережье США, что привело к панической покупке газа среди населения. Colonial заплатила DarkSide выкуп в размере 4,4 миллиона долларов, большую часть которой ФБР удалось вернуть.

Памела Клегг, директор по образованию и расследованиям компании CipherTrace, занимающейся блокчейн-аналитикой, выступая на ежегодной конференции по цифровым расследованиям, организованной в июне швейцарским торговым посредником по цифровым расследованиям Ариной, заявила, что у нее есть «достоверные сведения» о том, что ФБР получило доступ к DarkSide. биткойн-кошелек через закрытый ключ к кошельку, обнаруженный на устройстве, которое было конфисковано иностранным правоохранительным органом до того, как произошла атака Colonial Pipeline или был выплачен выкуп.

Выпущен бесплатный дешифратор REvil

Некоторые эксперты по безопасности, в том числе технический директор Emsisoft Фабиан Восар, ранее отмечали, что доступ к инфраструктуре REvil со стороны правоохранительных органов - Reuters сообщает, что это не ФБР, а иностранный партнер - привел к получению рабочего ключа дешифрования для REvil.

Директор ФБР Кристофер Рэй в сентябре подтвердил сообщение Washington Post о том, что ФБР хранило этот ключ дешифрования REvil в течение трех недель, прежде чем разрешить передать его жертвам. Выступая перед комитетом Сената по национальной безопасности и делам правительства, Рэй сказал, что бюро не хотело сообщать злоумышленникам о том, что оно получило некоторый доступ к их инфраструктуре.

«Чтобы убедиться, что они действительно собираются делать то, что они должны делать, требуется много тестов и проверок», - сказал Рэй о ключах дешифрования.«И для разработки этого инструмента требуется много инженерных усилий… Иногда нам приходится делать расчеты, как лучше всего помочь большинству людей, потому что максимальная отдача - это всегда цель, и всякий раз, когда мы делаем это в этих совместных упорядоченных операциях, мы делаем это совместно с другими правительственными агентствами и прочими ».

Но, как сообщалось ранее, правоохранительные органы передали ключ. Это привело к тому, что в прошлом месяце охранная фирма Bitdefender смогла разработать и выпустить бесплатный дешифратор почти для всех версий REvil, которые были до его исчезновения в июле.

Первая перезагрузка REvil

Представители Белого дома и ФБР ранее заявляли, что не знают, почему REvil погас в июле. Судя по показаниям Рэя и решению ФБР не раскрывать полученный универсальный ключ дешифрования, это, похоже, застало бюро врасплох.

Как сообщает Reuters, иностранные партнеры из правоохранительных органов сыграли важную роль в получении ключа REvil, а также в последнем вмешательстве.

По словам экспертов по безопасности, один из основных администраторов REvil, известный под ником «Неизвестный», с июля не публиковал сообщения на форумах, посвященных киберпреступности.

Однако ранее в этом месяце другой предполагаемый основной оператор REvil, известный под ником «0_neday», объявил в сообщении на форуме XSS по киберпреступности, что программа-вымогатель снова запущена и что судьба Unknown остается неизвестной; возможно, он был мертв.

«После июльских сбоев считается, что REvil сбросил ключи кампании, используемые каждым филиалом», - говорит Джейк Уильямс, технический директор компании BreachQuest, занимающейся реагированием на инциденты. Он добавляет, что 0_neday пообещал предоставить филиалам новые ключи кампании, чтобы они могли возобновить вытряхивание жертв, чтобы они заплатили, в обмен на обещание ключа дешифрования.

Однако в воскресенье, когда впервые заметил Recorded Future, 0_neday объявил, что сайты REvil были захвачены, что он, по крайней мере, временно отключит их от сети и что кто-то, очевидно, «ищет» его.

«Я проверил сайты и не обнаружил никаких признаков компрометации», - сказал 0_neday в своих сообщениях XSS. Но он предположил, что кто-то, похоже, получил полную резервную копию сайтов Tor REvil, включая закрытый ключ, необходимый для создания сайта.

Любой, у кого есть такой ключ, может запустить свою собственную версию сайта, заменяющую все предыдущие версии. Другими словами, сотрудники правоохранительных органов могли бы заменить свою собственную версию сайта утечки данных и платежного портала REvil, потенциально, чтобы шпионить за администраторами и аффилированными лицами и помогать им идентифицировать их.

После июльского закрытия банда вымогателей REvil восстановила инфраструктуру из резервных копий, предположив, что она не была взломана.По-видимому, это были резервные копии, а также их личные служебные ключи .onion, сообщил Information Security Media Group Олег Скулкин, заместитель начальника лаборатории судебной экспертизы российской охранной компании Group-IB. «По иронии судьбы, любимая тактика банды - компрометация резервных копий - была обращена против них», - говорит он.

Как именно правоохранительные органы получили ключи и резервные копии, остается неясным.«Хотя ключи потенциально могли быть получены исключительно путем взлома, трудно представить, что это так, учитывая исчезновение Неизвестного», - говорит Уильямс.«Очевидный вывод состоит в том, что, скорее всего, Неизвестный - или близкий соучастник - был арестован, хотя арест, возможно, был произведен с помощью операций взлома».

Удар в спину ведет к Fallout

Правоохранительные органы и исчезновение лидеров - не единственные проблемы REvil. Операции «программа-вымогатель как услуга», такие как REvil, полагаются на филиалы, которые заберут их вредоносное ПО и заразят жертв, что они и делают в обмен на долю любой прибыли, полученной в результате выплаты выкупа. Как правило, 70% остается у партнера. Но эксперты по обратному инжинирингу на форуме по киберпреступности обнаружили, что до июля вредоносная программа REvil для криптоблокировки включала в себя бэкдор, призванный помочь администраторам сократить количество филиалов, чтобы операторы могли удерживать 100% всей прибыли.

Как сообщает компания Digital Shadows, занимающаяся разведкой угроз, компания REvil с момента своего перезапуска предлагала филиалам 90% скидку.

Но высококвалифицированные партнеры - популярный товар. «Хотя отслеживание активности на уровне аффилированных лиц RaaS остается проблемой, очевидно, что диаспора аффилированных лиц из REvil была поглощена другими крупными операциями RaaS, такими как Conti и LockBit 2.0», - сообщает компания Coveware, занимающаяся реагированием на инциденты с программами-вымогателями.«LockBit 2.0, в частности, похоже, продвигает модель RaaS на новые территории, чтобы привлечь наиболее талантливых партнеров. В частности,

операция RaaS рекламирует большую прозрачность для аффилированных лиц и прямое получение доходов от программ-вымогателей. Кажется, что это соперничество между LockBit 2.0 и REvil. вынудили эти изменения».

Все еще ждете нокаутирующего удара?

Итак, перезагрузится ли REvil снова? Несмотря на то, что инфраструктура группы была нарушена, неясно, понесли ли она или все ее основные члены нокаутирующий удар.

«Даже несмотря на то, что REvil может не восстановиться после этого последнего отключения, это не обязательно означает, что они собираются остановить вредоносную деятельность», - говорит Скулкин из Group-IB. «Это может быть просто попыткой начать новую серию ценных кибер-ограблений под другим названием. Мы видели такой сценарий с DarkSide, DoppelPaymer и Avaddon».

Пока что, по крайней мере, некоторые важные возможности REvil, похоже, не были получены правоохранительными органами.«На данный момент кажется маловероятным, что у правительства США есть главный ключ для REvil», - говорит Уильямс.«После негативной реакции по поводу отказа от раскрытия ключа кампании, использованного в атаке Касеи, трудно поверить, что правительство рискнет получить еще больше негативной огласки. Отдельные филиалы могут выпустить свои ключи кампании, но в настоящее время сомнительно, что основная группа REvil сделает это.»

Если группа попытается снова возобновить операции, она столкнется с перспективой более скоординированных попыток коалиции правоохранительных и спецслужб 30 стран помешать ее усилиям, вслед за их предыдущим успехом.

«Эта однозначно хорошая новость является примером того, как сотрудничающие правительства могут накладывать издержки на участников программ-вымогателей», - говорит Аллан Лиска, аналитик разведывательной компании Recorded Future. «Смогут ли они перегруппироваться и запустить новую программу-вымогатель? Возможно. Но подобные агрессивные действия заставляют другие группы программ-вымогателей дважды подумать». ***(Mathew J. Schwartz. REvil Revelations: Law Enforcement Behind Disruptions // Information Security Media Group, Corp. (https://www.govinfosecurity.com/revil-revelations-law-enforcement-behind-disruptions-a-17779). 22.10.2021).***

***

«Когда бизнес, правительственное учреждение или любая другая организация поражается программой-вымогателем и решает заплатить выкуп своему злоумышленнику в обмен на ключ дешифрования или какое-либо другое обещание, в среднем они платят 140 000 долларов.

Так утверждает компания Coveware, занимающаяся реагированием на инциденты с программами-вымогателями, основываясь на тысячах инцидентов, расследованных с июля по август.

В новом отчете, подробно описывающем тенденции третьего квартала, Coveware сообщает, что средний размер выкупа оставался в основном стабильным

по сравнению со вторым кварталом, в то время как медиана увеличилась более чем на 50%.

В нем говорится, что этот сдвиг начался после ряда громких атак, которые начались в мае, в том числе DarkSide, разрушивший американский Colonial Pipeline, заставив потребителей в панике покупать топливо. Вскоре после этого REvil - также известный как Sodinokibi - атаковал гиганта мясопереработки JBS, а в праздничные выходные четвертого июля он поразил программное обеспечение компании Kaseya, занимающейся программным обеспечением удаленного управления, которое используется поставщиками управляемых услуг для шифрования и удержания систем выкупа, используемых более чем 1500 клиентов этих MSP.

Атаки вызвали яростную политическую реакцию со стороны администрации Байдена и других правительств, активизировав международные усилия по нацеливанию на злоумышленников с помощью правоохранительных средств, нарушив потоки криптовалюты, чтобы отобрать у них прибыль, и сосредоточить внимание на повышении устойчивости отечественного бизнеса к кибербезопасности. Белый дом также усиливает дипломатическое давление на Москву, чтобы заставить ее расправиться с киберпреступниками, действующими изнутри России.

По-видимому, в ответ на последствия, DarkSide прекратила свою деятельность, переименовавшись в BlackMatter. REvil был отключен от сети в июле по необъяснимым причинам, а затем снова появился в сентябре. В том же месяце охранная фирма Bitdefender получила от сотрудников правоохранительных органов ключи, которые позволили ей создать и выпустить бесплатный дешифратор почти для всех заражений REvil, начиная с июля и ранее. В этом месяце инфраструктура REvil снова отключилась, и администратор заявил, что операторы отключили сеть после того, как кто-то взломал сайты утечки данных и платежных порталов REvil на базе Tor.

'Охота в середине игры'

Между тем, картина атак программ-вымогателей продолжала меняться и в других направлениях.«С тех пор, как этой весной произошла атака на конвейер, мы стали свидетелями статистических данных и разведданных, показывающих, что участники программ-вымогателей пытаются избежать более крупных целей, которые могут вызвать реакцию национальных политиков или правоохранительных органов», - говорит Ковевар. «Этот переход от«охоты на крупную дичь»к«охоте в середине игры»олицетворяется как в статистике суммы выкупа, так и в демографии размера жертвы по кварталу».

Действительно, основываясь на исследованиях третьего квартала, Coveware заявляет, что малые и средние фирмы, оказывающие профессиональные услуги, особенно юридические и финансовые компании, по всей видимости, наиболее подвержены риску атак программ-вымогателей из-за недостаточной готовности к информационной безопасности, по-видимому, потому, что они считают, что они слишком малы, чтобы быть целью.

Но злоумышленники, использующие программы-вымогатели в поисках незаконной прибыли, обычно не нацелены на какую-либо конкретную

организацию, а скорее ищут в более широком плане плохо подготовленные секторы, которые предлагают максимальные возможности для получения прибыли, что сделало небольшие и средние фирмы, предоставляющие профессиональные услуги, «громоотводом для атак», Coveware говорит.

В то же время, хотя усилия, предпринимаемые для уничтожения программ-вымогателей, приветствуются, пока они, похоже, не оказывают заметного эффекта, говорит Coveware.

«Субъекты индустрии программ-вымогателей практически не подвергаются риску при проведении атак», - говорится в сообщении.«Фактически нет никаких недостатков в том, чтобы стать партнером программы-вымогателя, а экономика вымогательства привлекает новых участников каждый день. Пока экономика не будет нарушена и риски не начнут перевешивать выгоды, проблема будет сохраняться и расти».

Наиболее популярные сорта: Conti, Mespinoza.

Самыми популярными штаммами вымогателей, замеченными фирмой в третьем квартале, были Conti, Mespinoza, Sodinokibi, также известные как REvil, LockBit 2.0 и Hello Kitty. Все операции представляют собой вымогатель как услугу, что означает, что основная группа разработчиков и администраторов обслуживает вредоносное ПО и любой выделенный сайт утечки данных и нанимает аффилированных лиц для заражения жертв. Всякий раз, когда жертва платит, ответственный партнер и оператор программы-вымогателя должны делить прибыль.

Но REvil, по крайней мере, недавно был уличен в том, что он включил бэкдорв свое вредоносное ПО, позволяя администраторам красть долю филиалов.

Основные тактики и угрозы

Что касается тактики, методов и процедур, или TTP, используемых злоумышленниками, 83% всех атак с использованием программ-вымогателей в третьем квартале - по сравнению с 80% во втором квартале - включали угрозу утечки украденных данных.Но эксперты по безопасности продолжают предупреждать, что злоумышленники часто лгут о краже данных, имеющих какую-либо ценность.

Кроме того, полная или частичная выплата выкупа за обещание злоумышленников удалить украденные данные не дает никаких гарантий. Эксперты по безопасности предупреждают, что компании, которые все же платят выкуп, часто сталкиваются с дополнительным денежным требованием от той же группы злоумышленников или снова подвергаются ударам в результате той же операции или другой операции, стремясь извлечь выгоду из склонности жертвы платить.

Совет для защитников

Как организации могут лучше защитить себя от программ-вымогателей, основываясь на последних тенденциях атак?

«Защита большой корпоративной сети - это бесконечная задача, - говорит Ковевар. «Однако скорость, с которой злоумышленники повторно используют TTP, дает защитникам возможность выбрать слабые места, которые можно устранить

быстро и с минимальными затратами», имея в виду, что успешные атаки всегда требуют объединения нескольких тактик.

Примечательно, что первоначальные тенденции доступа в последние годы оставались в основном стабильными: плохо защищенный доступ к удаленному рабочему столу - также известный как RDP - и фишинговые атаки остаются двумя основными тактиками, используемыми преступниками, использующими программы-вымогатели, для получения первоначального доступа к сети жертвы. Но Coveware заявляет, что больше атак, чем раньше, также нацелены на известные уязвимости в программном обеспечении.

«Выявляя возможности в цепочке уничтожения для предотвращения этих атак, предприятия могут оппортунистически снизить риск», - говорит Ковевар». ***(Mathew J. Schwartz. Ransomware: Average Ransom Payment Stays Steady at $140,000 // Information Security Media Group, Corp.(https://www.govinfosecurity.com/ransomware-average-ransom-payment-stays-steady-at-140000-a-17773). 21.10.2021).***

***

«Не все злоумышленники, использующие программы-вымогатели, крадут данные жертв или угрожают публично назвать их имена и опозорить их, чтобы побудить их заплатить выкуп. Но одним из показателей ущерба, наносимого вредоносными программами с криптоблокировкой, по-прежнему является подсчет того, сколько организаций-жертв попадают в списки на выделенных сайтах утечки данных операторов программ-вымогателей в рамках так называемой тактики двойного вымогательства.

К сожалению, несмотря на то, что Белый дом объявил войну программам-вымогателям, включая инициативы по повышению киберустойчивости предприятий США, по крайней мере, до сих пор количество жертв, перечисленных на таких сайтах, не снижается, сообщает Аллан Лиска, аналитик разведки по угрозам. разведывательная фирма Recorded Future.

«В сентябре количество жертв, размещенных на сайтах-вымогателях, оставалось на рекордно высоком уровне», -пишет Лиска.«Как всегда, помните, что лишь небольшая часть жертв программ-вымогателей попадает на сайты-вымогатели, поэтому эти цифры не репрезентативны для всех атак».

Согласно его предостережениям, количество организаций, которые в конечном итоге попадают в списки сайтов утечки данных, не равно количеству организаций, являющихся объектами атак злоумышленников, или подмножества организаций, пострадавших от успешной атаки программ-вымогателей. По оценкам многих экспертов по безопасности, лишь небольшая часть - возможно, 25% - жертв программ-вымогателей когда-либо публично обнаруживается.

Например, некоторые организации будут поражены, стирают и восстанавливают свои системы и не делают публичных заявлений, и по какой-либо причине не будут перечислены на сайте утечки данных злоумышленника - возможно, потому, что у злоумышленников его нет.

Но, как отмечает Лиска, на таких сайтах перечисляются по крайней мере некоторые жертвы, и не всегда известные игроки.

Например, с 4 октября израильская разведывательная компания Kela сообщает, что эти 12 групп программ-вымогателей перечислили новых жертв на своих сайтах утечки данных: AtomSilo, BlackByte, BlackMatter, Conti, Grief, Hive, LockBit, Pysa, REvil / Sodinokibi, Spook, Порочное общество и Син.

В прошлом году охранные фирмы Kaspersky и Emsisoft подсчитали, что было совершено около 65 000 успешных атак с использованием программ-вымогателей. По оценкам Liska, в этом году на сайтах утечки данных будут перечислены в общей сложности 5000 жертв. Конечно, после публичного раскрытия информации жертвами будут обнаружены и другие атаки, возможно, в соответствии с правилами уведомления об утечке данных.

Подсчет жертв остается постоянным

Emsisoft сообщает, что, несмотря на недавнюю высокую оценку списков жертв, в целом количество организаций, перечисленных на таких сайтах, похоже, остается стабильным.

«Количество глобальных инцидентов с программами-вымогателями оставалось относительно стабильным в течение некоторого времени, поэтому неудивительно, что количество компаний, появляющихся на сайтах утечек, также оставалось относительно стабильным», - говорит Бретт Кэллоу, аналитик угроз Emsisoft.«Разрыв между предполагаемым количеством инцидентов и количеством жертв, оказавшихся на сайтах утечек, просто связан с тем фактом, что не все операторы программ-вымогателей используют сайты утечек, в том числе некоторые наиболее загруженные операторы, а также такие операторы, как FIN12.»

Просто взглянув на FIN12, например, русскоязычная группа, владеющая Рюком, стремится избегать двойного вымогательства, вместо этого добиваясь быстрых и более высоких выплат выкупа, говорит охранная фирма Mandiant.

Во втором квартале этого года в Emsisoft и на бесплатный сайт ID Ransomware, созданный Майклом Гиллеспи, исследователем безопасности в Emsisoft, было отправлено 137 537 штаммов программ-вымогателей. Основным штаммом, на который приходится 70% заражений, была ориентированная на потребителя программа-вымогатель Stop - также известная как Djvu - программа-вымогатель, которая, по мнению компании по обеспечению безопасности Cyble, «проникает в системы пользователей, когда они загружают и запускают вредоносные файлы, маскируясь под программные взломы или генераторы ключей, которые позволяют пользователи могут бесплатно пользоваться платным программным обеспечением, скачав его с торрента».

За исключением Stop / Djvu, другие популярные штаммы вымогателей, включая Phobos, REvil / Sodinokibi, QLocker, Makop и Dharma, в основном ориентированы на бизнес.Но из топ-10 Q2 только REvil / Sodinokibi и LockBit имеют сайты утечки данных.

Средство - это сообщение

Сайты утечки данных - еще одна тактика, созданная злоумышленниками, чтобы заставить жертв как можно скорее заплатить. Многие записки о выкупе, оставленные злоумышленниками в системах, которые они зашифровали, например, будут отображать таймер обратного отсчета и предупреждать жертву о том, что, например, у них есть только 48 часов, чтобы заплатить выкуп, иначе требование

выкупа удвоится. Эксперты говорят, что некоторые жертвы платят исключительно ради репутации, чтобы попытаться не допустить обнародования атаки.

Для жертв, которые не платят быстро, многие операции с программами-вымогателями в следующий раз публикуют имя жертвы на своем специальном сайте утечки данных, чтобы попытаться назвать и заставить их заплатить, обещая, что, если они отправят выкуп, их имя будет удалено, предоставляется дешифратор, и все данные, украденные злоумышленниками, удаляются.

Если этот шаг не приведет к тому, что жертва заплатит, злоумышленники часто начнут утечку украденных данных, если им удалось их получить во время атаки. Тем самым они посылают сигнал будущим жертвам, что, если они решат не платить, их постигнет такая же участь.

Предостережение плательщика выкупа

Однако многие из этих вымогательств меньше, чем кажутся .Например, многие злоумышленники утверждают, что украли данные, но в конечном итоге не получают ничего ценного, что могло бы быть утечкой. Другие просто лгут, когда заявляют, что украли данные.

Еще одна загвоздка: в некоторых случаях дешифраторы не работают так, как рекламируется, в результате чего жертвы не могут использовать их, чтобы легко или быстро восстановить свои данные.

Это одна из причин, по которой эксперты по реагированию на программы-вымогатели рекомендуют, чтобы организация всегда работала с авторитетной фирмой по реагированию на инциденты с программами-вымогателями, если они рассматривают возможность выплаты выкупа. Такие фирмы могут направлять реакцию жертвы, основываясь на информации о том, как данный набор злоумышленников имеет тенденцию к переговорам и вероятности того, что жертва получит рабочий дешифратор, или, возможно, привлечь стороннюю службу для перезаписи дешифратора, как только жертва получит ключ.

Некоторые операции с программами-вымогателями предупреждают, что любая жертва, которая попытается работать с полицией или сторонней фирмой по реагированию, будет наказана утечкой украденных данных или удалением ключа дешифрования, что не позволит им восстановить какие-либо данные. Но эксперты по безопасности цитируют такие любительские угрозы как доказательство того, что жертвы должны делать противоположное тому, что могут требовать злоумышленники, и помогать раскрывать свои атаки, не в последнюю очередь для того, чтобы полиция могла лучше отслеживать и пресекать их. Для нынешних и будущих жертв программ-вымогателей молчание - не золото». ***(Mathew J. Schwartz. Ransomware: No Decline in Victims Posted to Data Leak Sites // Information Security Media Group, Corp. (https://www.govinfosecurity.com/ransomware-no-decline-in-victims-posted-to-data-leak-sites-a-17719). 12.10.2021).***

***

«Исследователи безопасности, взломавшие шифрование вредоносного ПО для криптоблокировки, выпустили бесплатный дешифратор для вымогателя BlackByte.

Trustwave, чикагский поставщик услуг кибербезопасности и управляемой безопасности, принадлежащий сингапурской телекоммуникационной компании Singtel Group Enterprise, в пятницу объявил о выпуске бесплатного дешифратора, доступного для загрузки с GitHub.

Фирма заявляет, что получила образец вредоносного ПО, который она проанализировала в рамках цифровой криминалистической экспертизы и реагирования на инциденты. Компания отказалась сообщить какие-либо подробности о жертве, например, сектор или географию, в которых она работает, и заявила, что также неясно, как жертва была изначально заражена.

К сожалению, основная проблема шифрования в BlackByte, вероятно, уже решается разработчиком вредоносного ПО, говорит Карл Сиглер, старший менеджер по исследованиям в области безопасности Trustwave SpiderLabs.

«Информационная безопасность всегда была и всегда будет игрой в кошки-мышки между хорошими парнями и злоумышленниками», - сказал он Information Security Media Group. «В этом конкретном случае, однако, похоже, что участники BlackByte осознали слабость в своем механизме шифрования и уже отключили ключ еще до того, как был выпущен наш анализ или дешифратор. Перевыпустить».

Слабое шифрование в вредоносном ПО

Но этот недостаток означает, что любой, кто был поражен версией вредоносной программы, содержащей уязвимость шифрования, должен иметь возможность бесплатно расшифровать свои файлы.

«Исходя из того, что ключ шифрования отключен, эта конкретная версия, скорее всего, мертва для всех намерений и целей», - говорит Сиглер.«Мы активно отслеживаем, пересматривается ли семейство программ-вымогателей или возрождается для новой кампании. Злоумышленники обычно переоснащают свое оружие-вымогатель вместо того, чтобы создавать совершенно новое».

Trustwave заявляет, что не пыталась связаться с предполагаемыми жертвами BlackByte.

«Мы не связались ни с одной из предполагаемых жертв, и у нас нет никаких сведений о том, кто мог пострадать от этой программы-вымогателя, помимо организации, которая взаимодействовала с нашей группой цифровой криминалистики и реагирования на инциденты для дальнейшего расследования программы-вымогателя», - говорит Сиглер.«Мы надеемся, что, опубликовав подробный анализ программ-вымогателей и средства дешифрования, мы сможем помочь организациям, правоохранительным органам и другим охранным фирмам понять угрозу и сами предпринять необходимые меры предосторожности».

BlackByte: не крупный игрок

Большинство разработчиков программ-вымогателей сегодня проводят операции «программа-вымогатель как услуга», в ходе которых онинанимают партнеров для заражения жертв своим вредоносным ПО, а затем обещают делиться выручкой всякий раз, когда жертва платит.

Эксперты по безопасности говорят, что крупнейшие и наиболее продвинутые операции с программами-вымогателями, которые часто преследуют цель охоты за крупными играми, то есть нацелены на крупные организации в поисках более крупных выкупов, включают BlackMatter, ранее известную как DarkSide; Конти;

LockBit; и REvil, он же Sodinokibi; и Рюк.BlackByte, однако, не выглядит крупным игроком, по крайней мере, пока.

Чтобы попытаться заставить жертв заплатить, многие операции с программами-вымогателями запускают специальные сайты утечки данных, доступные только через анонимную сеть Tor. Например, с 4 октября израильская компания по разведке угроз Kela сообщает, что эти 12 групп программ-вымогателей перечислили новых жертв на своих сайтах утечки данных: AtomSilo, Avos, BlackByte, BlackMatter, Conti, Grief, Hive, LockBit, Pysa, REvil / Sodinokibi, Призрак, Порочное общество и Син. Однако многие другие программы-вымогатели, включая Ryuk, не запускают сайты утечки данных.

Список новых жертв BlackByte

BlackByte, похоже, недавно изменил дизайн своего сайта утечки данных.Ранее на сайте были указаны жертвы и ссылка для загрузки образцов украденных файлов, «но сама программа-вымогатель не имеет функции кражи», - отмечает Trustwave в техническом анализе. «Это просто, наверное, чтобы напугать своих жертв?»

Последними жертвами, размещенными на сайте BlackByte и появившимися соответственно в пятницу и четверг, были американская фирма по установке систем пожарной сигнализации и спринклерных систем, а также американский производитель одноразовых продуктов для борьбы с инфекциями для сектора здравоохранения.

По состоянию на пятницу таймеры обратного отсчета для жертв, соответственно, указывали 28 и 27 дней как оставшиеся для выплаты неуказанной суммы выкупа. В обоих случаях ссылка «скачать бесплатно» вела к службе анонимной загрузки файлов Anonfile, в которой для каждого из них размещался файл размером менее 5 МБ, содержащий предположительно украденные данные.

Неясно, когда предполагаемые жертвы были поражены программой-вымогателем и могла ли это быть свежая версия, которая исправила недостатки шифрования, обнаруженные Trustwave - и, возможно, другими.

С точки зрения времени злоумышленники обычно используют свои сайты утечки данных, чтобы попытаться назвать жертву и заставить их заплатить через несколько дней или недель после того, как жертва отклонит их первоначальные требования.

Но неясно, является ли какая-либо из предположительно украденной информации конфиденциальной или была получена злоумышленниками с помощью каких-либо передовых методов взлома.

«Извлеченные файлы показались исследователям Trustwave блефом, поскольку BlackByte не имеет функции эксфильтрации», - говорит Сиглер. Если так, то это вряд ли будет первый случай, когда злоумышленники, использующие программы-вымогатели, лгали о краже конфиденциальных данных.

«Если злоумышленники каким-то образом получили файлы от каких-либо жертв, это было сделано через какой-то другой канал или потенциально было захвачено во время первоначального взлома как отдельная задача», - говорит он.

Технический анализ

Согласно техническому анализу версии BlackByte, полученному Trustwave, вредоносная программа попадает в систему с помощью файла запуска JavaScript.

Файл является частью процесса, предназначенного для декодирования и запуска вредоносной полезной нагрузки, которая представляет собой файл.NET DLL, предназначенный для обхода интерфейса сканирования Microsoft Antimalware и подготовки системы к принудительному шифрованию большинства файлов. Trustwave сообщает, что вредоносная программа также может изменять параметры реестра для повышения привилегий, идентифицировать другие системы через Active Directory и монтировать внешние диски.

По словам Сиглера, для этой похожей на червя возможности «эта вредоносная программа не требует доступа к Active Directory с правами администратора».«Вместо этого он использует обычную технику« передачи хэша»с использованием локального ключа реестра LocalAccountTokenFilterPolicy для получения доступа к локальному администратору. Затем он использует этот расширенный локальный доступ для сети и перечисления общих ресурсов».

Для систем, идентифицированных через Active Directory, вредоносная программа может отправлять«волшебный пакет», который выполняет команду пробуждения по локальной сети, которая пробуждает автономные устройства, чтобы их можно было зашифровать.

Однако, как и многие другие типы программ-вымогателей, Trustwave сообщает, что BlackByte сначала проверяет язык системы по умолчанию, чтобы узнать, находится ли устройство в Армении, Азербайджане, Беларуси, Грузии, Казахстане, России, Таджикистане, Туркменистане, Украине или Узбекистане.Если это так, вредоносная программа закрывается.

Эксперты по безопасности говорят, что большинство операторов программ-вымогателей, похоже, говорят по-русски и будут избегать атак на цели в России или других странах, которые были частью Советского Союза, чтобы избежать репрессалий со стороны местных правоохранительных органов.

В случае продолжающихся заражений Trustwave сообщает, что анализируемая им версия BlackByte будет загружать предполагаемый файл изображения PNG с внешнего сервера, который содержит информацию, необходимую программе-вымогателю для генерации ключа и шифрования файлов. «Если программе-вымогателю не удастся загрузить ключ, она выйдет из строя и спасет зараженную систему от шифрования файлов», - говорится в сообщении. В противном случае программа-вымогатель начинает перечислять диски для шифрования, по его словам, используя «алгоритм с симметричным ключом AES», полученный из файла изображения PNG.

Требуемый PNG-файл больше не находится в сети, сообщает Trustwave, что подтверждает его анализ: разработчики BlackByte, вероятно, уже заметили слабое шифрование и готовят новую версию своей программы-вымогателя». ***(Mathew J. Schwartz. BlackByte: Free Decryptor Released for Ransomware Strain// Information Security Media Group, Corp.(https://www.govinfosecurity.com/blackbyte-free-decryptor-released-for-ransomware-strain-a-17738). 15.10.2021).***

***

«Sinclair Broadcast Group, Inc., которая владеет или управляет 186 телевизионными станциями на 87 рынках США, подверглась атаке программы-вымогателя, которая нарушила работу, включая рекламу, некоторые выпуски новостей и программы.

В объявлении компания подтверждает, что 16 октября обнаружила инцидент с безопасностью, а на следующий день определила, что определенные серверы и рабочие станции в ее среде были зашифрованы с помощью программы-вымогателя. В нем говорится, что в результате атаки были нарушены некоторые офисные и операционные сети. Компания также подтверждает, что данные были перекачаны из ее сети, хотя она работает над определением типа и серьезности потери.

Sinclair Broadcast Group также раскрыла инцидент в форме 8-KКомиссии по ценным бумагам и биржам США, которая используется для информирования акционеров о значимых крупных событиях.

Sinclair, базирующийся за пределами Балтимора, штат Мэриленд, сообщил о выручке почти в 6 миллиардов долларов в 2020 году и связан с Fox, ABC, CBS, NBC и The CW. В его предложениях также 21 региональная спортивная сеть. По данным Baltimore Sun, Sinclair Broadcast Group охватывает примерно 40% домохозяйств США.

Текущее расследование

Объявляя об атаке в понедельник, компания пишет: «Сразу после обнаружения события безопасности высшее руководство было уведомлено, и компания выполнила свой план реагирования на инцидент, приняла меры по сдерживанию инцидента и начала расследование».

Медиакомпания сообщает, что были задействованы юрисконсульт, судебно-экспертная фирма по кибербезопасности и другие специалисты по реагированию на инциденты. Компания также уведомила правоохранительные и другие государственные органы, говорится в сообщении. Соответствующие расследования «продолжаются».

В заявлении, распространенном для Information Security Media Group, представитель Sinclair Broadcast Group не сообщил подробностей об атаке или продолжающемся сбое, но подтвердил: «Мы внедрили наши протоколы реагирования на инциденты и обеспечения непрерывности бизнеса, приняли меры по сдерживанию инцидента и запустили Была привлечена фирма по кибербезопасности, которая оказывала помощь другим компаниям в аналогичных обстоятельствах.

«Мы усердно работаем над устранением инцидента и быстрым и безопасным восстановлением операций. Работая над завершением расследования, мы будем искать возможности для усиления наших существующих мер безопасности».

Представитель не указал, заплатила ли Sinclair Broadcast Group или собирается ли заплатить какой-либо выкуп, потребованный хакерами для расшифровки систем.

Джон Бамбенек, главный специалист по поиску угроз в охранной фирме Netenrich, говорит ISMG: «Взаимосвязь Sinclair с местными станциями выбила из эфира некоторые станции, показывая, что риски цепочки поставок по-прежнему значительны. И снова у нас есть еще один пример того, насколько хрупкими. наша

технология может применяться тогда, когда высококвалифицированные злоумышленники преследуют цели, вероятно, с небольшим количеством ресурсов безопасности».

«Нарушение бизнеса»

В своем заявлении компания сообщает, что «событие вызвало - и может продолжать вызывать - нарушение части бизнеса компании», включая доставку местной рекламы.

Sinclair также заявляет, что его расследование находится на ранней стадии, и поэтому оно не может определить, «окажет ли событие существенное влияние на его бизнес, операции или финансовые результаты».

Согласно отраслевому изданию FTVLive, медиакомпания также пережила киберинцидент в июле и, как сообщается, приказала своим станциям изменить свои системные пароли.

Широко распространенные сбои

Контент Sinclair Broadcast Group доставляется через несколько платформ, включая эфирные, многоканальные дистрибьюторы видеопрограмм, а также цифровые и потоковые платформы.

Согласно ранним сообщениям, злоумышленники, как сообщается, могли использовать корпоративный домен Active Directory компании, базу данных и набор служб, управляющих пользователями и сетевыми устройствами. По сообщениям BleepingComputer, атака достигла систем телевещания Sinclair и вызвала отключение как ее бизнеса, так и дочерних компаний.

Сообщается, что при отключенных корпоративных активах некоторые телеканалы прибегали к использованию Gmail для полевых новостных советов и PowerPoint для экранной графики. Согласно сообщениям и сообщениям в социальных сетях, другие транслировали шоу по выходным через Facebook Live.

Более того, на некоторых рынках США трансляции НФЛ были прерваны инцидентом - игры, как сообщается, переключаются на другое программирование, включая боулинг.

ВТвиттере один пользователь пожаловался на путаницу, написав: «Я не знаю, @hulu или @ FOX42KPTM, но боулинг Криса Пола и Ганнибала Буресса - это не игра «упаковщики-медведи»».

Отправив ответ в Твиттере,Hulu признал: «Приносимизвинения за проблемы! Проблема с каналами с некоторых местных станций, в настоящее время расследуется».

По данным издания The Record, радиостанции от Восточного побережья до Техаса сообщили о технических проблемах в воскресенье.

Устранение угрозы

Об этом инциденте Оливер Таваколи, технический директор охранной фирмы Vectra, добавляет: «Отключение медиа-компаний, таких как Sinclair Broadcasting, безусловно, более заметно, чем компрометация операций мясоперерабатывающего предприятия, такого как JBS Holdings. Обратите внимание, что медиа-компании, такие как Sinclair, используют изрядное количество специализированного Интернета вещей, включая камеры, микрофоны [и] вещательное оборудование, в

которые были внесены отдельные исправления и которые могут затруднить восстановление работы».

Билл Лоуренс, бывший инструктор по кибербезопасности в Военно-морской академии США, а в настоящее время - директор по информационной безопасности в компании SecurityGate, говорит ISMG: «Каким-то образом атака не распространилась на широковещательную систему «главного управления» Синклера, поэтому, если это была сегментация сети или более высокая уровень защиты и заботы о «жемчужинах короны» - вот хорошие практики, которым стоит подражать ».

Кейн МакГлэдри, член консультативного совета Technology Alliance Group NW и стратег кибербезопасности компании Ascent Solutions, говорит, что как только инцидент будет разрешен, Синклер «должен провести внутреннюю горячую промывку», чтобы определить извлеченные уроки, что позволит им укрепить техническую защиту и обновить / проверить свой план реагирования на инциденты.

Однако в этих случаях Бамбенек из Netenrich добавляет: «[Но] до тех пор, пока правительства не найдут способ привлечь к ответственности операторов программ-вымогателей, мы будем продолжать видеть подобные истории».

Атака Sinclair выпала на год, очень загруженный программами-вымогателями - с такими же разрушительными ударами по Colonial Pipeline, которые временно отключили подачу топлива на Восточное побережье; наряду с инцидентами с поставщиком мяса JBS USA и поставщиком управляемых услуг Kaseya, атака, которая в конечном итоге затронула 1500 дочерних организаций в праздничные дни четвертого июля.

В ответ на этот всплеск правительство США заявило, что оно применяет «общегосударственный», а точнее «общенациональный» подход к сдерживанию программ-вымогателей, включая попытки вывести из строя его финансовую инфраструктуру - например, использование криптовалют и связанные с ними услуги по отмыванию денег. Кроме того, в прошлом месяце министерство финансов США наложило санкции на базирующуюся в России криптовалютную биржу Suex - первое такое обозначение - за якобы помощь участникам программы-вымогателя.

А на прошлой неделе Совет национальной безопасности Белого дома организовал двухдневный саммит 30 стран по борьбе с программами-вымогателями, заявив, что был достигнут прогресс в идентификации этих атак как глобальной угрозы безопасности». ***(Dan Gunderman. Sinclair TV Stations Targeted in Weekend Ransomware Attack // Information Security Media Group, Corp. (https://www.govinfosecurity.com/sinclair-tv-stations-targeted-in-weekend-ransomware-attack-a-17753). 18.10.2021).***

***

«Компания Ermetic, занимающаяся облачной безопасностью, обнаружила, что почти все предприятия имеют идентификационные данные, которые в случае взлома подвергают риску большую часть их корзин S3.

Исследователи обнаружили, что на основе «токсичного сочетания чрезмерно привилегированных идентификаторов и плохо настроенных сред» 90% корзин S3

во всех протестированных ими учетных записях AWS были уязвимы для атак программ-вымогателей.

В отрезвляющем отчете сделан вывод, что вопрос был не в том, «если», а в том, «когда» произойдет массовая атака программ-вымогателей на облачную платформу AWS.

Токсичные комбинации в аккаунтах AWS подвергают большинство корзин S3 атакам программ-вымогателей.

Исследование Ermetic показало, что почти половина (45%) всех учетных записей AWS имеют сторонние удостоверения, которые могут выполнять атаки программ-вымогателей, повышая свои привилегии до уровня администратора.

Кроме того, они обнаружили, что более чем в 70% сред были машины с уязвимыми идентификаторами, публично открытыми для доступа в Интернет.

По словам исследователей, пользователи IAM, подверженные указанным выше угрозам, имели ключи доступа без ротации в течение как минимум 90 дней в 95% сред.

Исследователи также сообщили, что более чем в трех четвертях (80%) сред пользователи IAM с активированными ключами доступа неактивны в течение как минимум 180 дней. Кроме того, у этих ключей доступа были разрешения, которые позволяли им выполнять атаки программ-вымогателей.

Кроме того, в шести из десяти (60%) протестированных сред были пользователи IAM с консольным доступом без многофакторной аутентификации (MFA).

Согласно отчету, 96% сред с неактивными ролями пользователей и 80% сред с неактивными пользователями IAM были уязвимы для вышеуказанных факторов риска.

Исследователи также отметили, что в их исследовании анализировались только сценарии «разбей и захвати» с использованием одной скомпрометированной личности. Однако целевые кампании обычно ставят под угрозу несколько идентификаторов и используют их комбинированные разрешения, тем самым усугубляя факторы риска для успешной атаки программы-вымогателя.

«Очень немногие компании осведомлены о том, что данные, хранящиеся в облачных инфраструктурах, таких как AWS, подвержены риску атак программ-вымогателей, поэтому мы провели это исследование, чтобы выяснить, насколько часто существуют подходящие условия для компрометации корзин Amazon S3», - сказал генеральный директор Ermetic Шай Мораг.«Мы обнаружили, что в каждой проверенной нами учетной записи почти все сегменты S3 организации были уязвимы для программ-вымогателей. Таким образом, мы можем сделать вывод, что дело не в том, если, а в том, когда произойдет крупная атака программ-вымогателей на AWS ».

Защита корзин S3 от атак программ-вымогателей

Исследователи отметили, что, несмотря на повышенный риск атак программ-вымогателей на корзины S3, организации могут предпринять различные шаги для защиты своих учетных записей AWS и улучшения общей безопасности облака.

Они рекомендовали стратегию доступа «с наименьшими привилегиями», чтобы исключить наиболее опасные комбинации, необходимые для компрометации корзин S3 в уязвимых учетных записях AWS. Эта стратегия включает в себя назначение «минимума разрешений», необходимых пользователям IAM для выполнения своей работы. Это также включает в себя отказ от конфиденциальных действий, приватизацию всех общедоступных сегментов S3, разделение обязанностей и удаление неактивных ролей и неактивных пользователей из их учетных записей AWS.

Другие предложения включают удаление факторов риска (ротацию ключей доступа, включение MFA и отключение неиспользуемых учетных данных), ведение журнала и мониторинг, предотвращение удаления и репликацию корзины.

«В этом отчете подчеркивается насущная необходимость« обнаруживать угрозы »в облаке, а не просто сосредотачиваться на неправильной конфигурации», - говорит Саумитра Дас, технический директор и соучредитель Blue Hexagon.«Исследование Cloud Security Alliance показывает, что даже если в корзинах S3 обнаруживаются неправильные конфигурации или ключи доступа IAM не используются в течение длительного времени, их обнаружение и устранение занимает некоторое время - иногда дни, недели и даже месяцы».

Дас отметил, что невозможно гарантировать безопасность всех аккаунтов AWS. Однако риск утечки, разрешительной или устаревшей информации может быть уменьшен». ***(ALICIA HOPE. Study Shows Virtually All AWS Accounts Have Vulnerable Identities Exposing 90% Of S3 Buckets To Potential Ransomware Attacks // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/study-shows-virtually-all-aws-accounts-have-vulnerable-identities-exposing-90-of-s3-buckets-to-potential-ransomware-attacks/). 18.10.2021).***

***

«Агентство по кибербезопасности и безопасности инфраструктуры (CISA), Федеральное бюро расследований (ФБР) и Агентство национальной безопасности (АНБ) опубликовали сегодня рекомендации по кибербезопасности в отношении кибер-вторжений программ-вымогателей BlackMatter, нацеленных на несколько критически важных инфраструктурных объектов США, в том числе два американских предприятия пищевой промышленности и сельского хозяйства. отраслевые организации. Консультации включают технические подробности, анализ и оценку этой киберугрозы, а также несколько действий по смягчению, которые могут быть предприняты для снижения риска для этой программы-вымогателя.

Впервые появившись в июле 2021 года, кибер-акторы использовали BlackMatter со встроенными, ранее скомпрометированными учетными данными, которые позволяли им получать доступ к сети и удаленно шифровать хосты и общие диски. Когда субъекты находили хранилища резервных данных и устройства в сети, а не хранятся вне офиса, они стирали или переформатировали данные. BlackMatter - это программа-вымогатель как услуга (Raas), что означает, что разработчики могут получать прибыль от аффилированных лиц киберпреступников (то есть субъектов BlackMatter), которые его развертывают.

«Этот совет подчеркивает эволюционирующий и устойчивый характер киберпреступников и необходимость коллективного государственного и частного подхода к снижению воздействия и распространенности атак программ-вымогателей», - сказал Эрик Голдштейн, исполнительный помощник директора по кибербезопасности, CISA.«CISA, ФБР и АНБ делают все возможное, чтобы усложнить работу киберпреступников. Американцы могут помочь нам в этом долгосрочном начинании, посетив Stopransomware.gov, чтобы узнать, как снизить риск стать жертвой программ-вымогателей ».

«ФБР, наряду с CISA и NSA, занимается предотвращением, разрушением и борьбой с развивающейся угрозой вымогателей, - сказал Брайан Ворндран, помощник директора Cyber Dvision ФБР.«К сожалению, о слишком многих инцидентах с программами-вымогателями не сообщается, и поскольку молчание приносит наибольшую пользу киберпреступникам, мы просим целевые организации связаться с их местным полевым офисом ФБР и поговорить с киберагентом. Сообщая о киберинцидентах, целевые организации расширяют наши возможности реагировать и расследовать с целью срыва киберпреступных операций. Мы продолжим использовать наши уникальные полномочия и возможности для защиты американского народа от этой угрозы; однако мы не можем добиться этого в одиночку.

«Угроза программ-вымогателей выходит за рамки конкретных последствий для компании-жертвы - она переросла в проблему национальной безопасности», - сказал Роб Джойс, директор по кибербезопасности АНБ. «Технические навыки и анализ угроз АНБ будут и впредь поддерживать наших партнеров в правительстве и отрасли, чтобы ослабить плацдарм злоумышленников в сетях, где они запускают программы-вымогатели. Использование мер по снижению рисков в совместном консультативном заключении с CISA и ФБР защитит сети и снизит риск от атак BlackMatter и других программ-вымогателей ».

CISA, ФБР и АНБ едины во мнении, что подчеркивают ценность и важность для организаций применения передовых методов защиты своих сетей, систем и данных, таких как (1) внедрение и обеспечение выполнения процедур резервного копирования;(2) Используйте надежные уникальные пароли;(3) Используйте многофакторную аутентификацию; и (4) реализовать сегментацию сети и мониторинг обхода. Всем организациям, стремящимся защитить свои сети от атак программ-вымогателей и обеспечить отказоустойчивость своих систем, следует ознакомиться с совместными рекомендациями по всему спектру рекомендуемых мер защиты.В этот совет также включены сигнатуры обнаружения, которые могут использоваться для обнаружения сетевой активности, связанной с активностью BlackMatter.

Этот совет включает анализ образца программы-вымогателя BlackMatter и информацию от доверенных третьих лиц. Поведение злоумышленников сопоставлено со структурой MITER ATT & CK, общим лексиконом злоумышленников, рекомендованным CISA». ***(CISA, FBI, AND NSA RELEASE BLACKMATTER RANSOMWARE ADVISORY TO HELP ORGANIZATIONS REDUCE RISK OF ATTACK // Cybersecurity and Infrastructure Security Agency***

(CISA) (https://www.cisa.gov/news/2021/10/18/cisa-fbi-and-nsa-release-blackmatter-ransomware-advisory-help-organizations-reduce). 18.10.2021).

***

«Крупная операция вымогателя не позволила заработать миллионы долларов после того, как исследователи кибербезопасности обнаружили недостаток в программе-вымогателе, которая позволяла восстанавливать зашифрованные файлы без выплаты выкупа киберпреступникам.

Исследователи кибербезопасности из Emsisoft подробно рассказали, как им удалось тайно помешать киберпреступникам, стоящим за вымогателем BlackMatter, избавив нескольких жертв от необходимости платить выкуп.

Сохранив то, что они делали в секрете, чтобы избежать обнаружения киберпреступниками, исследователи теперь раскрыли, как они подрывали BlackMatter, предоставляя ключи дешифрования жертвам своих атак.

BlackMatter в своем текущем воплощении активен с июля этого года, но на самом деле существует гораздо дольше, потому что аналитики информационной безопасности сходятся во мнении, что BlackMatter – это измененная версия программы-вымогателя DarkSide.

Ранее в этом году DarkSidestал известен как виновника так и вымогателей Colonial Pipeline. Инцидент привел к нехватке газа и топлива на северо-восточном побережье США, в то время как преступники ушли с миллионами долларов, когда Colonial заплатила выкуп.

Но последствия атаки не остались незамеченными, и вскоре после того, как Белый дом пообещал принять меры против виновных, DarkSide потеряла контроль над частью своей критически важной инфраструктуры, анекоторые из их биткойн-кошельков были конфискованы. После этого группа, казалось, померкла.

Однако вскоре DarkSide снова превратился в BlackMatter, и киберпреступники, стоящие за ним, похоже, не оттолкнули себя, оказавшись в поле зрения правительства США. Ониначали серию атак с использованием программ-вымогателей против компаний в Северной Америке.

В сообщениях BlackMatter на подпольных форумах, предлагающих купить доступ к взломанным сетям в США, Канаде, Великобритании и Австралии, утверждалось, что BlackMatter не пойдет против больниц или государственных учреждений. Но это было неправдой, и в дополнение к критически важной инфраструктуре в виденескольких сельскохозяйственных компанийгруппа также нанесла удар по центрам анализа крови.

«Заявление банды о том, что атаки на критически важную инфраструктуру и некоторые другие сектора были пустыми: она атаковала те самые организации, которые, по ее словам, не будет», - сказал ZDNet Бретт Кэллоу, аналитик угроз Emsisoft.

«Так почему они вообще сделали это требование? Возможно, это была попытка избежать немедленного привлечения внимания правоохранительных органов после инцидента с колониальным трубопроводом или, возможно, они считали, что компании будут более склонны к переговорам если бы они не оказались головорезами, напавшими на больницы ».

В декабре прошлого года исследователи Emsisoft заметили ошибку, допущенную операторами DarkSide, которая позволила расшифровать данные, зашифрованные версией вымогателя для Windows, без необходимости уплаты выкупа, хотя преступники исправили ее в январе.

Однако выясняется, что группа вымогателей снова совершила аналогичную ошибку при ребрендинге, и исследователи обнаружили недостаток в полезной нагрузке программы-вымогателя BlackMatter, которая позволяла жертвам восстанавливать файлы, не платя выкуп.

После обнаружения второй уязвимости Emsisoft вместе с другими работала над тем, чтобы предоставить как можно большему количеству жертв BlackMatter ключ дешифрования, прежде чем они заплатят выкуп, что не позволило киберпреступникам присвоить десятки миллионов долларов.

К сожалению, BlackMatter в конце концов выяснил, что что-то не так, и закрыл лазейку.

«BlackMatter, вероятно, заподозрила, что что-то пошло не так, когда их доход начал падать, и становился все более подозрительным, чем дольше это продолжалось. К сожалению, банды неизбежно поймут, что у них проблемы в таких ситуациях. Все, что мы можем сделать, это работать быстро и незаметно, чтобы помочь как можно большему количеству жертв, пока есть возможности, - сказал Кэллоу.

«Эти усилия демонстрируют важность сотрудничества государственного и частного секторов. Работая вместе, мы можем значительно снизить прибыльность киберпреступности, а это ключевой элемент в борьбе с проблемой программ-вымогателей», - добавил он.

Программы-вымогатели остаются серьезной проблемой информационной безопасности, и лучший способ избежать реакции на атаку - это вообще не стать жертвой. Стратегии кибербезопасности, такие как своевременное применение исправлений безопасности, обеспечение применения многофакторной аутентификации во всей сети и предоставление пользователям только необходимого доступа - например, не давая привилегий администратора людям, которые в них не нуждаются - - все это может помочь предотвратить атаки программ-вымогателей.

Что касается BlackMatter, вполне вероятно, что они продолжат дело, но их ошибки могли нанести ущерб их репутации в киберпреступных кругах.

«Я не удивлюсь, если операторы откажутся от названия BlackMatter и проведут ребрендинг. Их репутация будет в унитазе. Их повторные ошибки стоили филиалам денег. Очень много денег», - сказал Кэллоу». ***(Danny Palmer. These ransomware criminals lost millions of dollars in payments when researchers secretly found mistakes in their code // ZDNet (https://www.zdnet.com/article/cybersecurity-researchers-secretly-cost-ransomware-criminals-millions-of-dollars-after-finding-mistakes-in-their-code/). 26.10.2021).***

***

«Одна из крупнейших инженерных фирм Шотландии пострадала от взлома ее ИТ-систем, что обошлось ей в миллионы фунтов стерлингов.

Атака программ-вымогателей на Weir, базирующуюся в Глазго, произошла в прошлом месяце, что вынудило ее прекратить некоторые операции.

В заявлении компании по добыче оборудования говорится, что она быстро отреагировала на «изощренную» атаку, но была вынуждена отложить поставки на сумму более 50 миллионов фунтов стерлингов.

По его оценкам, инцидент может стоить до 5 миллионов фунтов стерлингов.

Вейр сказал, что нет никаких доказательств того, что какие-либо личные или другие конфиденциальные данные были «извлечены или зашифрованы».

Он также сообщил, что не вступал в контакт с хакерами и продолжает поддерживать связь с регулирующими органами и «соответствующими разведывательными службами» по поводу инцидента.

'Изощренная атака'

Генеральный директор Джон Стэнтон сказал: «Мы быстро и всесторонне отреагировали на изощренную внешнюю атаку на наш бизнес.

«Активные меры по защите нашей инфраструктуры и данных привели к значительным временным сбоям в работе, но наши команды великолепно отреагировали на этот вызов и сумели свести к минимуму воздействие на наших клиентов.

«Мы продолжим уделять особое внимание безопасному восстановлению всех наших систем, одновременно повышая нашу устойчивость в будущем».

Компания заявила, что после атаки она приняла ряд мер, таких как изоляция и отключение ИТ-систем, включая инженерные приложения.

В своем заявлении говорится: «Эти приложения сейчас восстанавливаются частично, а другие приложения возвращаются в оперативный режим постепенно в порядке приоритета бизнеса.

Вышеупомянутые действия привели к ряду текущих, но временных сбоев, включая изменение этапов проектирования, производства и отгрузки, что привело к отсрочке выручки и недопоставке накладных расходов.

«Эффективные возможности постепенно восстанавливаются в ближайшие недели, но ожидается, что последствия операционных сбоев и связанной с ними неэффективности сохранятся и в четвертом квартале». ***(Engineering firm Weir hit by major ransomware attack // BBC (https://www.bbc.com/news/uk-scotland-scotland-business-58801753). 08.10.2021).***

***

«Да, безопасность - это сложно - никто никогда не застрахован на 100 процентов от скрытых угроз. Но как получается, что компании - большие компании - снова и снова становятся жертвами атак программ-вымогателей? Почему мы не стали лучше предотвращать их?

Давайте рассмотрим основные причины этого, начав с некоторых основ, прежде чем углубляться в детали:

2FA лаги

Ошибка пользователя никогда не исчезнет

Устаревший AV

Задержки обнаружения и ответа

Обнаружение «жизни за пределами земли» не удается

Cobalt Strike и другие легальные инструменты перепрофилированы

Сотрудничество в сфере киберпреступности - это мастер-класс

Провал государственной политики и геополитические проблемы

Криптовалютное топливо

2FA не применяется повсеместно

Двухфакторная аутентификация (2FA), вероятно, является самым простым улучшением безопасности, которое может реализовать организация, и одним из наиболее популярных решений профессионалов в области информационной безопасности. Несмотря на это, мы по-прежнему наблюдаем такие нарушения, как Colonial Pipeline, потому что организации либо не смогли реализовать 2FA, либо не смогли реализовать его полностью.

Для всего, что требует имени пользователя и пароля для доступа, должна быть включена двухфакторная аутентификация. Это означает электронную почту, бизнес-приложения, облачные развертывания, виртуальные частные сети - все, что требует учетных данных.

Ошибки пользователей никогда не прекратятся - зачем притворяться иначе?

Современные методы фишинга настолько развиты, что их жертвами становятся даже специалисты, практикующие информационную безопасность, так как же можно ожидать, что средний пользователь будет работать лучше?

Злоумышленники проводят разведку своих целей и настраивают свои методы для достижения успеха. И рабочие процессы многих сотрудников - это буквально пример того, на что нацелены фишинговые атаки. В конце концов, как можно ожидать, что Пэт в бухгалтерском учете, чья работа заключается в открытии PDF-файлов и обработке заказов на поставку, узнает на месте, какой PDF-файл безопасен, а какой может содержать вредоносное ПО?

Мы возлагаем на пользователей нереалистичные ожидания, а затем удивляемся и обвиняем их, когда они совершают ту же ошибку, которую сделали сами многие профессионалы в области информационной безопасности. Дейв Эйтел попал в яблочко год назад, когда он утверждал, что сотрудники не могут ожидать не испортить. Сотрудники всегда совершают ошибки, так почему мы делаем вид, что это изменится?

В антивирусных решениях используется простая логика обнаружения

Антивирус, старейшее из существующих программ безопасности, за последние 20 лет прошел долгий путь. Однако многие антивирусные решения по-прежнему полагаются на устаревшие системы на основе сигнатур для обнаружения вредоносного ПО.

Обнаружение вредоносного кода с помощью AV основывается на наличии бинарной подписи кода или хэша файла, и это работает только в том случае, если код не меняется. Переименование функций внутри кода перед его компиляцией или перемещение блоков кода внутри кода может сделать ранее жизнеспособное обнаружение бесполезным.

Традиционный антивирус не «детонирует» вредоносное ПО, то есть запускает код в защищенной песочнице, поэтому, даже если поведение

вредоносного ПО будет идентичным независимо от его сигнатуры, это чрезвычайно сложно обнаружить.

Эта проблема настолько системна, что существуют такие фреймворки, какI nvoke-Obfuscation, чтобы помочь красным командам, а впоследствии и злоумышленникам, обойти антивирусные решения.

Решения EDR / XDR / MDR подвержены задержкам

Множество решений для конечных точек «DR» (обнаружение и реагирование) значительно более надежны, чем антивирус, но у них тоже есть свои ограничения.

Поскольку логика обработки событий конечной точки находится в облаке, это означает, что между возникновением события и его прибытием в консоль администратора может быть задержка от нескольких секунд до нескольких минут. Это делает их уязвимыми для пропуска выполнения программы-вымогателя.

При активации полезной нагрузки вымогателя вся сеть может быть отключена в течение нескольких секунд, а может быть и минут. Операторы программ-вымогателей часто заранее устанавливают фактическую полезную нагрузку программы-вымогателя во всех системах в сети, так что полезная нагрузка выполняется почти одновременно во всех системах в организации и намного быстрее, чем решение аварийного восстановления может обнаружить.

Стоит отметить, что решения DR + AV от одного и того же поставщика часто поставляются с опцией «блокировки», которая может позволить администратору изолировать / поместить в карантин машину при обнаружении вредоносной полезной нагрузки или последовательности действий. Однако на практике эта опция обычно отключена по умолчанию и - из-за опасений по поводу снижения производительности пользователей из-за ложных срабатываний - ее часто оставляют отключенной.

Методы LOLBin труднее обнаружить

Еще одна распространенная причина успеха программ-вымогателей заключается в том, что операторы научились использовать технику, называемую «жизнь за счет наземных двоичных файлов» (LOLBins).

Это обычные инструменты администрирования, как правило, в Microsoft Windows, но они есть во всех современных операционных системах. Эти инструменты преследуют законные, законные цели и используются администраторами каждый день, что чрезвычайно затрудняет обнаружение злонамеренного использования этих инструментов. Например, недавняя утечка пособия группы Conti свидетельствует о сильной зависимости от стандартных инструментов администрирования Windows.

Для антивирусов и решений аварийного восстановления легко отловить специальные инструменты, разработанные участниками, но практически невозможно определить, были ли команды для поиска локальных контроллеров домена и кем являются администраторы домена были выполнены как часть устранения неполадок сетевого подключения или предшествовало боковому перемещению. По этой причине большинство поставщиков DR либо не предупреждают об использовании этих LOLBin, либо предупреждают с низким уровнем серьезности, поскольку эти команды имеют очень высокий уровень

ложных срабатываний при использовании для обнаружения вредоносной активности.

В некоторых случаях инструменты LOLBin могут использоваться для дополнительных функций, которые были добавлены в код, потому что разработчик или заказчик в какой-то момент хотел, чтобы их административные инструменты имели возможность загружать произвольные файлы из Интернета, или сами инструменты могут запускаться вторично. Приложения.

Это сделано для обхода контроля безопасности, называемого списком разрешений приложений. Список разрешений указывает операционной системе не запускать какое-либо программное обеспечение, если оно не подписано цифровой подписью надежного поставщика (Apple, Google, Microsoft и т. Д.).Однако, обманом заставив действительное подписанное приложение открыть ненадежное неподписанное приложение, злоумышленники могут обойти этот контроль безопасности с помощью не более чем приложений по умолчанию, которые являются частью операционной системы.

Свободно доступные наборы инструментов для атак снизили планку для групп программ-вымогателей

У злоумышленников никогда не было лучше с точки зрения свободно доступных инструментов, таких как Metasploit и Mimikatz, или пиратских копий Cobalt Strike.

Независимо от того, нужны ли им наборы инструментов для фишинга, фреймворки обфускации, инструменты начального доступа, инфраструктура управления и контроля (C2), инструменты для злоупотребления учетными данными или даже полезные нагрузки вымогателей с открытым исходным кодом, почти все это можно бесплатно найти на GitHub. Большинство людей полагают, что злоумышленники прячутся в Dark Web, продавая инструменты для биткойнов только самым темным из черных шляп, но это просто неправда.

Отрасль дала возможность профессионалам в области безопасности разрабатывать и выпускать фреймворки для атак, мотивируя это тем, что «защитники должны понимать эту тактику». Но это приукрашивает тот факт, что структуры атаки также помогают атакующим и усложняют защиту обороняющимся.

Хотя это правда, что защитники действительно должны понимать наступательную тактику, на самом деле большинство защитников слишком загружены повседневной работой, чтобы иметь время, чтобы протестировать каждую наступательную структуру, а затем выработать оборонительное руководство.

Большинство этих инструментов атаки хорошо задокументированы в их использовании, но не в их обнаружении. И хотя барьер для проникновения злоумышленника снизился до «можете ли вы использовать Google, GitHub и иметь базовые компьютерные навыки», защитникам остается платить огромные суммы денег за сложные инструменты и устройства, которые могут хорошо работать только в контролируемом тестовом сценарии.

Группы программ-вымогателей сотрудничают лучше, чем отрасль информационной безопасности

Картели программ-вымогателей существуют потому, что они сотрудничают. Фактически, большинство в индустрии безопасности согласны с тем, что злоумышленники на самом деле сотрудничают лучше, чем команды и организации, пытающиеся их остановить.

Распространение работы на несколько преступных группировок усложняет приписывание тактики, методов и процедур (ДТС) какому-либо одному субъекту, может скрыть намерения злоумышленника и позволяет использовать программу-вымогатель как услугу (RaaS). картели ставят приоритетные цели.

Модель распределения прибыли RaaS хорошо работает, чтобы мотивировать этих участников постоянно искать новые цели, перекладывая тяжелую работу на более опытных профессионалов. Этот метод сотрудничества приводит к высокоэффективному разделению труда, при котором преступные группировки получают первоначальный доступ и требуют от своих филиалов выбирать дорогостоящие организации с высоким доходом, которые с большей вероятностью заплатят выкуп, чем небольшая семья. собственный бизнес (хотя последний явно не застрахован).

Как только злоумышленник определит бизнес, на который он повлиял, и стоимость компании, он установит выкуп на сумму, которую жертва может себе позволить. Атака, которая стоит одной компании 10 000 долларов, может стоить другой компании 10 миллионов долларов, и при этом будут использоваться те же инструменты, поток атаки, брокер доступа и полезная нагрузка программы-вымогателя.

Отсутствие скоординированного реагирования и стратегии как в частном, так и в государственном секторах

Программы-вымогатели - не новая угроза, но их становится все проще реализовать, получить деньги и избежать наказания. Большая часть проблемы находится на уровне государственного сектора - в течение многих лет не существовало четкой политики, направления или стратегического планирования того, как федеральное правительство должно реагировать на эти атаки. Мы изо всех сил пытаемся разработать последовательную политику сдерживания, а также ответных мер.

Таким образом, многие компании, которые пострадали, не имеют другого выхода, кроме как заплатить выкуп.

Целенаправленное преследование отдельных лиц правительством США практически не повлияло на преступную деятельность или деятельность национального государства. К тому же координация между государственным и частным секторами остро ощущалась; только недавно он стал более приоритетным.

Геополитическая загадка

Вышеупомянутые проблемы государственной политики усугубляются тем фактом, что банды вымогателей часто действуют в странах за пределами юрисдикции США и без соглашений об экстрадиции США.

Такие страны, как Россия, ясно дали понять, что не будут экстрадировать злоумышленников из своей страны, если это не является частью гораздо более крупной сделки с США (и геополитической стратегии), и не будут предпринимать никаких внутренних правоохранительных действий, если эти субъекты не атакуют

российский бизнес. Это означает, что преступники, по сути, могут действовать беспрепятственно и безнаказанно.

Вот почему большинство программ-вымогателей проверяют наличие русского языка и языков соседних стран, используемых операционной системой, и немедленно, безвредно, самоуничтожаются, если обнаруживают, что работают в системе в стране, где атака может вызвать гнев правительства России.

Геополитические аспекты этой проблемы нетривиальны, если их вообще можно решить. Интернет не имеет границ, и, хотя злоумышленник может решить скрыть свое местоположение и имитировать злоумышленника, базирующегося в России, невозможно с абсолютной уверенностью определить, что атака исходила из российских границ. Это делает традиционные правительственные методы подчинения страны своей воле - такие как санкции, эмбарго, повышение налогов на импорт и т. Д. - невозможным способом навлечь на себя последствия.

Криптовалюта питает всю отрасль

Криптовалюта запомнится по двум причинам: поддержка программ-вымогателей и экспоненциальный рост выбросов CO2. А если серьезно, без надежной экосистемы криптовалюты банды вымогателей просто исчезли бы с голоду.

Криптовалюта подпитывает всю преступную индустрию, поскольку она обеспечивает финансовую основу, которая обходит контролируемую США глобальную финансовую систему, и ее часто трудно отследить (даже несмотря на то, что платежи выкупа часто требуются в биткойнах, они затем переводятся в другую, не отслеживаемую криптовалюту, прежде чем вывод средств) и легко пересекает международные границы.

Хотя министерство финансов США недавно наложило санкции на криптовалютную биржу SUEX за ее предполагаемое участие в преступлениях с использованием программ-вымогателей, это действие - всего лишь капля в море. Эти группы также могут переключаться на разные биржи, требовать прямых транзакций от жертв или переключаться на более сложную отслеживаемую криптовалюту, такую как Monero.

Если правительство США хочет серьезно отнестись к нанесению вреда криминальной индустрии криптовалюты, оно должно нацеливаться на сами не отслеживаемые монеты - санкционируя любой бизнес (криптовалютный или иной), который разрешает эти транзакции и конверсии.

Что делать с угрозой программ-вымогателей

К сожалению, нет серебряной пули, чтобы остановить экзистенциальную угрозу, которую вымогатели представляют для компьютеров, критической инфраструктуры и все более взаимосвязанного мира, в котором мы живем.

Пользователи и организации должны быть всегда бдительными, применять многоуровневые подходы к безопасности и понимаем, что раннее обнаружение и быстрое устранение любого нарушения, независимо от его незначительности, является гораздо более экономичным подходом, чем альтернатива». ***(Nate Warfield. Why is Cybersecurity Failing Against Ransomware?// Threatpost (https://threatpost.com/cybersecurity-failing-ransomware/175637/). 21.10.2021).***

***

«По словам исследователей, преступная группа, известная как TA551, добавила в свой набор треков инструмент Sliver red-teaming - шаг, который может сигнализировать об усилении атак программ-вымогателей.

По словам исследователей Proofpoint, TA551 (также известный как Shathak) наращивает кибератаки, которые начинаются с перехвата цепочки сообщений электронной почты – все более популярной тактики, при которой злоумышленники вставляют себя в существующие электронные сообщения. В одном из нападений, имевших место только на этой неделе, сообщения содержали заархивированные документы Word, защищенные паролем. При открытии и включении макросов вложения в конечном итоге приводят к загрузке Sliver, кроссплатформенного моделирования противников с открытым исходным кодом и платформы красной команды.

Согласно Proofpoint, это мероприятие демонстрирует «существенное отклонение» от предыдущих тактик, методов и процедур (TTP) от TA551.Как правило, конечной целью TA551 было удаление трояна начального доступа / банковского обслуживания, такого как IcedID, Qbot или Ursnif (иEmotet в прошлом), что в конечном итоге привело к атакам программ-вымогателей. Например, имплантаты IcedID были связаны ссобытиями, связанными с программами-вымогателями Maze и Egregorв 2020 году, как выяснили в компании.

«Обычно TA551 использует больше массовых вредоносных программ, таких как банковские трояны», - сказал Threatpost Шеррод ДеГриппо, вице-президент по исследованию и обнаружению угроз в Proofpoint. «Они могут скомпрометировать жертву и потенциально получить доступ к брокеру для развертывания Cobalt Strike и, в конечном итоге, программы-вымогателя. Теперь с Sliver им не нужно полагаться на доступ к другим группам. Злоумышленник может взломать самостоятельно с гораздо большей гибкостью, чтобы распространять программы-вымогатели, красть данные или совершать какие-либо боковые перемещения через целевую организацию».

Набор инструментов Red Teams для борьбы с киберпреступностью

По словам ДеГриппо, переход к установке Sliver свидетельствует о стремительном росте использования киберпреступниками законных инструментов для поиска угроз и защиты. Proofpoint, например, зафиксировал рост на 161% использования злоумышленниками инструмента красной команды Cobalt Strike в период с 2019 по 2020 годы.

Это явление отметили и другие исследователи.

«У злоумышленников никогда не было лучше с точки зрения свободно доступных инструментов, таких как Metasploit и Mimikatz, или пиратских копий Cobalt Strike», - написал Нейт Варфилд, технический директор Prevailion, в колонке Threatpost наэтой неделе.«Независимо от того, нужны ли им наборы инструментов для фишинга, инфраструктуры обфускации, инструменты начального доступа, инфраструктура управления и контроля (C2), инструменты для злоупотребления учетными данными или даже полезные нагрузки программ-вымогателей с открытым исходным кодом, почти все это можно бесплатно найти на GitHub. Большинство людей полагают, что злоумышленники прячутся в Dark Web,

продавая инструменты для биткойнов только самым темным из черных шляп, но это просто неправда».

Он добавил: «Индустрия дала профессионалам в области безопасности свое благословение на разработку и выпуск фреймворков для атак, исходя из того, что «защитники должны понимать эту тактику». Но это приукрашивает тот факт, что схемы атаки также помогают нападающим и усложняют защиту обороняющимся».

Sliver доступен бесплатно в Интернете, и его возможности включают сбор информации, функции управления и контроля (C2), манипулирование токенами, внедрение процессов и другие функции. Согласно Proofpoint, к числу дополнительных атакующих фреймворков, которые появляются как полезные нагрузки первого уровня, используемые киберпреступниками, относятся Lemon Tree и Veil.

«Злоумышленники используют как можно больше легитимных инструментов, включая выполнение процессов Windows, таких как PowerShell и WMI; внедрение вредоносного кода в легитимные двоичные файлы; и частое использование допустимых сервисов, таких как Dropbox, Google Drive, SendGrid и Constant Contact, для размещения и распространения вредоносных программ», - сказал ДеГриппо Threatpost. «Они гибкие, простые в доступе и использовании».

Защита от атак по электронной почте

Proofpoint заявил, что не публикует никаких данных кампании, включая виктимологию, географическое распределение атак или объем активности, поэтому трудно сказать, какие компании должны быть обеспокоены. Однако TA551 известен широкомасштабными глобальными атаками, которые бросают большую сеть. И ДеГриппо предложил следующие советы по защите:

Обучите пользователей обнаруживать вредоносную электронную почту и сообщать о ней: регулярное обучение и имитация атак могут остановить многие атаки и помочь выявить особо уязвимых людей. Лучшие симуляторы имитируют реальные методы атаки. Ищите решения, которые связаны с реальными тенденциями атак и последними данными об угрозах.

Убедитесь, что макросы отключены. Злоумышленники часто распространяют документы, требующие включения макросов для развертывания вредоносных полезных данных. Также включайте макросы моделирования атак в демонстрации обучения безопасности.

Предположим, что пользователи со временем щелкнут по некоторым угрозам. Злоумышленники всегда найдут новые способы эксплуатировать человеческую природу. Ваше решение для защиты электронной почты должно анализировать как внешнюю, так и внутреннюю электронную почту - злоумышленники могут использовать скомпрометированные учетные записи, чтобы обмануть пользователей внутри одной организации. Веб-изоляция может быть важной защитой от неизвестных и опасных URL-адресов». ***(Tara Seals. TA551 Shifts Tactics to Install Sliver Red-Teaming Tool // Threatpost (https://threatpost.com/ta551-tactics-sliver-red-teaming/175651/). 21.10.2021).***

***

«Согласно новому отчету службы аналитики угроз NCC Group, за меньшее время, чем на доставку фаршированной пиццы, новая группа под названием SnapMC может взломать системы организации, украсть ее конфиденциальные данные и потребовать плату за то, чтобы они не были опубликованы .team- программа-вымогатель не требуется.

Вместо того, чтобы нарушать бизнес-операции, блокируя данные и системы цели, SnapMC просто фокусируется на прямом вымогательстве. Однако этот низкотехнологичный, свободный от программ-вымогателей подход к вымогательству на сжатой временной шкале основан на известных уязвимостях с легкодоступными исправлениями.

«В электронных письмах с вымогательством, которые мы видели от SnapMC, жертвам давалось 24 часа на то, чтобы связаться с ними, и 72 часа на переговоры», - говорится в отчете. «Эти сроки редко соблюдаются, поскольку мы видели, что атакующий начал увеличивать давление задолго до того, как обратный отсчет достигнет нуля».

Исследователи не смогли связать группу с какими-либо известными злоумышленниками и дали ей название за ее скорость («Snap») и выбранный им инструмент для эксфильтрации mc.exe.

В качестве доказательства того, что у группы есть данные, SnapMC предоставляет жертвам список украденных данных. Если им не удастся начать переговоры в установленные сроки, злоумышленники угрожают опубликовать данные и сообщить о нарушении клиентам и СМИ.

Аналитики заявили, что они наблюдали, как SnapMC успешно взламывает незащищенные и уязвимые VPN с помощью ошибки удаленного выполнения кода CVE-2019-18935в пользовательском интерфейсе Telerik для ASPX.NET и приложений веб-серверов, использующих SQL-инъекции.

Уязвимости VPN

По словам Хэнка Шлесса, старшего менеджера службы облачной безопасности Lookout, недавний рост уязвимостей VPN оставил компании незащищенными.

«Несмотря на то, что решения VPN имеют свое место, было множество историй об уязвимостях в этих решениях, которые использовались в дикой природе», - объяснил Шлесс Threatpost. «Для обеспечения того, чтобы только авторизованные и безопасные пользователи или устройства могли получить доступ к корпоративной инфраструктуре, необходимы политики доступа к сети с нулевым доверием (ZTNA) для локальных или частных приложений и возможности брокера безопасности облачного доступа (CASB) для облачных приложений и инфраструктуры».

В июне прошлого года Colonial Pipeline был взломан со старым паролем VPN.А в июле прошлого года SonicWall выпустила исправление для ошибки в своих старых моделях VPN, которые больше не поддерживаются компанией после обнаружения атак, которые были частью продолжающейся более широкой кампании по эксплуатации (CVE-2019-7418).

В следующем месяце Cisco Systems выпустила несколько патчей для 8 800 гигабитных VPN-маршрутизаторов, уязвимых для взлома через CVE-2021-1609.

А к концу прошлого месяца Агентство национальной безопасности (АНБ) и Агентство по кибербезопасности и безопасности инфраструктуры (CSIA) выпустили руководство для Министерства обороны, систем национальной безопасности и оборонной промышленной базы по укреплению их виртуальныхчастных сетей против угроз со стороны нескольких национальных государств. субъекты постоянной угрозы (APT).

Помимо национальных государственных субъектов, базовая установка исправлений защитит от этой последней попытки вымогательства данных со стороны подобных SnapMC.

Эволюция программ-вымогателей

Оливер Таваколи, технический директор Vectra, сказал, что полное избавление от шифрования атаки является «естественным развитием» бизнес-модели программ-вымогателей. Команда NCC также прогнозирует, что тенденция к простым атакам в более короткие сроки, вероятно, сохранится.

«Группа аналитики угроз NCC Group прогнозирует, что количество атак с целью взлома данных со временем будет увеличиваться, поскольку они требуют меньше времени и даже меньше технических знаний или навыков по сравнению с полномасштабной атакой с использованием программ-вымогателей», - заявили специалисты. «Таким образом, обеспечение способности обнаруживать такие атаки в сочетании с наличием плана реагирования на инциденты, готового к выполнению в кратчайшие сроки, жизненно важно для эффективного и действенного смягчения угрозы, которую SnapMC представляет для вашей организации». ***(Becky Bracken. 30 Mins or Less: Rapid Attacks Extort Orgs Without Ransomware // Threatpost (https://threatpost.com/rapid-attacks-extort-ransomware/175445/). 13.10.2021).***

***

«Банда вымогателей Groove призывает другие группы вымогателей атаковать интересы США после того, как на прошлой неделе правоохранительные органы разрушили инфраструктуру REvil.

На выходных BleepingComputer сообщил, что программа-вымогатель REvil снова прекратила работу после того, как неизвестная третья сторона захватила их темные веб-домены.

В рамках этого отключения известный оператор REvil утверждал, что неизвестная сторона «искала» их, изменяя файлы конфигурации, чтобы злоумышленник мог обманом перейти на сайт, управляемый неизвестной организацией.

Вчера агентство Reuters сообщило, что уничтожение REvil явилось результатом международной правоохранительной операции, при поддержке ФБР.

Призывы к атакам на интересы США

Сегодня банда вымогателей Groove опубликовала в русском блоге сообщение, в котором призвала ко всем другим операциям с программами-вымогателями нацеливаться на интересы США.

Сообщение в блоге также предупреждает, что операции с программами-вымогателями не должны быть нацелены на китайские компании, поскольку бандам придется использовать страну как безопасное убежище, если Россия займет

более жесткую позицию в отношении киберпреступлений, действующих внутри ее страны.

Полностью переведенное сообщение с некоторой цензурой неуместных слов можно прочитать ниже.

«В наше трудное и беспокойное время, когда правительство США пытается с нами бороться, я призываю все партнерские программы прекратить конкуренцию, объединиться и начать усиление государственного сектора США, показать этому старику, кто здесь хозяин, кто здесь хозяин и будет в Интернете пока наши мальчики умирали на приманках, сети из грубого айби выдавливали их собственные... но он был вознагражден более высоким и теперь он сядет в тюрьму за измену, так что давайте поможем нашему государству бороться с такими упырями, как фирмы по кибербезопасности, которые продаются к амерам, как и к госструктурам США, призываю не нападать на китайские компании, ведь где нам ущипнуть, если наша Родина вдруг отвернется от нас, только нашим добрым соседям - китайцам! Я ВЕРЮ, ЧТО ВСЕ ЗОНЫ В США БУДУТ ОТКРЫТЫ, ВСЕ xxOES ВЫЙДЕТ И xxCK ЭТО xxCKING BIDEN ВО ВСЕХ ТРЕЩАХ, я сам лично приложу усилия для этого»- программа-вымогатель Groove.

Призыв к атакам на интересы США коррелирует с другой информацией, которую на этой неделе передал Bleeping Computer исследователь разведки угроз голландского банка.

В июле 2021 года злоумышленник, известный как Orange, запустил форум по взлому RAMP после закрытия и выхода из исходной операции Babuk Ransomware.

Поскольку Orange все еще контролировал сайт Tor Бабука, он использовал его для запуска хакерского форума, на котором выступал в качестве администратора. Orange также считается одним из представителей операции вымогателя Groove.

Недавно Orange ушел с поста администратора форума, чтобы продолжить новую операцию, но не предоставил никакой дополнительной информации о том, что планировалось.

Однако в более позднем сообщении указывается, что злоумышленник, вероятно, начинает новую операцию с использованием программы-вымогателя, поскольку он начал активно добиваться покупки сетевого доступа к больницам и правительственным учреждениям США...

Сообщение Groove коррелирует с вышеупомянутыми сообщениями на форуме от Orange, что указывает на то, что нацеливание на все интересы США планировалось в течение некоторого времени.

Сегодняшнее объявление Groove Ransomware коррелирует с сообщениями на форуме Orange, указывая на то, что в течение некоторого времени планировалось преследование всех интересов США, при этом правоохранительная операция REvil стала катализатором объявления Groove.

Неясно, будет ли Orange осуществлять эти атаки на организации США в рамках операции Groove или запускать новую операцию вымогателей». ***(Lawrence Abrams. Groove ransomware calls on all extortion gangs to attack US interests // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/groove-ransomware-calls-on-all-extortion-gangs-to-attack-us-interests/). 22.10.2021).***

***

«В понедельник ФБР заявило, что операторы программ-вымогателей Ranzy Locker в этом году взломали по меньшей мере 30 американских компаний из различных секторов промышленности.

«Неизвестные киберпреступники, использующие программу-вымогатель Ranzy Locker, по состоянию на июль 2021 года взломали более 30 американских предприятий», - говорится в сообщении ФБР во флэш-предупреждении TLP: WHITE.

«Среди пострадавших - строительный подсектор важнейшего производственного сектора, академический подсектор государственного сектора, сектор информационных технологий и транспортный сектор».

Флэш-предупреждение было выпущено в координации с CISA и предназначено для предоставления информации, которая поможет специалистам по безопасности обнаруживать такие попытки атак программ-вымогателей и защищаться от них.

Большинство жертв Ranzy Locker, сообщивших об атаках, сообщили ФБР, что операторы взломали их сети, взломав учетные данные протокола удаленного рабочего стола (RDP).

Совсем недавно другие сообщали, что злоумышленники также использовали уязвимые серверы Microsoft Exchange или учетные данные, украденные при фишинговых атаках

Ребрендинг Ako Ransomware

Оказавшись внутри сети жертвы, операторы Ranzy Locker также украдут незашифрованные документы перед шифрованием систем в корпоративных сетях своих жертв - тактика, используемая большинством других банд вымогателей.

Эти извлеченные файлы, содержащие конфиденциальную информацию, включая информацию о клиентах, данные, позволяющие установить личность (PII) и финансовые записи, используются в качестве рычага, чтобы заставить жертв заплатить выкуп, чтобы вернуть свои файлы и не допустить утечки данных в Интернете.

Когда жертвы посещают платежный сайт группы Tor, они видят сообщение «Заблокировано Ranzy Locker» и экран живого чата для переговоров с злоумышленниками.

В рамках этой «услуги» операторы программ-вымогателей также позволяют своим жертвам бесплатно расшифровать три файла, чтобы доказать, что дешифратор может восстановить их файлы.

Украденные документы жертв, которые не заплатят выкуп, будут опубликованы на сайте утечки данных Ranzy Locker, получившем название Ranzy Leak.

Домен, используемый их сайтом утечки, также использовался в прошлом Ako Ransomware, что стало частью ребрендинга банды с Ako на ThunderX, а затем на Ranzy Locker.

ThunderX - это программа-вымогатель, запущенная в конце августа 2020 года. В течение месяца после запуска Tesorion обнаружила слабые места в своем шифровании, что помогло создать бесплатный дешифратор.

Вскоре после этого киберпреступная группа исправила ошибки и выпустила новую версию своего штамма вымогателей под названием Ranzy Locker.

ФБР также предоставляет технические подробности относительно тактики, используемой в атаках Ranzy Locker, рекомендуемых мер защиты, а также индикаторов компрометации и правил YARA, которые можно использовать для обнаружения и защиты от таких попыток». ***(Sergiu Gatlan. FBI: Ranzy Locker ransomware hit at least 30 US companies this year // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-ranzy-locker-ransomware-hit-at-least-30-us-companies-this-year/). 26.10.2021).***

***

«Evil Corp запустила новую программу-вымогатель под названием Macaw Locker, чтобы обойти санкции США, которые не позволяют жертвам выплачивать выкуп.

Хакерская группа Evil Corp, также известная как Индрик Паук и банда Dridex, участвовала в киберпреступности с 2007 года, но в основном в качестве аффилированных лиц с другими организациями.

Со временем группа начала концентрироваться на собственных атаках, создав и распространяя в фишинговых атаках банковского трояна, известного как Dridex.

Переход на программы-вымогатели

По мере того, как атаки программ-вымогателей становились все более прибыльными, Evil Corp запустила операцию под названием BitPaymer, которая доставлялась через вредоносное ПО Dridex в скомпрометированные корпоративные сети.

Преступная деятельность хакерской группы в конечном итоге привела ксанкциям правительства США в 2019 году.

Из-за этих санкций фирмы, ведущие переговоры о программах-вымогателях, больше не будут способствовать выплате выкупа за операции, приписываемые Evil Corp.

Чтобы обойти санкции США, Evil Corp начала создавать операции с программами-вымогателями ограниченного использования под разными именами, такими как WastedLocker, Hades, Phenoix Locker и PayloadBin.

Evil Corp начала переименовывать свои операции с программами-вымогателями на разные имена, такие какWastedLocker, Hades, Phoenix CryptoLockerиPayLoadBin.

Другим семейством программ-вымогателей, которые, как считается, но не доказано, связаны с Evil Corp, являютсяDoppelPaymer, недавнопереименованный в Grief.

Представляем шкафчик ара

В этом месяце деятельность компаний OlympusиSinclair Broadcast Group была серьезно нарушена из-за атак программ-вымогателей в выходные дни.

Для Синклера это привело к отмене телетрансляций, выходу в эфир различных шоу и репортажам дикторов новостей с помощью досок и бумаги.

На этой неделе было обнаружено, что обе атаки были проведены новым вымогателем, известным как Macaw Locker.

В разговоре с техническим директором Emsisoft Фабианом Восаром BleepingComputer сказали, что на основе анализа кода MacawLocker является последним ребрендингом семейства программ-вымогателей Evil Corp.

BleepingComputer также узнал из источников в индустрии кибербезопасности, что единственными двумя известными жертвами Macaw Locker являются SinclairиOlympus.

Источники также поделились частными страницами жертв Macaw Locker для двух атак, где злоумышленники требуют выкуп в размере 450 биткойнов или 28 миллионов долларов за одну атаку и 40 миллионов долларов за другую жертву.

Неизвестно, какая компания связана с каждым требованием выкупа.

Программа-вымогатель Macaw Locker шифрует файлы жертв и добавляет расширение .macawk имени файла при проведении атак.

При шифровании файлов программа-вымогатель также создает заметки о выкупе в каждой папке с именем macaw_recover.txt. Для каждой атаки записка с требованием выкупа содержит уникальную страницу переговоров жертвы на сайте Tor в Macaw Locker и связанный с ней идентификатор дешифрования или идентификатор кампании…

Сайт банды для переговоров в темной сети содержит краткое описание того, что случилось с жертвой, инструмент для бесплатного дешифрования трех файлов и чат для переговоров с злоумышленниками.

Теперь, когда Macaw Locker был разоблачен как вариант Evil Corp, мы, вероятно, увидим, как злоумышленники снова ребрендируют свои программы-вымогатели.

Эта постоянная игра в кошки-мышки, вероятно, никогда не закончится, пока Evil Corp не перестанет проводить атаки программ-вымогателей или пока не будут сняты санкции.

Однако ни один из этих сценариев вряд ли состоится в ближайшем будущем». ***(Lawrence Abrams. Evil Corp demands $40 million in new Macaw ransomware attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/evil-corp-demands-40-million-in-new-macaw-ransomware-attacks/). 21.10.2021).***

***

«Аналитики угроз из Sentinel Labs обнаружили доказательства того, что программа-вымогатель Karma была просто еще одним эволюционным шагом в штамме, который начинался как JSWorm, затем стал Nemty, затем Nefilim, Fusion, Milihpen и совсем недавно Gangbang.

Имя Karma использовалось злоумышленникам и еще в 2016 году, но нет никакой связи между этой группой и той, которая возникла в этом году.

JSWorm впервые появился в 2019 году и в течение следующих двух лет претерпел серию ребрендингов, при этом всегда сохраняя сходство кода, которого было достаточно для исследователей, чтобы установить связь.

Сходства широкие и глубокие

Отчет основан на анализе восьми образцов, взятых из равного числа вымогателей нападений в июне 2021 года, все имеющую заметную коду сходство с Milihpen варианте, которые появились примерно в январе 2021 года.

Степень сходства варьируется до исключения папок, типов файлов и отладочных сообщений, используемых, казалось бы, несвязанными штаммами.

Еще одно примечательное сходство можно заметить при проведении «bindiff» для образцов Karma и Gangbang, когда мы видим почти неизменную функцию main ().

С точки зрения используемой схемы шифрования, в выборках произошла эволюция: более ранние использовали алгоритм шифрования Chacha20, а самые последние образцы переключились на Salsa20.

Еще одно изменение, которое было внесено на этом пути, заключалось в создании нового потока для перечисления и шифрования, возможно, для достижения более надежного результата.

Авторы вредоносной программы также добавили поддержку параметров командной строки в последних версиях.

В целом, работа над вредоносным ПО и сжатые сроки компиляции проанализированных образцов отражают тот факт, что Karma в настоящее время находится в активной разработке.

Что касается общения с жертвой и метода вымогательства, Karma следует типичному подходу: сбрасывать записки с выкупом, красть данные из скомпрометированных систем и следить за процессом двойного вымогательства.

Исторически Nemty предназначалась в основном для китайских компаний в машиностроительном и производственном секторе, используя открытые протоколы RDPи опубликованные эксплойты VPN для проникновения в уязвимые сети.

Карма может быть временным ребрендингом

В частном разговоре BleepingComputer с исследователем, подписывающим анализ, Антонисом Терефосом, мы получили следующую оценку текущего состояния Кармы:

Страница утечки лука Nemty «Корпоративные утечки» в настоящее время работает на (Onion) версии 2, поддержка которой скоро будет прекращена, а последняя утечка произошла 20 июля. Страница утечки Karma была создана 22 мая, а первая утечка произошла 1 сентября.

С текущими данными, программа-вымогатель Karma и ее луковые страницы, похоже, являются еще одним ребрендингом утечек Nemty и Corporate.С точки зрения кода основные отличия проявляются в алгоритме шифрования, который является областью экспериментов для многих авторов программ-вымогателей.

Действительно, «Корпоративные утечки» перестали действовать примерно в то же время, когда Karma Leaks появилась как новый портал для утечки данных.

Примечательно, что в последнее время новый портал также вошел в короткий период бездействия, причем самая последняя жертва, указанная там, была 20 дней назад.

С учетом всего сказанного, Karma может быть лишь кратковременной станцией в продолжении долгосрочной операции по вымогательству группы, которая притворяется меньше, чем они есть на самом деле». ***(Bill Toulas. New Karma ransomware group likely a Nemty rebrand // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-karma-ransomware-group-likely-a-nemty-rebrand/). 19.10.2021).***

***

«Как выяснила группа Symantec Threat Hunter Team Broadcom, новый штамм вымогателей, который все еще находится в стадии разработки, используется в узконаправленных атаках на корпоративные объекты.

Вредоносная программа, получившая название программы-вымогателя Yanluowang (в честь китайского божества Янлуо Ванга, одного из десяти королей ада), основана на расширении, которое она добавляет к зашифрованным файлам в скомпрометированных системах.

Он был недавно обнаружен при расследовании инцидента с участием известной организации после обнаружения подозрительной активности с использованием законного инструмента запросов Active Directory из командной строки AdFind.

AdFind обычно используется операторами программ-вымогателей для разведывательных задач, включая получение доступа к информации, необходимой для горизонтального перемещения через сети своих жертв.

Жертв предупредили, чтобы они не просили о помощи

Через несколько дней после того, как исследователи заметили подозрительное использование AdFind, злоумышленники также попытались развернуть полезные нагрузки программы-вымогателя Yanluowang в системах взломанной организации.

Перед развертыванием на скомпрометированных устройствах операторы вымогателей запускают вредоносный инструмент, предназначенный для выполнения следующих действий:

Создает файл.txt с количеством удаленных машин для проверки в командной строке.

Использует инструментарий управления Windows (WMI) для получения списка процессов, запущенных на удаленных машинах, перечисленных в файле.txt.

Записывает все процессы и имена удаленных машин в файл process.txt.

После развертывания Yanluowang остановит виртуальные машины гипервизора, завершит все процессы, собранные инструментом-предшественником (включая SQL и Veeam), зашифрует файлы и добавит расширение .yanluowang.

В зашифрованных системах Yanluowang также отправляет записку о выкупе под названием README.txt, в которой жертвам рекомендуется не обращаться в правоохранительные органы и не просить помощи у фирм, занимающихся переговорами о программах-вымогателях.

Угрозы DDoS-атак

«Если правила злоумышленников нарушаются, операторы программ-вымогателей заявляют, что они проведут распределенные атаки типа «отказ в обслуживании» (DDoS) против жертвы, а также будут «звонить сотрудникам и деловым партнерам», - добавили исследователи Broadcom.

«Преступники также угрожают повторить атаку «через несколько недель» и удалить данные жертвы» - обычная тактика, используемая большинством банд вымогателей, чтобы заставить своих жертв заплатить выкуп.

Индикаторы взлома, включая хэши вредоносных программ, можно найти в конце отчета Symantec Threat Hunter Team.

Несмотря на то, что Yanluowang находится в стадии разработки, он все еще является опасным вредоносным ПО, учитывая, что программы-вымогатели являются одной из самых больших угроз, с которыми организации сталкиваются во всем мире.

Совет национальной безопасности Белого дома организует на этой неделе серию встреч между высокопоставленными должностными лицами из более чем 30 стран в рамках виртуального международного мероприятия по борьбе с программами-вымогателями, чтобы присоединиться к усилиям США по борьбе с группами киберпреступников-вымогателей.

После атак программ-вымогателей на Colonial Pipeline и JBS этим летом заместитель советника по национальной безопасности Энн Нойбергер также призвала американские компании серьезно относиться к программам-вымогателям». ***(Sergiu Gatlan. New Yanluowang ransomware used in targeted enterprise attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-yanluowang-ransomware-used-in-targeted-enterprise-attacks/). 14.10.2021).***

***

«Высокопоставленные официальные лица из 31 страны и Европейского Союза заявили, что их правительства примут меры, чтобы нарушить каналы оплаты криптовалютой, используемые бандами вымогателей для финансирования своих операций.

Совместное заявление было выпущено после виртуальных встреч по инициативе Counter-Ransomware Initiative, организованных на этой неделе Советом национальной безопасности Белого дома в ответ на продолжающиеся атаки, которые выявили значительные уязвимости в критически важной мировой инфраструктуре.

Его выпустили министры и представители из Австралии, Бразилии, Болгарии, Канады, Чехии, Доминиканской Республики, Эстонии, Европейского Союза, Франции, Германии, Индии, Ирландии, Израиля, Италии, Японии, Кении, Литвы, Мексики, Нидерландов., Новая Зеландия, Нигерия, Польша, Республика Корея, Румыния, Сингапур, Южная Африка, Швеция, Швейцария, Украина, Объединенные Арабские Эмираты, Великобритания и США.

Блокирование злоупотреблений бандами вымогателей криптовалютой

Публично раскрытые платежи программ-вымогателей достиглипочти 500 миллионов долларов в криптовалюте во всем мире за последние два года (400 миллионов долларов в 2020 году и более 80 миллионов долларов в первом квартале 2021 года).

Предотвращение злоупотребления виртуальными активами в глобальном масштабе повлияет на бизнес-модель и основной инструмент, используемый группами киберпреступников-вымогателей для сбора выкупа со своих жертв и отмывания средств, полученных в результате атак, направленных на организации по всему миру.

Инициатива по борьбе с программами-вымогателями надеется истощить их финансирование и прекратить их операции, нарушив каналы финансирования групп программ-вымогателей.

«Мы признаем, что неравномерное глобальное внедрение стандартов Группы разработки финансовых мер борьбы с отмыванием денег (FATF) в отношении виртуальных активов и поставщиков услуг виртуальных активов (VASP) создает среду, допускающую юрисдикционный арбитраж со стороны злоумышленников, ищущих платформы для перемещения незаконных доходов, не подвергаясь соответствующие обязательства по борьбе с отмыванием денег (AML) и другие обязательства», -заявили официальные лица.

«Мы стремимся активизировать наши усилия по разрушению бизнес-модели программ-вымогателей и связанной с ними деятельности по отмыванию денег, в том числе путем обеспечения того, чтобы наши национальные системы AML эффективно выявляли и снижали риски, связанные с VASP и связанной с ними деятельностью».

Усилия по пресечению злоупотреблений криптовалютой группами программ-вымогателей будут включать регулирующие органы, подразделения финансовой разведки и правоохранительные органы, регулирующие, контролирующие, расследующие и принимающие меры против эксплуатации виртуальных активов.

«Мы также будем искать способы сотрудничества с индустрией виртуальных активов для улучшения обмена информацией, связанной с программами-вымогателями», - добавили официальные лица.

Государства, стоящие за этим действием, будут использовать свои финансовые институты и инфраструктуру для совместного отражения действий программ-вымогателей, нацеленных на критически важную инфраструктуру международных партнеров.

Дополнительные усилия также будут включать в себя нарушение экосистемы программ-вымогателей посредством сотрудничества правоохранительных органов, повышение устойчивости сети для предотвращения атак, устранение убежищ преступников-вымогателей и дипломатическое взаимодействие с целью побудить другие страны противодействовать операциям с программами-вымогателями, действующим на их территории.

Постоянные усилия по предотвращению угроз программ-вымогателей

В сентябре министерство финансов США объявило о первых в истории санкциях против криптовалютной биржи за содействие операциям с выкупом для банд вымогателей и помощь им в уклонении от санкций.

В последние годы правительство США также ввело санкции против других участников угроз и организаций, связанных с бандами вымогателей.

Два года назад, в 2019 году, США обвинили нескольких членов Evil Corpв хищении более 100 миллионов долларов и добавили их в санкционный список Управления по контролю за иностранными активами (OFAC).

Evil Corp была связана с несколькими семействами программ-вымогателей на протяжении многих лет, включая WastedLocker, Hades, Phoenix CryptoLockerиPayLoadBin…». ***(Sergiu Gatlan. Governments worldwide to crack down on ransomware payment channels // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/governments-worldwide-to-crack-down-on-ransomware-payment-channels/). 15.10.2021).***

***

«По словам директора британского агентства спецсвязи (GCHQ), агентство рассматривает возможность использования военных хакеров из новых национальных киберсил Великобритании для «отслеживания» и противодействия группировкам кибер-вымогателей.

Сэр Джереми Флеминг предупреждает, что в 2021 году количество атак программ-вымогателей, в ходе которых хакеры захватили корпоративные системы и данные и опубликовали их, удвоилось в разы.

«Причина, по которой это распространяется, заключается в том, что кибер-вымогательство дает свои плоды… Преступники зарабатывают на этом очень хорошие деньги и часто чувствуют, что это безнаказанно», - отметил он, добавив, что британские граждане с большей вероятностью могут стать жертвами киберпреступлений, чем любого другого из видов преступлений. Во время пандемии Covid-19 рост атак программ-вымогателей был стремительным, поскольку удаленная работа увеличивала уязвимость организаций и сотрудников для хакеров.

Директор GCHQ, который в понедельник участвовал в Конференции по угрозам криптографии в США по видеосвязи, сказал, что одним из способов охвата целевых групп, недоступных для полиции и прокуратуры, было «таргетирование». Это также включает агрессивные кибер-кампании.

Детали таких операций конфиденциальны, но обычно включают такие действия, как блокирование сигналов враждебных телефонов или уничтожение серверов. В прошлом году Соединенное Королевство объявило о создании национальных сил кибербезопасности (NCF), совместно управляемой спецслужбами и военными, для усиления британского потенциала кибервойны.

В то же время, США возглавляет международные действия по борьбе с программами-вымогателями после серии атак с нулевым кодом, в том числе атаки в начале этого года на Колониальный трубопровод, нефтяную артерию, которая снабжает восточное побережье Соединенных Штатов.

Коалиция из более чем 30 стран, включая США, Индию, Австралию, Соединенное Королевство, Германию, Украину и Эстонию, в этом месяце провела эффективную встречу, чтобы скоординировать свои действия в ответ на угрозы

хакерских атак, исходящих преимущественно от российских и китайских киберпреступных группировок

Флеминг подчеркнул, что борьба с программами-вымогателями предполагает установление связей между государством и преступной сетью. «Нам необходимо не просто избавиться от программ-вымогателей, что само по себе не имеет особого значения. Нам нужно прояснить границы и действия, которые мы хотим видеть. Между преступниками и государственными чиновниками», - сказал он на встрече.

Этим летом на саммите в Женеве президент США Джо Байден сообщил президенту России Владимиру Путину, если российское государство или базирующиеся в России хакеры нацелены на критическую инфраструктуру США, то Соединенные Штаты предупреждают, что «ответят кибернетикой».Энн Нойбергер, заместитель советника Белого дома национальной безопасности по киберугрозам, заявила, что США «видят краткосрочный прогресс в действии» после того, как поделились с Москвой информацией о группировках кибер-вымогателей, действующей в России.

Эмили Тейлор, эксперт по кибербезопасности и международной безопасности из аналитического центра Chatham House, выразила обеспокоенность тем, что использование NCF для борьбы с группировками кибер-вымогателей может создать риск эскалации. Кроме того, ситуацию усложняет отсутствие жизнеспособной системы международного уголовного правосудия в сфере киберпреступлений.

Тейлор также выразила некоторые сомнения в том, что Россия ответит на публичные обвинения в том, что хакерские группировки могут процветать и распространяться. «Считается, что Россия - это государство, которое позволяет своей территории стать безопасной гаванью для кибергрупп организованной преступности», - сказала она.«Мы видели государства, призывающие к этим связям, и регулярные отрицания этого факта Россией. Международный имидж и порицание работают, только если нация заботится о своем положении в международном сообществе». ***(Романов Роман. Великобритания будет использовать военных хакеров для борьбы с бандами кибер-вымогателей // Internetua (http://internetua.com/Velikobritaniya-budet-ispolzovat-voennyh-hakerov-dlya-borby-s-bandami-kiber-vymogatelei). 25.10.2021).***

***

«Операторы вымогателя Grief утверждают, что атаковали американскую Национальную стрелковую ассоциацию (National Rifle Association, NRA). В качестве доказательства своих слов хакеры опубликовали украденные у NRA данные.

На своем сайте в даркнете группировка выложила скриншоты таблиц Excel, демонстрирующие налоговую и инвестиционную информацию, а также протоколы заседания правления. Кроме того, злоумышленники опубликовали архив объемом 2,7 Мб под названием National Grants.zip, в котором содержатся заявки на гранты NRA. Хакеры традиционно угрожают обнародовать больше данных, если им не выплатят выкуп.

Представители NRA не комментируют случившееся, лишь сообщают в Twitter, что не дают комментариев по вопросам «связанным с физической или электронной безопасностью», а также уверяют, что «предпринимают чрезвычайные меры для защиты информации, касающейся членов, жертвователей и операций NRA»

Пока неясно, атаковали вымогатели центральный офис NRA или жертвой хакеров стало некое региональное отделение. Также стоит отметить, что многие эксперты выражают недоумение относительно этого взлома, ведь Национальная стрелковая ассоциация недавно объявила о своем банкротстве и не совсем понятно, как NRA может выплатить злоумышленникам выкуп.

Более того, вымогатель Grief представляет собой ребрендинг другой малвари, DoppelPaymer, и оба эти вымогателя связывают с известной хак-группой Evil Corp. Еще в 2019 году власти СШАввели санкции в отношении 24 организаций и лиц, связанных с этой хак-группой. В результате компании-переговорщики, которые обычно договариваются с вымогателями об уплате выкупа и расшифровке данных, отказались «работать» с Evil Corp, чтобы избежать штрафов и судебных исков со стороны Министерства финансов США.

В ответ на это Evil Corp стала переименовывать свое малварь и маскировать операции, чтобы избежать санкций. Так, в арсенале группировки числятся такие вымогатели, как WastedLocker, Hades и Phoenix и PayloadBIN, DoppelPaymer (теперь Grief или Pay or Grief), Macaw. Однако, учитывая санкции, любые компании и организации в США должны получить разрешение Казначейства, прежде чем переводить деньги организациям и лицам, связанным с EvilCorp». ***(Мария Нефёдова. Национальная стрелковая ассоциация США стала жертвой атаки шифровальщика Grief // хакер (https://хакер.ru/2021/10/28/nra-grief/). 28.10.2021).***

***

«Финансовый отдел Папуа-Новой Гвинеи подвергся атаке с использованием программ-вымогателей, заблокировав доступ к сотням миллионов долларов в виде иностранной помощи. Об этом сообщает Bloomberg со ссылкой на людей, знакомых с ситуацией.

По словам источников, на прошлой неделе произошла атака на Интегрированную систему финансового управления (IFMS) Министерства финансов. IFMS объединила бюджет тихоокеанской страны и отчетность для всех уровней и департаментов правительства на платформе. Он контролирует доступ к фондам для правительства, которое сильно зависит от иностранной помощи.

Хакеры потребовали от властей выкуп в биткойнах. При этом сумма не называется.

По словам источников, в государственных сетевых системах есть несколько критических уязвимостей, которые позволили бы злоумышленникам взломать сети.

Сотрудники бухгалтерии одного министерства подтвердили Bloomberg, что система не работает, и что Департамент финансов занимается решением проблемы, но не объяснил причину.

Пока официальных комментариев из правительства Папуа — Новой Гвинеи по этому вопросу не поступало». ***(Вымогатели атаковали минфин Папуа-Новой Гвинеи // SecurityLab.ru(https://www.securitylab.ru/news/526038.php). 28.10.2021).***

***

«Немецкий производитель компонентов для автомобилей Eberspdcher Group подвергся вымогательской атаке, повлекшей сбой в работе IT-систем компании. В результате концерн был вынужден отправить часть работников в оплачиваемый отпуск.

Eberspdcher Group специализируется на разработке и производстве систем отопления и кондиционирования воздуха для автотранспорта. В настоящее время концерн имеет 70 представительств в 28 странах.

В сообщении на сайте компания признала, что стала жертвой организованной кибератаки, затронувшей IT-системы, и привлекла специалистов в области безопасности для устранения угрозы.

Из-за инцидента, имевшего место 24 октября, Eberspdcher отключила официальные web-сайты, системы электронной почты и производственные системы. В связи с невозможностью координировать производственный процесс и обрабатывать заказы компания отправила часть сотрудников в Германии и Румынии в оплачиваемый отпуск.

Представители компании не предоставили подробности о кибератаке, однако, по данным немецкого издания Automobilwoche, инцидент расследуется как случай «компьютерного саботажа и шантажа»…». ***(Вымогательская атака нарушила работу заводов Eberspdcher // SecurityLab.ru (https://www.securitylab.ru/news/526042.php). 28.10.2021).***

***

Програми-трояни

«Группа угроз Lyceum снова появилась, на этот раз со странным вариантом трояна удаленного доступа (RAT), который не имеет возможности общаться с сервером управления и контроля (C2) и может вместо этого быть новым способом прокси-трафик между кластерами внутренней сети.

Марк Лехтик из «Лаборатории Касперского», старший исследователь безопасности в группе глобальных исследований и анализа (GReAT), заявил впонедельник, что команда определила новый кластер деятельности лицея, который сосредоточен на двух организациях в Тунисе.

В документе (PDF), представленном ранее в этом месяце на конференции Virus Bulletin, Лехтик и его коллеги-исследователи из «Лаборатории Касперского» Асел Каял и Пол Раскагерес написали, что злоумышленник атаковал известные тунисские организации, такие как телекоммуникационные или авиационные компании.

Это вписывается в целевой список группы. Лицей был активен еще в апреле 2018 года, когда он атаковал телекоммуникационные компании и критически

важную инфраструктуру в ближневосточных нефтегазовых организациях. Лицей поступает легко, но несет большую палку: «Все это время он вел себя сдержанно, не привлекая мало внимания со стороны исследователей безопасности», - написали трио исследователей.

Группа Lyceum (также известная как Hexane) была впервые раскрыта в 2019 году компанией Secureworks, которая обнаружила, что группа, нацеленная на ближневосточные энергетические компании и телекоммуникационные компании, с помощью целевых фишинговых электронных писем, содержащих вредоносное ПО.

В то время Lyceum использовал различные сценарии PowerShell и новый троян удаленного доступа (RAT) на основе.NET под названием DanBot, который развертывал инструменты после вторжения для распространения по сетям зараженных компаний, кражи учетных данных и другой информации учетной записи и регистрации нажатий клавиш. DanBot взаимодействует с сервером C2 через специально разработанные протоколы через DNS или HTTP.

Новые открытия Лаборатории Касперского были вызваны сценарием PowerShell (MD5: 94eac052ea0a196a4600e4ef6bec9de2), который был отправлен в VirusTotal в ноябре прошлого года и помог исследователям отслеживать последние следы группы угроз.

«Сценарий запутан и закодирован в кодировке Base64, что позволяет предположить, что он, возможно, пытался избежать обнаружения в среде жертвы», - говорится в документе. «Но после деобфускации полученный код показывает множество комментариев, оставленных злоумышленниками, с подробным описанием того, что делает сценарий, и даже с объяснением изменений по сравнению с предыдущими версиями. Некоторые функции также были отмечены как устаревшие, что говорит о том, что этот сценарий, возможно, находится в стадии разработки».

Хотя здесь относительно тихо, Лицей не молчал. Фактически, Kaspersky нашел достаточно потоков, чтобы связать его с злоумышленником APT34 / OilRig, как подробно описано ниже.

От.NET, на C ++

По трекам группы видно, что арсенал лицея эволюционировал. Группа перешла от своих более ранних вредоносных программ.NET к новым версиям, написанным на C ++. Касперский определил два кластера вариантов, названные «Джеймс» и «Кевин», просто потому, что это были имена в системах, используемых для компиляции вредоносного ПО.

Эти варианты DanBot возникли через несколько месяцев после того, как Secureworks опубликовала свои выводы о Lyceum, предполагая, что публичность нанесла некоторый ущерб группе, как отметил Каял во время конференции Virus Bulletin:

«Между ранее задокументированным DanBot и двумя более новыми вариантами существует промежуток в пару месяцев», - сказала она. «Мы полагаем, что это, вероятно, связано с публикацией SecureWorks, и что злоумышленники, возможно, решили внести некоторые изменения в свой набор инструментов после того, как некоторые из них были раскрыты в этом отчете».

Оба новых варианта DanBot, как и оригинальный DanBot, поддерживают аналогичные настраиваемые протоколы C2, туннелируемые через DNS или HTTP, пояснил Лехтик в своем брифинге в понедельник. «При этом мы также выявили необычный вариант, в котором не было механизма сетевой коммуникации», - сказал он. «Мы предполагаем, что он использовался как средство для прокси-трафика между двумя внутренними сетевыми кластерами».

Кевин, ты чудак

По мнению Касперского, вариант Кевина может «представлять собой новую ветвь разработки в арсенале группы».

Вариант впервые появился в июне 2020 года, и в большинстве образцов есть строка, означающая, что это внутренняя версия с именем v1.0.2. Затем, 10 месяцев назад, в декабре, появилась новая волна образцов из варианта Кевина с номером версии v2.1.0.2.

Вариант внес изменения в протоколы связи и в основном скомпилирован для 64-битных систем. Согласно описанию Касперского, его цель - «облегчить канал связи, который передает произвольные команды для выполнения имплантатом».

«Для этого вредоносная программа запрашивает файлы, которые будут созданы в файловой системе и записаны с помощью команд, полученных с сервера в указанном формате», - говорится в документе.«Содержимое файла будет считываться и интерпретироваться имплантатом в соответствии с этим форматом, где предопределенные ключевые слова будут заменены определенными путями, связанными с вредоносным ПО, или использованы для обновления внутренних конфигураций времени выполнения. В свою очередь, команды будут выполнены, дав ответ серверу».

Но до того, как произойдет коммуникация, вариант Кевина может выполнить загрузку и подготовить среду жертвы к ее выполнению с помощью набора действий, общих для многих его образцов, как описали исследователи.

Неполный список этих действий:

Скрывает текущее окно от пользователя с помощью функции API ShowWindow.

Создает мьютекс со значением GUID в нижнем регистре, жестко закодированным в двоичном файле.

Проверяет аргументы, с которыми он был выполнен. Обязательно, чтобы первый аргумент был равен номеру версии (например, v1.0.2 или v2.1.0.2). «Мы полагаем, что это могло быть включено, чтобы избежать полного выполнения функций вредоносного ПО в изолированных средах», - пояснили исследователи.

Отслеживание потоков к другим APT

Исследователи «Лаборатории Касперского» заявили, что они заметили определенное сходство между Lyceum и печально известной спонсируемой государством кампанией группы DNSpionage, которая собирала учетные данные, нацеливаясь на организации национальной безопасности на Ближнем Востоке и в Северной Африке (MENA) - и в других местах - с системой доменных имен (DNS) атаки с перехватом.

DNS-шпионаж, в свою очередь, связан с APT34 / OilRig, сказал Лехтик в своем обзоре в понедельник: Расширенная постоянная угроза (APT), которая

запустила сериюкибератак на ближневосточную телекоммуникационную компаниюв июле 2020 года.

«Помимо схожего выбора географических целей, а также использования DNS или поддельных веб-сайтов для туннелирования данных C2 в качестве TTP [тактика, методы и процедуры], мы смогли проследить значительное сходство между документами-приманками, предоставленными Lyceum в прошлом, и теми, которые использовались DNSpionage», - написал он. «Это стало очевидным благодаря общей структуре кода и выбору имен переменных».

Исследователи отметили, что методы работы Lyceum «поразительно похожи на методы работы APT34 / OilRig».

Согласно документу, «Обе группы имеют схожие геополитические ориентиры и предпочитают использовать DNS-туннелирование в различных полезных нагрузках, которые они разработали на протяжении многих лет. Хотя мы не нашли убедительных доказательств, подтверждающих это, мы заметили некоторое сходство между доставочными документами, используемыми Lyceum еще в 2018-2019 годах, и документами DNSpionage, который, как полагают, также связан с OilRig».

Кроме того, макросы, встроенные в документы из двух групп, имеют одинаковые имена переменных и аналогичную структуру кода, как показано ниже.

Атаки, начатые с документов Excel

Когда Lyceum / Hexane был впервые обнаружен, его атаки были начаты с документов Excel, заминированных вредоносными макросами. В одной из наблюдаемых атак использовались сообщения с обещанием отобразить список событий, связанных с системами управления производством или с ближневосточным газонефтяным составом. Еще одна вредоносная электронная таблица якобы связана с безопасностью и содержит список худших паролей с 2017 года.

В своем недавнем расследовании Kaspersky идентифицировал некоторые другие MO Lyceum, в том числе некоторые команды, которые злоумышленники использовали в скомпрометированных средах, а также то, как учетные данные пользователей, хранящиеся в браузерах, были украдены с помощью сценария PowerShell, и подробности о развернутом настраиваемом кейлоггере. на некоторых целевых машинах.

В статье Касперского подробно рассматриваются технические аспекты расследования Lyceum, но версия TL; DR заключается в том, что APT не прекратил свое существование после его обнаружения в 2019 году, и мы, вероятно, еще услышим о нем больше.

«Благодаря значительным разоблачениям деятельности DNSpionage в 2018 году, а также дополнительным данным, проливающим свет на очевидную связь с APT34, мы можем оценить, что последний, возможно, изменил некоторые из своих методов работы и организационной структуры, проявившись в новой операционной системе. сущности, инструменты и кампании», - говорится в статье Касперского.

Лицей = Рост DNS-шпионажа?

По утверждению Касперского, одним из новых оперативных подразделений DNSpionage на самом деле является Лицей. «После дальнейшего разоблачения Secureworks в 2019 году [Lyceum] пришлось еще раз переоборудовать», что привело к кампании, которую Касперский описал в своей статье.

Лицей не перестает работать; скорее, группа «снова и снова пыталась закрепиться в целевых сетях», - заявили исследователи.

APT не только продолжал предпринимать попытки атак до 2021 года. И его образцы также показывают вариации кода, которые указывают на то, что группа снова начала переоснащение…». ***(Lisa Vaas. Lyceum APT Returns, This Time Targeting Tunisian Firms // Threatpost (https://threatpost.com/lyceum-apt-tunisian-firms/175579/). 19.10.2021).***

***

«Исследователи обнаружили эксплойт «нулевого дня» для Microsoft Windows, который этим летом использовался для повышения привилегий и захвата серверов Windows в рамках шпионской кампании APT (англоговорящей китайской группы). Цепочка эксплойтов закончилась тем, что недавно обнаруженный троян удаленного доступа (RAT), получивший название MysterySnail, был установлен на взломанных серверах с целью кражи данных.

Microsoft исправила ошибку (CVE-2021-40449) в рамках октябрьских обновлений во вторник, выпущенных на этой неделе.

Согласно анализу, проведенному во вторник исследователями «Лаборатории Касперского», проблема кроется в драйвере ядра Win32k. Это уязвимость использования после освобождения, и «основная причина этой уязвимости заключается в возможности устанавливать обратные вызовы в пользовательском режиме и выполнять неожиданные функции API во время выполнения этих обратных вызовов», - пояснили они. «CVE-2021-40449 срабатывает, когда функция ResetDC выполняется второй раз для того же дескриптора во время выполнения собственного обратного вызова».

По словам Касперского, в конечном итоге это приводит к появлению висящего указателя в памяти, который указывает на ранее уничтоженный объект Proactive Data Container (PDC). Это означает, что искаженный объект PDC может использоваться для вызова произвольной функции ядра и оттуда позволяет злоумышленникам читать и записывать память ядра.

«Можно использовать общеизвестные методы для утечки адресов ядра загруженных в настоящее время драйверов / модулей ядра», - говорят исследователи.

MysterySnail RAT в действии

Как уже упоминалось, киберпреступники использовали эксплойт в рамках более широких усилий по установке удаленной оболочки на целевые серверы, то есть вредоносной программы MysterySnail, о которой до этой кампании не было известно.

Исследователи «Лаборатории Касперского» заявили, что образец, который они проанализировали, имел значительный размер 8,29 МБ, что сразу привлекло их внимание.

«Одна из причин такого размера файла заключается в том, что он статически скомпилирован с библиотекой OpenSSL и содержит неиспользуемый код и данные, принадлежащие этой библиотеке», - пояснили они. «Но основной причиной его размера является наличие двух очень больших функций, которые ничего не делают, кроме пустой траты тактовых циклов процессора. Эти функции также используют случайно сгенерированные строки, которые также присутствуют в двоичном файле».

Они добавили, что это, вероятно, функции антианализа, отметив, что код также содержит другую избыточную логику и «наличие относительно большого количества экспортируемых функций, в то время как реальная работа выполняется только одной из них».

Согласно анализу, функция, отвечающая за выполнение фактических действий вредоносного ПО, называется GetInfo.

Вредоносная программа декодирует командный адрес (C2) и пытается подключиться к нему. Он также запрашивает туннелирование через прокси-сервер в случае, если он не может напрямую подключиться к C2.

Оттуда вредоносная программа собирает основную информацию о машине жертвы: имя компьютера, текущая кодовая страница OEM / идентификатор по умолчанию, название продукта Windows, локальный IP-адрес, имя пользователя, вошедшего в систему, и название кампании.

«Интересным фактом является то, что «название кампании» по умолчанию установлено на Windows», - считают исследователи. «Это имя перезаписывается, но это может означать, что существуют версии того же RAT, скомпилированные для других платформ».

Затем он ожидает зашифрованных команд от C2. Он поддерживает 20 из них. Эти:

Запустите интерактивную оболочку cmd.exe. Перед запуском cmd.exe копируется во временную папку с другим именем

Создать новый процесс

Создать новый процесс (консоль)

Получите существующие дисковые накопители и их тип. Эта функция также работает в фоновом режиме, проверяя наличие новых дисков.

Создать (загрузить) новый файл. Если файл существует, добавить к нему данные

Получить список каталогов

Убить произвольный процесс

Удалить файл

Прочитать файл

Подключить повторно

Установить время сна (в миллисекундах)

Выключить сеть и выйти

Выход

Убить интерактивную оболочку

Завершить операцию чтения файла

Нет операции

Открыть прокси-соединение с указанным хостом. Поддерживается до 50 одновременных подключений.

Отправлять данные на прокси-соединение

Закройте все прокси-соединения

Закрыть запрошенное прокси-соединение

«Сама вредоносная программа не очень сложна и имеет функциональность, аналогичную многим другим удаленным оболочкам», - отмечают исследователи. «Но он все же каким-то образом выделяется относительно большим количеством реализованных команд и дополнительных возможностей, таких как мониторинг вставленных дисков и возможность действовать в качестве прокси».

Ссылка на IronHusky

В ходе анализа MysterySnail RAT, проведенного «Лабораторией Касперского», они связали кампанию с APT-активностью группы IronHusky благодаря повторному использованию инфраструктуры C2, которая использовалась в других атаках, начиная с 2012 года.

Они также обнаружили другие кампании этого года, в которых использовались более ранние варианты вредоносного ПО, что также помогло привязать его к китайскому APT, известному как IronHusky.

«Мы смогли обнаружить, что прямой код и функциональность частично совпадают с вредоносным ПО, приписываемым субъекту IronHusky», - заявили исследователи. «Мы также смогли обнаружить повторное использование адресов C2, используемых в атаках китайскоязычным APT еще в 2012 году. Это открытие связывает IronHusky с некоторыми из более старых известных действий».

IronHusky был впервые обнаружен летом 2017 года, и у него есть история использования эксплойтов для доставки RAT к целям. Например, в 2017 году Касперский обнаружил, что группа, использующая CVE-2017-11882, распространяет распространенные RAT PlugX и PoisonIvy.

«Он очень сосредоточен на отслеживании геополитических целей в Центральной Азии с особым упором на Монголию, что кажется необычной целью», - отметила фирма в своем отчете о деятельности. «Этот актер готовит кампании к предстоящим интересным событиям. В данном случае они подготовили и запустили один прямо перед встречей с Международным валютным фондом и правительством Монголии в конце января 2018 года. В то же время они прекратили свои предыдущие операции, направленные на российских военных подрядчиков, что красноречиво говорит о деятельности группы. ограничения.»

Последние атаки были целенаправленными, но масштабными. Согласно описанию, исследователи «Лаборатории Касперского» обнаружили варианты MysterySnail, используемые в широко распространенных шпионских кампаниях против ИТ-компаний, военных и оборонных подрядчиков, а также дипломатических структур». ***(Tara Seals. Windows Zero-Day Actively Exploited in Widespread Espionage Campaign // Threatpost (https://threatpost.com/windows-zero-day-exploited-espionage/175432/). 12.10.2021).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Південна Корея заявила, що звернулася до Інтерполу з проханням про допомогу в арешті двох іноземців, втому числі українця, які, за її твердженням, зіграли провідну роль в кібератаках і великомасштабному вимаганні проти південнокорейських і американських компаній…

Деталі

Агентство поліції Кореї заявило, що воно отримало ордера на арешт всередині країни, і попросило Інтерпол видати «червоне повідомлення» для двох підозрюваних, щоб їхд оставити до Південної Кореї.

Південнокорейська влада не назвала імена або додаткову інформацію про двох підозрюваних, щодо яких вони запросили повідомлення Інтерполу, за винятком того, що один з них є громадянином України.

Підозрюваний, який є громадянином України, був серед шести осіб, затриманих українською поліцією в червні, коли влада Південної Кореї і США приєдналися до рейдів по домівках підозрюваних, пов’язаних з синдикатом вимагачів «Clop», у Києві та інших містах. Поліцейські операції були націлені на кандидатів у партнери російськомовної банди здирників, обвинуваченої в кібератаках на півмільярда доларів в результаті кібератак, які можуть бути зупинені тільки за допомогою програмного ключа, отриманого шляхом оплати злочинцям.

«Найпотужніші банди здирників діють з терпимістю Кремля, поза досяжністю західних правоохоронних органів. Російська влада їх не переслідує і не екстрадує»,— йдеться в повідомленні.

У заяві поліції Південної Кореї кажуть, що підозрювані, затримані в Україні в червні, нібито, співпрацювали з хакерською організацією і відмивали віртуальну валюту, отриману за допомогою програми-здирника, і конвертували її в готівку.

Раніше в цьому місяці поліція Південної Кореї вирішила вжити заходів до того, щоб троє із затриманих раніше в Україні і ще одна особа, громадянство якої вони відмовляються розкривати, були звинувачені в порушенні законів Південної Кореї про мережі зв’язку і захисту інформації, вимаганні та приховуванні злочинних доходів.

Південна Корея тепер намагається екстрадувати двох підозрюваних, які відіграли провідну роль в кібератаках.

Доповнення

За словами корейської поліції, український закон недозволяє екстрадувати підозрюваних в скоєнні кримінальних злочинів закордон, а правовий статус і місце знаходження одного з підозрюваних невідомі. Три компанії і університет в Південній Кореї постраждали від атак програм-вимагачів в 2019 році. Злочинці вимагали викуп в біткойнах, еквівалентний 4,5 мільярда вон (3,8 мільйона доларів) готівкою.

У більш ранній заяві української поліції говорилося, що банда також була націлена на університети США, втому числі Стенфордської медичної школи і Університет Меріленда.

Південнокорейська поліція заявила, що продовжить розслідування, щоб розібратися з хакерською групою, відповідальною за кібератаки. Поліція не встановила, де знаходиться ця організація і звідки її хакери».***(Галина Крижанівська. Південна Корея звернулася до Інтерполу з проханням заарештувати двох іноземців, в тому числі українця, через причетність до кібератаки // Українські Національні Новини (https://www.unn.com.ua/uk/news/1948278-pivdenna-koreya-zvernulasya-do-interpolu-z-prokhannyam-zaareshtuvati-dvokh-inozemtsiv-v-tomu-chisli-ukrayintsya-cherez-prichetnist-do-kiberataki). 15.10.2021).***

***

«Немецкие правоохранители раскрыли личность, как они полагают, одного из ключевых участников вымогательской группировки REvil, известной благодаря громким атакам на крупные компании по всему миру. Как сообщило издание Zeit Online, речь идет о некоем Николае К., позиционирующем себя как криптоинвестор и трейдер.

Журналисты немецкой национальной телекомпании Bayerischer Rundfunk и ZEIT ONLINE провели собственное расследование, в рамках которого в течение нескольких месяцев изучали цифровые следы в социальных медиа, анонимных Telegram-каналах и «в мире криптовалюты». Они выявили по меньшей мере шесть переводов биткойнов с аккаунтов, связываемых с киберпреступными операциями, на адрес, предположительно принадлежащий Николаю К.

Поиск в Google по имени «подозреваемого», используемого в соцсетях, вывел журналистов на адрес электронной почты, служащий для регистрации на различных web-сайтах, связанных с несколькими российскими мобильными номерами. Один из номеров привел к Telegram-аккаунту, в котором был опубликован Bitcoin-адрес. На данный адрес было перечислено более 400 тыс. евро, предположительно полученных в результате вымогательства.

Такие Bitcoin-адреса и вывели полицию Баден-Вюртемберга на след Николая К. в рамках расследования вымогательской атаки на Штутгартский Национальный театр, произошедшей в 2019 году. Атака, в ходе которой использовалось вымогательское ПО Gandcrab, на несколько дней вывела из строя компьютеры театра, вынудив сотрудников продавать билеты написанные от руки. Предполагается, что руководство театра в конечном итоге выплатило вымогателям 15 тыс. евро в качестве выкупа, и полиция начала отслеживать этот платеж.

В то время хакерская группировка, членом которой предположительно является Николай К., действовала под названием Gandcrab, но следователи и ИБ-эксперты считают, что та же группировка теперь управляет REvil…». ***(Zeit Online: Немецкая полиция идентифицировала одного из ключевых участников REvil // SecurityLab.ru (https://www.securitylab.ru/news/526061.php). 28.10.2021).***

***

«Использование компонентов программного обеспечения с открытым исходным кодом становится все более популярным среди многих разработчиков.

Однако эта растущая зависимость от библиотек с открытым исходным кодом создает определенный риск, когда это программное обеспечение, которое оказывается целью кибератак, включает в себя все более изощренные уязвимости.

Открытый исходный код: средство вторжения в логистическую цепочку

Сегодня 90% программных компонентов приложения происходят из открытых источников.

Программное обеспечение с открытым исходным кодом (программное обеспечение с открытым исходным кодом/ OSS на английском языке), созданное на основе открытого исходного кода и бесплатное- или почти - позволяет разрабатывать с меньшими затратами, без необходимости покупать лицензию для проприетарных компаний (хотя это не исключает подсчета установки и обслуживания расходы).

Ежегодно загружается в среднем 373 000 программ с открытым исходным кодом. Эта практика только увеличивается, поскольку в 2020 году разработчики получили доступ к более чем 1,5 триллиона программных компонентов и контейнеров с открытым исходным кодом.

Вот почему библиотеки с открытым исходным кодом теперь являются прерогативой компаний.

Помимо доступности и низкой стоимости, еще одним преимуществом этих библиотек с открытым исходным кодом является то, что они позволяют ускорить цепочку поставок.

Эта стратегическая эволюция использования открытого исходного кода полезна в трех масштабах: модернизация ИТ-инфраструктуры, разработка приложений и цифровая трансформация компании.

Такое ускорение инноваций чаще всего перекликается с проблемами повышения уровня поддержки, совместимости программного обеспечения и внутреннего обучения сотрудников.

Наблюдается еще одна трудность: используемые программные зависимости происходят из сторонних источников и могут содержать уязвимости.

Издатель платформы управления с открытым исходным кодом Nexus указывает, что «эти артефакты используются в качестве повторно используемых строительных блоков, которые помещаются в общедоступные репозитории (npm, Maven Central, PyPI, NuGet Gallery, RubyGems и т. Д.), где они свободно заимствуются миллионы разработчиков стремятся быстрее внедрять инновации».

Кибер-злоумышленники атакуют основную часть программной цепочки: производственный код, написанный не разработчиком.

Кибератаки нового поколения, основанные на программном обеспечении с открытым исходным кодом

Эти кибератаки, называемые «путаницей зависимостей», состоят в изменении сценариев установки, используемых разработчиками программного обеспечения с открытым исходным кодом, путем их замены совершенно обманчивыми вредоносными программами, что приводит к нарушению работы внутренней системы компании.

Почему их трудно остановить?

Проекты с открытым исходным кодом основаны на вкладе большого сообщества людей, участвующих в постоянном улучшении предлагаемого программного обеспечения, трудно оценить хорошие или плохие намерения каждого;

Проекты с открытым исходным кодом иногда зависят от других дополнительных проектов (плагинов) с открытым исходным кодом, которые сами по себе содержат уязвимости;

Дух открытого исходного кода основан на общем доверии в сообществе людей.

Кибер-злоумышленники больше не хотят использовать известные уязвимости в открытом исходном коде.Они применяют все более изощренные методы, чтобы проникнуть в основу цепочки поставок программного обеспечения искомпрометировать ее различные компоненты.

Эти кибератаки «нового поколения» предоставляют кибератакам значительную свободу действий, упрощая загрузку вредоносных программ и их дальнейшее распространение во внутренние бизнес-приложения.

Цифры, которые вызывают тревогу

Согласно последнему ежегодному отчету Sonatype, озаглавленному «Состояние цепочки поставок программного обеспечения в 2020 году», оказывается, что 29% программного обеспечения с открытым исходным кодом содержит по крайней мере один известный недостаток безопасности…

21% команд разработчиков испытали хотя бы одно нарушение безопасности с открытым исходным кодом за последние двенадцать месяцев.

Сообщалось, что в 2020 году количество кибератак, направленных на проникновение в эти программные компоненты, увеличилось на 430%. Предполагается, что к 2021 году они снова вырастут до 650%...» ***(Gŭrard Haas, Marussia Samot. Les logiciels open source, nouvelle cible des cyberattaques // HAAS Avocats (https://info.haas-avocats.com/droit-digital/les-logiciels-open-source-nouvelle-cible-des-cyberattaques). 01.10.2021).***

***

«Исследователи из американского университета разработали новую атаку с захватом отпечатков пальцев и спуфингом в браузере, которая называется Gummy Browsers. Они предупреждают, насколько легко осуществить атаку и какие серьезные последствия она может иметь.

Цифровой отпечаток пальца - это уникальный онлайн-идентификатор, связанный с конкретным пользователем, на основе комбинации характеристик устройства. Эти характеристики могут включать IP-адрес пользователя, версию

браузера и ОС, установленные приложения, активные надстройки, файлы cookie и даже то, как пользователь перемещает мышь или вводит текст на клавиатуре.

Веб-сайты и рекламодатели могут использовать эти отпечатки пальцев, чтобы подтвердить, что посетитель - человек, отслеживать пользователя между сайтами или для целевой рекламы. Отпечатки пальцев также используются как часть некоторых систем аутентификации, позволяя потенциально обходить MFA или другие функции безопасности при обнаружении действительного отпечатка пальца.

Цифровые отпечатки пальцев настолько ценны, что их продают на торговых площадках в темной сети, что позволяет злоумышленникам и мошенникам подделывать онлайн-отпечатки пальцев пользователей, чтобы упростить захват учетных записей или мошенничество с рекламой.

Мармеладные браузеры

Атака «липких браузеров» - это процесс получения отпечатка пальца человека, заставляя его посетить веб-сайт, контролируемый злоумышленником, а затем использовать этот отпечаток на целевой платформе для подделки личности этого человека.

После создания отпечатка пальца пользователя с использованием существующих или настраиваемых скриптов исследователи разработали следующий метод обмана пользователя на других сайтах:

Внедрение сценария- подмена отпечатка пальца жертвы путем выполнения сценариев (с помощью Selenium), которые обслуживают значения, извлеченные вызовами API JavaScript.

Инструмент настройки и отладки браузера - оба могут использоваться для изменения атрибутов браузера на любое настраиваемое значение, влияющее как на API JavaScript, так и на соответствующее значение в заголовке HTTP.

Модификация скрипта - изменение свойств браузера с поддельными значениями путем изменения скриптов, встроенных в веб-сайт, перед их отправкой на веб-сервер.

Захватив отпечаток пальца жертвы только один раз, исследователи заявили, что они могут обмануть современные системы снятия отпечатков пальцев, такие как FPStalker и Panopliclick, на длительное время.

«Наши результаты показали, что Gummy Browsers могут успешно прозрачно олицетворять браузер жертвы почти все время, не влияя на отслеживание законных пользователей», - поясняют исследователи в опубликованной вчера статье Arxiv.

«Поскольку получение и подмена характеристик браузера не ведется ни пользователем, ни удаленным веб-сервером, браузеры Gummy могут быть легко запущены, но при этом их трудно обнаружить»

Их тесты дали истинно положительный результат 0,9 и не вызвали тревогу, чтобы предупредить обманутого пользователя о том, что его «личность» в сети была украдена.

Атакой можно сильно злоупотреблять

Исследователи заявляют, что злоумышленники могут легко использовать атаку Gummy Browsers, чтобы обмануть системы с помощью снятия отпечатков пальцев.

«Влияние Gummy Browsers может быть разрушительным и продолжительным для онлайн-безопасности и конфиденциальности пользователей, особенно с учетом того, что отпечатки пальцев браузера начинают получать широкое распространение в реальном мире», - предупреждают исследователи.

«В свете этой атаки наша работа поднимает вопрос о том, безопасно ли использование отпечатков браузера в больших масштабах».

Атака может подделать личность пользователя, чтобы скрипт выглядел как человек, а не как бот, и ему показывалась таргетированная реклама для мошенничества с рекламой.

Атака Gummy Browsers также может помочь обойти функции безопасности, используемые для обнаружения законных пользователей в службах аутентификации. Примеры систем аутентификации, использующих отпечатки пальцев, включают Oracle,InauthиSecureAuth IdP.

Например, SecureAuth ADP можно настроить так, чтобы не выполнять многофакторную аутентификацию при обнаружении легитимного отпечатка пальца.

«Когда пользователь входит в область, можно использовать распознавание устройств, чтобы предотвратить необходимость использования MFA каждый раз, когда они обращаются к области», - поясняется в статье поддержки SecureAuth IDP.

Наконец, многие банки и сайты розничной торговли используют снятие отпечатков пальцев как часть своих механизмов обнаружения мошенничества, которые можно обойти, подделав личность законного пользователя». ***(Bill Toulas. New Gummy Browsers attack lets hackers spoof tracking profiles // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-gummy-browsers-attack-lets-hackers-spoof-tracking-profiles/). 20.10.2021).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Команда подразделения 42 Palo Alto Networks обнаружила, что почти все сторонние облачные контейнеры, развернутые в общедоступных облаках, имеют уязвимости и неправильные конфигурации, которые подвергают организации атакам на цепочки поставок.

Согласно отчету Unit 42 Cloud Threat Report 2H 2021, 96% сторонних контейнерных приложений, развернутых в облачной инфраструктуре, содержат известные уязвимости. А 63% сторонних шаблонов кода, используемых при построении облачной инфраструктуры, содержали небезопасные конфигурации.

Исследователи отметили, что продвинутые постоянные злоумышленники могут использовать эти недостатки безопасности, чтобы захватить облачную инфраструктуру и выполнить атаки на цепочку поставок, такие как SolarWinds и Kaseya.

Облачные контейнеры являются вероятными источниками атак в цепочке поставок.

Команда проанализировала данные из нескольких общедоступных источников по всему миру, чтобы выявить растущую угрозу атак на цепочки поставок программного обеспечения, поскольку большинство организаций внедряют цифровую трансформацию.

Исследователи обнаружили, что в большинстве облачных контейнеров есть непроверенный сторонний код, который может создавать уязвимости для атак на цепочку поставок. Кроме того, сторонний код имеет зависимости, видимость безопасности которых была ограничена.

По мнению исследователей, злоумышленники могут использовать эту лазейку для создания уязвимостей для выполнения атак на цепочку поставок.

«Команды продолжают пренебрегать безопасностью DevOps, отчасти из-за недостаточного внимания к угрозам цепочки поставок. «Нативные для облака» приложения имеют длинную цепочку зависимостей, и эти зависимости имеют собственные зависимости », - заявили они.

Исследователи постулировали, что DevOps и группы безопасности должны получить представление о перечне материалов по программному обеспечению в облачных контейнерах во всех облачных рабочих нагрузках, чтобы оценить основные угрозы безопасности на каждом этапе цепочки зависимостей программного обеспечения и создать меры по их устранению.

Не обошли стороной и организации со зрелой облачной безопасностью

К сожалению, эти угрозы безопасности затронули не только новичков в облаке, но и организации со зрелой позицией в области безопасности облачных вычислений.

Исследователи Unit 42 провели упражнение Red Team на крупном заказчике SaaS и обнаружили несколько недостатков, которые подвергали клиента потенциальным атакам на цепочку поставок. Исследователи имитировали злоумышленника с ограниченными правами доступа и попытались получить доступ к средам непрерывной интеграции (CI) организации.

Удивительно, но им удалось загрузить все репозитории GitLab и идентифицировать 80 000 облачных ресурсов с 154 уникальными репозиториями CI. Они также обнаружили 26 жестко запрограммированных пар ключей IAM, включая пять токенов сеанса и ключи доступа.В то время как ключи сеанса истекают в течение нескольких часов, ключи доступа могут позволить APT взломать среду CI во время атак на цепочку поставок.

Распространенные проблемы безопасности в IaC

Точно так же команда проанализировала 4055 шаблонов Terraform и 38 480 файлов Terraform с помощью Bridgecrew's Checkov. Они обнаружили, что 63% шаблонов Terraform содержат одну или несколько небезопасных конфигураций, а 49% имеют как минимум одну критическую или крайне небезопасную конфигурацию. Ошибка неправильной настройки затронула как минимум 2500 модулей в нескольких областях, таких как управление идентификацией и доступом, шифрование, работа в сети, ведение журнала, а также резервное копирование и восстановление.

Исследователи Unit 42 также проанализировали 3155 диаграмм Helm и 8805 файлов YAML. Они обнаружили, что 99,95% диаграмм Helm содержат одну или несколько небезопасных конфигураций, а 6% содержат как минимум одну критическую или крайне небезопасную конфигурацию.

Исследователи также проанализировали 1544 облачных контейнера, используемых в диаграммах Kubernetes Helm.Эти облачные контейнеры размещались в общедоступных реестрах, таких как Docker Hub, Google Container Registry (GCR) и Quay. Они обнаружили, что 96% облачных контейнеров и 91% образов контейнеров содержат по крайней мере одну критическую или высокую уязвимость.Исследователи пришли к выводу, что уязвимости могут появиться, если специалист по сопровождению диаграмм Helm не сможет обновить диаграммы или если разработчик изображений не сможет обновить изображения.

«Учитывая давление бизнеса на команды разработчиков, непрактично предполагать, что вы можете укрепить себя, чтобы обеспечить полную безопасность с помощью проверки IaC и управления уязвимостями, - сказала Саумитра Дас, технический директор и соучредитель Blue Hexagon.- Организации не могут обеспечить соблюдение IaC в масштабах всей компании и даже исправления известных CVE могут занять недели и месяцы только для внешних рабочих нагрузок.

«Даже для более простых исправлений, таких как неправильная конфигурация, требуются дни и недели даже после обнаружения. Этот отчет соответствует тому, что мы видим в организациях, пытающихся обеспечить безопасность в облаке. Ключ состоит не в том, чтобы класть все яйца в корзину с левым переключением, а в непрерывном обнаружении угроз жизненного цикла и реагировании в облаке», - заключил он». ***(ALICIA HOPE. Most Cloud Containers Deployed on Public Registries Contain Vulnerabilities and Misconfigurations That Could Result In a Supply Chain Attack // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/most-cloud-containers-deployed-on-public-registries-contain-vulnerabilities-and-misconfigurations-that-could-result-in-a-supply-chain-attack/). 15.10.2021).***

***

«BillQuick сообщил, что будет выпущен краткосрочный патч для устранения некоторых уязвимостей, выявленных в эти выходные Huntress.

В пятницу в блоге исследователь безопасности Huntress Калеб Стюарт сказал, что команда ThreatOps компании «обнаружила критическую уязвимость в нескольких версиях BillQuick Web Suite, системы учета времени и биллинга от BQE Software».

«Хакеры смогли успешно использовать CVE-2021-42258, используя его для получения первоначального доступа к американской инженерной компании, и развернуть программы-вымогатели в сети жертвы. Учитывая самопровозглашенную базу пользователей BQE в 400 000 пользователей по всему миру, злонамеренная кампания нацеливание на их клиентскую базу вызывает озабоченность», - сказал Стюарт.

«Этот инцидент подчеркивает повторяющуюся закономерность, характерную для программного обеспечения SMB: хорошо зарекомендовавшие себя поставщики очень мало делают для активной защиты своих приложений и подвергают своих ничего не подозревающих клиентов значительной ответственности в случае неизбежной утечки конфиденциальных данных и / или выкупа».

Huntress также обнаружила восемь других уязвимостей: CVE-2021-42344, CVE-2021-42345, CVE-2021-42346, CVE-2021-42571, CVE-2021-42572, CVE-2021-42573, CVE-2021-42741, CVE. -2021-42742.

… компания BQE Software сообщила, что их команда инженеров знает о проблемах с BillQuick Web Suite, который клиенты используют для размещения BillQuick, и сообщила, что уязвимость была исправлена.

«Huntress также выявила дополнительные уязвимости, которые мы активно исследуем. Мы ожидаем, что к концу дня 26.10.2021 будет выпущено краткосрочное исправление для уязвимостей BQE Web Suite вместе с точным графиком, когда будет реализовано полное исправление», - добавил представитель.

«Проблема с BQE Web Suite затрагивает менее 10% наших клиентов; мы будем проактивно сообщать каждому из них о существовании этих проблем, о том, когда они могут ожидать решения проблем и какие шаги они могут предпринять в промежуточный период. чтобы свести к минимуму их воздействие».

Huntress объяснила, как им удалось воссоздать атаку на основе SQL-инъекций, которую, как они показали, можно использовать для доступа к данным BillQuick клиентов и выполнения вредоносных команд на их локальных серверах Windows.

Huntress заявила, что работала с BQE Software над этим вопросом, и поблагодарила компанию за оперативность и серьезное отношение к проблемам.

Но в сообщении блога отмечается, что ошибка может быть легко вызвана «простым переходом на страницу входа и вводом одинарной кавычки (` '`)».

«Кроме того, обработчики ошибок для этой страницы отображают полную трассировку, которая может содержать конфиденциальную информацию о коде на стороне сервера», - написал Стюарт.

CVE-2021-42258 былисправлен BQE Software 7 октября в WebSuite 2021 версии 22.0.9.1. Но восемь других проблем все еще нуждаются в исправлении.

Стюарт сообщил BleepingComputer, что неназванные хакеры использовали CVE-2021-42258 в качестве точки входа в инженерную компанию США в рамках атаки вымогателей, которая произошла в выходные дни Дня Колумба. В новостях сообщалось, что группа вымогателей не оставила записки о выкупе и не имела легко узнаваемого имени». ***(Jonathan Greig. BillQuick says patch coming after Huntress report identifies vulnerabilities used in ransomware attack // ZDNet (https://www.zdnet.com/article/billquick-says-patch-coming-after-huntress-report-identifies-vulnerabilities-used-for-ransomware/). 25.10.2021).***

***

«Компания-разработчик программного обеспечения JFrog стала последней организацией, которая была назначена программой CVE в качестве центра нумерации CVE.

В настоящее время 189 организаций из 31 страны участвуют в качестве CNA, более 100 из которых находятся в США.

Классификация позволит компании присваивать идентификационные номера CVE вновь обнаруженным уязвимостям безопасности и публиковать соответствующие данные в связанных записях CVE для публичного использования.

Теперь JFrog будет уполномочен работать с сообществом кибербезопасности над различными проблемами безопасности и предоставлять клиентам дифференцированные данные по исправлению ситуации с помощью JFrog Xray.

Моран Ашкенази, директор по информационной безопасности и вице-президент по безопасности в JFrog, сказал, что, став CNA, они смогут помогать исследователям в области безопасности проверять и сортировать их уязвимости, а также обеспечивать безопасность двоичных файлов компаний за счет сотрудничества в борьбе с потенциальными угрозами с более широким сообществом специалистов по безопасности.

«Количество угроз безопасности в программном обеспечении и подключенных устройствах продолжает расти. Как CNA, мы уполномочены работать с сообществом, чтобы ускорить обнаружение угроз и быстро обмениваться информацией о новых уязвимостях - до того, как они поставят под угрозу бизнес», - сказал Ашкенази.

Записи CVE используются во всем мире для выявления и систематизации критических уязвимостей программного обеспечения, которые обнаруживаются ежедневно. Такие компании, как JFrog, присваивают каждой уязвимости идентификаторы CVE.

Технический директор JFrog Security Асаф Карас сказал, что с обозначением CNA компания может более эффективно и действенно распространять результаты своих исследований среди клиентов и программного сообщества в целом - как для недавно обнаруженных уязвимостей, так и для существующих записей CVE, которые могут быть неточными или неполными.

«Этим достижением JFrog подтверждает свое стремление быть активным участником сообщества безопасности и предоставлять нашим клиентам масштабируемые, безопасные решения DevSecOps для разработки на периферии», - сказал Карас». ***(Jonathan Greig. JFrog becomes latest organization authorized as numbering authority for vulnerabilities exposure // ZDNet (https://www.zdnet.com/article/jfrog-becomes-latest-organization-authorized-as-numbering-authority-for-vulnerabilities-exposure/). 04.10.2021).***

***

«Реализации Cisco SD-WAN уязвимы для серьезной уязвимости повышения привилегий в операционной системе IOS IE, которая может привести к выполнению произвольного кода.

Портфель Cisco SD-WAN позволяет компаниям любого размера подключать разрозненные офисы через облако с использованием различных сетевых технологий, включая стандартные подключения к Интернету. Устройства в каждом месте обеспечивают расширенную аналитику, мониторинг, спецификации

производительности для конкретных приложений и автоматизацию для любого соединения в глобальной сети компании.

Между тем, IOS XE - это операционная система производителя, которая запускает эти устройства. Это комбинация ядра Linux и монолитного приложения, которое работает поверх этого ядра.

Ошибка (CVE-2021-1529) представляет собой проблему внедрения команд в ОС, которая позволяет злоумышленникам выполнять неожиданные опасные команды непосредственно в операционной системе, которые обычно недоступны. Он специально существует в интерфейсе командной строки (CLI) для программного обеспечения Cisco IOS XE SD-WAN и может позволить аутентифицированному локальному злоумышленнику выполнять произвольные команды с привилегиями root.

«Уязвимость связана с недостаточной проверкой ввода системным CLI», - говорится в сообщении Cisco, опубликованном на этой неделе. «Успешный эксплойт может позволить злоумышленнику выполнять команды в базовой операционной системе с привилегиями root».

В сообщении также отмечалось, что путь к эксплуатации будет включать аутентификацию на уязвимом устройстве и отправку «созданных входных данных» в системный интерфейс командной строки. Успешная компрометация предоставит злоумышленнику возможность читать и записывать любые файлы в системе, выполнять операции от имени любого пользователя, изменять конфигурацию системы, устанавливать и удалять программное обеспечение, обновлять ОС и / или прошивку и многое другое, включая последующие доступ в корпоративную сеть.

CVE-2021-1529 имеет оценку 7,8 по шкале критичности уязвимости CVSS, а исследователи и Агентство по кибербезопасности и безопасности инфраструктуры (CISA)предупредили, что предприятиям следует исправить ошибку как можно скорее.

Грег Фицджеральд, соучредитель Sevco Security, предупредил, что у некоторых организаций могут быть устаревшие устройства, все еще подключенные к их сетям, что может быть скрытой опасностью с такими ошибками.

«Подавляющее большинство организаций отлично справляются с устранением уязвимостей в известных им системах», - сказал он по электронной почте. «Проблема возникает, когда предприятия не имеют полной видимости инвентаризации своих активов, потому что даже самые отзывчивые группы ИТ и безопасности не могут исправить уязвимость для актива, который, как они знают, подключен к их сети. Заброшенные и неизвестные ИТ-активы часто являются путем наименьшего сопротивления для злоумышленников, пытающихся получить доступ к вашей сети или данным».

Это только последняя уязвимость SD-WAN, которую Cisco исправила в этом году. В январе он исправил несколько критических ошибок переполнения буфера и внедрения команд в SD-WAN, наиболее серьезные из которых могли быть использованы удаленным злоумышленником, не прошедшим проверку подлинности, для выполнения произвольного кода в уязвимой системе с привилегиями root.

В мае Cisco устранила две критические уязвимости системы безопасности в программном обеспечении SD-WAN vManage, одна из которых могла позволить неаутентифицированному злоумышленнику выполнить удаленное выполнение кода (RCE) в корпоративных сетях или украсть информацию.

И только в прошлом месяце Cisco обнаружила две критические уязвимости системы безопасности, затрагивающие программное обеспечение IOS XE и его SD-WAN, наиболее серьезная из которых допускает неаутентифицированный RCE и отказ в обслуживании (DoS)». ***(Tara Seals. Cisco SD-WAN Security Bug Allows Root Code Execution // Threatpost (https://threatpost.com/cisco-sd-wan-bug-code-execution-root/175669/). 22.10.2021).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Входящий в ГК «Ростех» концерн «Автоматика» совместно с АО «Национальная инжиниринговая корпорация» (НИК) и компанией «Ти Хантер» создадут программно-аппаратный комплекс для борьбы с киберпреступлениями. Соответствующее соглашение было подписано на конференции «Микроэлектроника-2021» в Крыму.

«Также планируется создание информационно-аналитической платформы анализа по открытым источникам данных. Она может быть востребована у государственных организаций»,— уточнил гендиректор концерна Андрей Моторко…

Речь идет о применении технологии OSINT (Open Source Intelligence, разведка по открытым источникам). «Например, следователь сможет загрузить в систему e-mail или номер телефона подозреваемого, а программный комплекс, используя этот фрагмент, сопоставит с ним массивы данных: IP-адреса, информацию из платежных систем и рекламные идентификаторы — более 40 параметров. На выходе следователь получит отчет о личности объекта с источниками информации в текстовом и графическом виде»,— объяснил руководитель департамента информационно-аналитических исследований «Ти Хантера» Игорь Бедеров.

НИК предложит решение службам безопасности коммерческих компаний и правоохранительным органам, уточнил член совета директоров компании Евгений Елфимов.

Сбор цифрового профиля злоумышленника по контактным данным, которые он случайно обнародовал, позволяет его идентифицировать, подтверждает директор центра противодействия кибератакам Solar JSOC компании «Ростелеком-Солар» Владимир Дрюков. «Это иногда используется при поиске хакеров и кибергруппировок»,— отмечает он.

Разработчикам придется в какой-то мере составить конкуренцию Google и «Яндексу», создавая решение, которое будет настолько же точно находить

совпадения с открытыми источниками, отмечает директор по развитию web-технологий Artezio Сергей Матусевич. «Возможно, комплекс будет работать уже с выдачей поисковиков»,— добавляет он.

При этом работа по открытым источникам не позволит выявить опытных преступников: они используют анонимные почтовые серверы, ресурсы даркнета, до которых система вряд ли доберется, указывает господин Дрюков.

Использование такой системы должно контролироваться вышестоящими должностными лицами и судами, уверен эксперт «РосКомСвободы» Владимир Ожерельев. «Но на практике это происходит редко, и в результате данные о гражданах продаются на черном рынке»,— отмечает он. По его мнению, результаты обработки данных в системе должны проходить ручную проверку для использования в качестве доказательств». ***(Киберпреступников будут искать в открытых источниках // РосКомСвобода (https://roskomsvoboda.org/post/cyberslezhka-po-otkrytym-dannym/). 07.10.2021).***

***

«Агентство BBC New інформує, що компанія Google надає деяким користувачам особливі інструменти для захисту.

Компанія запропонувала 10 тис. клієнтів безкоштовні електронні ключі на пристроях USB. Пропозиція стосується лише окремих користувачів, які мають високий ризик взлому – політики, правозахисники. Подібний спосіб захисту забезпечується двофакторною аутентифікацією – тобто додається ще один рівень безпеки, крім паролю. Шейн Хантлі, директор групи аналізу загроз, заявив у пості Twitter, що наприкінці вересня виявили масовану атаку на 10 тис. користувачів Google. Хакерський напад здійснила група APT28, також відома як Fancy Bear. Кіберзловмисники пов'язані з російською розвідкою, як стверджують уряди США та Великобританії. Напад відносився до категорії фішингу: люди отримували електронні листи від поважних електронних сервісів, у яких їх просили підтвердити особисті дані, банківські реквізити та іншу конфіденційну інформацію. Заволодівши нею, злочинці займались вимаганням та викрадали кошти. Розслідування кібернападів у 2016 р. показало, що саме група Fancy Bear стояла за фішинговою атакою на 4 тис. акаунтів Google. Серед цілей були учасники виборчої кампанії Гілларі Клінтон та Демократична партія США. Хантлі зазначає, що до подібних атак повинні бути завжди готові активісти, журналісти, урядовці. Саме після низки подібних інцидентів Google оголосила, що 10 тис. користувачів отримають ключі безпеки "Titan". Номінальна ціна «Titan» – 41 дол., але компанія свої обраним клієнтам надає їх безкоштовно. Розповсюджуватимуть ключі організації-партнери.

Покращуватиметься захист і рядових клієнтів. Google наполягатиме на двофакторній авторизації ще для 150 млн. акаунтів електронної пошти та для двох млн. акаунтів Youtube. Фахівці стверджують: люди у більшій безпеці, якщо використовують одночасно два інструменти: пароль, «який ви знаєте», та фізичний пристрій (смартфон, USB-накопичувач), «який ви реально тримаєте у руках». Такий захист дуже ускладнює доступ зловмисників до вашого облікового запису…» ***(Елена Бурдейная. Як Google захищає від хакерів особливо важливих***

користувачів // Comments.ua (https://it.comments.ua/ua/news/technology/yak-google-zahischae-vid-hakeriv-osoblivo-vazhlivih-koristuvachiv-686112.html). 14.10.2021).

***

«По мере экспоненциального роста вычислительной мощности способность защитить наши данные от грубой силы и других типов атак становится все более сложной, поскольку масштаб и изощренность кибератак по-прежнему ставят под сомнение способность компаний внедрять эффективный контроль доступа к данным и шифрование.

Для повышения безопасности данных компания QuintessenceLabs из Канберры, австралийский поставщик решений квантовой кибербезопасности, защищает конфиденциальные данные с помощью генераторов квантовых случайных чисел и передового программного обеспечения для управления доступом к данным. Стартап уже собрал 25 миллионов долларов в раунде серии B для повышения своей безопасности в квантовых решениях.

Последнее финансирование возглавляли Main Sequence и TELUS Ventures при участии InterValley Venturesи Capital Property Group, поддерживаемых Mizuho FinancialGroup.

QuintessenceLabs будет использовать финансирование Series B для расширения своей клиентской базы, включая частные и государственные организации в сфере финансовых услуг, облачных провайдеров, правительственные агентства и оборонные секторы во всем мире, сказал TechCrunch генеральный директор и основатель QuintessenceLabs Викрам Шарма.

QuintessenceLabs использует квантовую физику для создания инструментов безопасности данных и разработала qStream, квантовый генератор случайных чисел (QRNG), который предоставляет ключи шифрования с полной энтропией, что означает, что они действительно случайны, объяснил Шарма. По его словам, рынок для этого типа технологий был небольшим, когда QuintessenceLabs начала свою работу в 2008 году, и потребовалось время, чтобы созреть и вывести его на коммерческий уровень.

«Мы потратили более десяти лет на разработку правильной технологии и подготовку к коммерческому внедрению», - сказал Шарма.

По словам Шармы, компания продает свою продукцию глобальным корпорациям. В прошлом году одним из значительных достижений компании было внесение в список одобренных продуктов для программы на 2 миллиарда долларов, проводимой Министерством внутренней безопасности США и направленной на усиление защиты данных во всех участвующих агентствах, сказал Шарма TechCrunch.

Компания со штаб-квартирой в Австралии открыла офис в США в 2013 году с первоначальной командой из трех человек, чтобы взять на себя более серьезные обязательства перед США.

По словам Шарма, поскольку США на сегодняшний день являются крупнейшим рынком кибербезопасности, QuintessenceLabs продолжит наращивать свою команду в США в течение следующих двух-трех лет.

По словам Шармы, Великобритания является вторым по величине рынком кибербезопасности и чем-то похожа на Австралию с точки зрения динамики рынка, правовых систем и деловой культуры. По словам Шарма, в первой половине следующего года QuintessenceLabs планирует открыть офис в Великобритании, который также является идеальным местом для штаб-квартиры в регионе EMEA. Параллельно QuintessenceLabs развивает партнерские отношения в Японии и Индии, отметил Шарма.

По словам Шармы, QuintessenceLabs отложила свои планы роста до 12-15 месяцев из-за неопределенности, вызванной глобальной пандемией. По его словам, компания будет реализовывать запланированную стратегию географического и отраслевого расширения, поскольку мир начнет открываться заново примерно в 2022 году.

Австралийское национальное научное агентство CSIRO недавно опубликовало отчет о квантовой индустрии Австралии, в котором прогнозируется, что к 2040 году объем мирового рынка квантовой индустрии составит 86 миллиардов долларов. Ожидается, что на рынок квантовой связи и кибербезопасности во всем мире будет приходиться около 16 миллиардов долларов. Согласно отчету, квантовые технологии Австралии к 2040 году, по прогнозам, принесут более 4 миллиардов долларов дохода и 16 000 новых рабочих мест.

По состоянию на сентябрь 2021 года в компании работает 50 сотрудников.

«Защита данных - наш самый ценный ресурс - как никогда важна, и мы с нетерпением ждем этого захватывающего нового этапа роста», - сказал Шарма.

«Поскольку вычислительная мощность растет экспоненциально, инструменты, необходимые для защиты критически важных данных и активов, должны оставаться на несколько шагов впереди», - сказал Билл Барти, партнер Main Sequence. «QuintessenceLabs - мировой лидер в разработке квантовых инструментов кибербезопасности, которые помогают защитить суверенный и коммерчески чувствительный бизнес и предоставляют клиентам критически важный уровень защиты». ***(Kate Park. Australian QuintessenceLabs grabs $25M to scale quantum-safe cybersecurity solutions // Verizon Media (https://techcrunch.com/2021/10/26/australian-quintessencelabs-grabs-25m-series-b-to-scale-quantum-safe-crypto-solutions/). 26.10.2021).***

***

«Программное обеспечение революционизирует то, как работает мир. Программное обеспечение переосмысливает возможности - от автомобилей без водителя до криптовалюты. Поскольку программное обеспечение лежит в основе всего, что мы делаем, мы обнаруживаем, что выпускаем код быстрее, чем когда-либо. Текущие оценки показывают, что в год пишется более 111 миллиардов строк нового кода. А наша зацикленность на стремительном развитии новейших технологий поставила безопасность приложений на препятствие, причем «за свою цену».

По мере того, как мы продолжаем накапливать долги по безопасности и бороться с нехваткой рабочей силы в сфере кибербезопасности, становится ясно, что мы живем на заимствованное время безопасности.

Дело не в том, чтобы останавливаться на наших недостатках в безопасности программного обеспечения, а в том, чтобы подчеркнуть, что мы должны мыслить масштабнее, если мы хотим решить эту критическую проблему кибербезопасности. Устранение вручную 20, 50, 100 ложных срабатываний из накопившихся 10 000 отчетов об ошибках - отчетов, количество которых увеличивается только в несколько раз каждый день, - не сдвинет иглу. И это невероятно дорого: средний инженер AppSec зарабатывает более 133 000 долларов в год, и его не хватает. Разве их время не должно быть лучше потрачено, чем обнаружение ложных срабатываний?

Что нужно, так это безопасность автономных приложений. Нам нужно решение для тестирования безопасности приложений, которое способно точно выявлять проблемы с высокой скоростью и масштабом.

Автономность - это не автоматизация

Я особенно хочу подчеркнуть острую необходимость в автономности этого следующего поколения. Не следует путать с автоматизацией. В отличие от автоматизации, автономные возможности включают в себя больше, чем выполнение заранее запрограммированной задачи на скорости машины.

Автономное тестирование безопасности приложений позволяет разумно адаптировать методы тестирования к конкретным потребностям каждого приложения - никаких готовых наборов тестов и универсального подхода. Он извлекает данные из результатов прошлых тестов и использует их, внося корректировки для следующего теста. Это позволяет группам по безопасности продукта избавиться от ручных усилий в процессе управления безопасностью приложений.

Текущие решения, такие как тестирование безопасности программного обеспечения (SAST), не являются гибкими. Они просматривают код построчно. У них также отсутствуют необходимые средства для проверки, которая решала бы проблему ложных срабатываний. Инженеры-программисты должны принять эту практику и выделить необходимое время для исследования каждого результата.

Между тем, Fuzz-тестирование - это метод динамического тестирования безопасности приложений (DAST), который отправляет искаженные входные данные целевым объектам с целью запуска плохого поведения в работающем программном обеспечении, такого как сбои, бесконечные циклы и / или утечки памяти. Такое аномальное поведение часто является признаком скрытой уязвимости.

Fuzz-тестирование - это тип динамического анализа, основанного на поведении. Первоначально в индустрии были веб-фаззеры DAST, инструменты которых не знали о самом коде. Они стали немного более продвинутыми благодаря интерактивному тестированию безопасности приложений (IAST), которое обеспечивает цикл обратной связи с кодом, но не помогает вам расширить охват, подвергая вас риску непроверенного кода. Непроверенный код - это рискованный код.

Таким образом, Fuzz-тестирование - это следующее поколение, которое автоматически обнаруживает ошибки. Нечеткое тестирование также является единственным решением для динамического анализа, которое помогает уменьшить облако неопределенности от непроверенного кода, поскольку оно постоянно расширяет охват кода. Возможность расширения вашего набора тестов помогает вам получать исправления быстрее и с большей уверенностью.

Тестирование безопасности автономных приложений на основе Fuzz-тестирования выходит за рамки простого выявления уязвимостей. Как правило, основным препятствием на пути к исправлению является то, нарушает ли оно существующие функции. Google сообщает, что 40 процентов его ошибок попадают в сбои регрессии. Путем тестирования и повторного тестирования, чтобы подтвердить, что каждая уязвимость действительно существует, разработчики могут сосредоточиться на конкретной строке кода, которая требует дальнейшего исследования, тем самым экономя время и ресурсы.

Эта проверка также критически важна для рабочих процессов непрерывной интеграции и доставки (CI / CD), поскольку она позволяет разработчикам формировать часть кода и автоматически проверять этот раздел перед слиянием с мастером.

Кроме того, тестирование безопасности автономных приложений следующего поколения включает в себя символьное выполнение, которое может абстрагировать входные данные и, следовательно, отображать больший объем кода, увеличивая охват в его тестовых примерах. Часто это области кода, в которых находятся уязвимости нулевого дня, и области, в которых обычное тестирование безопасности не проверяется.

Автономная безопасность

Только за последний год мы наблюдали сдвиги, которые еще больше подтверждают необходимость более автономной безопасности приложений:

Gartner добавила нечеткое тестирование, технологию, лежащую в основе автономного тестирования безопасности приложений, к своим критическим возможностям AST. В отчете Gartner Critical Capabilities изложены критерии для попадания в его Magic Quadrant.

Повышение уровня начальника службы безопасности продукта. Подобно усилению роли CISO и дисциплины информационной безопасности, мы видим, как организации внедряют дисциплину безопасности продукта и предоставляют CPSO место за исполнительным столом. Группы безопасности продуктов несут ответственность за безопасность продуктов, которые они предлагают, что существенно отличается от обеспечения безопасности операций компании.

Поставщики репозиториев Git входят в сферу тестирования безопасности приложений. GitHub и GitLab сделали шаги на рынке тестирования безопасности приложений, подчеркнув необходимость дать разработчикам возможность писать безопасный код .GitLab, в частности, приобрел не одно, а два решения для тестирования фаззинга». ***(David Brumley. Why the Next-Generation of Application Security Is Needed // Threatpost (https://threatpost.com/next-generation-application-security/175765/). 26.10.2021).***

***

«Компанія Eset повідомляє про вихід нової версії продуктів Eset NOD32 Antivirus, Eset Internet Security таEset Smart Security Premium для користувачів операційної системи Windows. Основними нововведеннями стали функція LiveGuard для додаткового захисту від невідомих загроз, платформа для управління безпекою Eset Home, атакож інші вдосконалення можливостей для всебічної безпеки пристроїв.

В умовах постійних кібератак забезпечення захисту власних пристроїв стає необхідністю. Оскільки сьогодні найактивніше використовуються смартфони, управління безпекою з їх допомогою є вирішальним.

Саме тому було оновлено платформу для управління безпекою домашніх пристроїв Eset Home (раніше myEset), яка забезпечує повний огляд всіх рішень Eset для операційних систем Windows та Android. Зокрема користувачі можуть бачити поточні статуси захисту різних пристроїв, підключених до їх облікових записів.

Варто зазначити, що Eset Home доступна через веб-портал тамобільні додатки для Android таiOS з можливістю управління безпекою находу. Застосунки дозволяють користувачам додавати ліцензії таділитися ними з сім'єю та друзями, ачерез веб-портал можна додатково здійснювати налаштування «Управління паролями», «Антикрадієм» та «Батьківським контролем».

В оновленому рішенні захист онлайн-платежів тепер працює за замовчуванням, захищаючи будь-який підтримуваний браузер за допомогою посиленого режиму. Завдяки методам виявлення на основі поведінки покращено захист від програм-вимагачів, а також удосконалено захист від додаткових шкідливих технік.

Нова функція LiveGuard (реалізована вEset Smart Security Premium) забезпечує додатковий рівень захисту користувачів від раніше невідомих загроз, запобігаючи запуску шкідливого коду. Цей сервіс аналізує підозрілі файли, включно з документами, скриптами, інсталяторами та виконуваними файлами, у безпечному середовищі пісочниці.

Оновлене управління паролями (доступне вEset Smart Security Premium) передбачає покращений рівень безпеки та простоту використання. Варто зазначити, що управління паролями доступне у всіх основних браузерах як розширення та на пристроях Android таiOS як окремий додаток. Крім цього, оновлений функціонал забезпечує підтримку KeePass та Microsoft Authenticator». ***(Eset випускає п'ятнадцяту версію лінійки продуктів для захисту пристроїв в домашньому офісі // Компьютерное Обозрение (https://ko.com.ua/eset_vipuskaye_p_yatnadcyatu_versiyu_linijki_produktiv_dlya_zahistu_pristroyiv_v_domashnomu_ofisi_139103). 21.10.2021).***

***

«Платформа кибербезопасности Varonis, предназначенная для защиты корпоративных данных от несанкционированного доступа и киберугроз, интегрирована с глобальной системой управления облачными хранилищами Panzura CloudFS8Defend.

Хранение данных в облаке стало дл множества компаний технологическим стандартом. Однако само по себе использование облачных хранилищ, будь то общедоступные, частные или гибридные системы, неспособно обеспечить надежную защиту от действий вымогателей, промышленного шпионажа или инсайдеров. Сотрудничество Varonis иPanzura предоставляет пользователям доступ ксистеме защиты информации, включая персональные данные и коммерческую тайну.

Panzura CloudFS обеспечивает целостное представление пользовательских данных, втом числе ивтех случаях, когда для их размещения используются разные облачные хранилища: публичные, частные или гибридные, вне зависимости от локаций, в которых они базируются.

Интеграция с платформой кибербезопасности Varonis открывает для пользователей Panzura возможности автоматического мониторинга и классификации данных, защиты от угроз, связанных с проникновением в инфраструктуру программ-вымогателей, активностью инсайдеров, атакже мониторинга аномального поведения благодаря поведенческому анализу.

Благодаря этой интеграции неструктурированные данные организаций получили надежную комплексную защиту от киберугроз с возможностью масштабирования. Компании, использующие Panzura CloudFS8Defend, теперь могут сформировать единый источник данных, хранящихся в нескольких облачных системах и локациях, объединенный единой файловой системой и нетребующий репликации». ***(Varonis защитит данные в облачных хранилищах под управлением Panzura CloudFS // Компьютерное Обозрение (https://ko.com.ua/varonis_zashhitit_dannye_v_oblachnyh_hranilishhah_pod_upravleniem_panzura_cloudfs_139183). 28.10.2021).***

***

«Чешская компания по разработке программного обеспечения для кибербезопасности Avast создала и выпустила инструмент для дешифрования, чтобы помочь жертвам программы-вымогателя Babuk бесплатно восстановить свои файлы.

По данным Avast Threat Labs, дешифратор Babuk был создан с использованием утекшего исходного кода и ключей дешифрования.

Бесплатный дешифратор может использоваться жертвами Бабука, чьи файлы были зашифрованы с использованием следующих расширений: .babuk,.babyk,.doydo.

Telegram запускает рекламную программу для публичных каналов Жертвы программы-вымогателя Babuk могут загрузить инструмент дешифрования с серверов Avast и сразу расшифровать целые разделы, используя инструкции, отображаемые в пользовательском интерфейсе дешифратора». ***(Выпущен дешифратор Babuk для бесплатного восстановления файлов // SecureNews (https://securenews.ru/babuk-ransomware-decryptor-released-to-recover-files-for-free/). 27.10.2021).***

***