**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

№ 2 (лютий)

Київ – 2023

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., 2023.– №2 (лютий) . – 199 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», 2023
© Національна бібліотека України імені В.І. Вернадського, 2023

ЗМІСТ

Кібервійна проти України

«Минулий рік розпочався для України із масштабних кібератак, які фактично стали першою фазою повномасштабного російського вторгнення.

Із якими викликами у цифровій сфері Україна зустріла 2023 рік?

Чому у чергу за українським додатком «Дія» вже вишикувалась низка країн?

Чи планує Україна проводити у «Дії» вибори та перепис населення?

Коли і завдяки чому може відбутись технологічний перелом на фронті?

Та коли українців припинять блокувати у Facebook, Instagram та TikTok через пости про російську агресію?

Про усе це Радіо Свобода поспілкувалось із віцепрем'єром та міністром цифрової трансформації Михайлом Федоровим…» ***(Софія Середа. «Ми платили мільйони гривень за кібератаки на «Дію». Інтерв'ю із міністром Михайлом Федоровим // Радіо Свобода (https://www.radiosvoboda.org/a/interview-fedorov-mintsyfry-diya-kiberarmiya/32253147.html). 04.02.2023).***

***

«Російська хакерська група, відома як «Нодарія» (UAC-0056), використовує нову шкідливу програму для крадіжки інформації «Graphiron» для крадіжки даних українських організацій. Зловмисне програмне забезпечення на основі Go може збирати широкий діапазон інформації, включаючи облікові дані облікового запису, дані системи та програм. Зловмисне програмне забезпечення також буде робити знімки екрана та вилучати файли зі зламаних машин. Команда дослідження загроз Symantec виявила, що Nodaria використовувала Graphiron для атак принаймні з жовтня 2022 року до середини січня 2023 року.

Graphiron складається із завантажувача та додаткового корисного навантаження для крадіжки інформації. Після запуску завантажувач перевірить наявність різноманітного програмного забезпечення безпеки та інструментів аналізу зловмисного ПЗ, і, якщо їх не виявлено, завантажить компонент, що викрадає інформацію. Деякі з процесів, які перевіряє завантажувач, включають BurpSuite, Charles, Fiddler, rpcapd, smsniff, Wireshark, x96dbg, ollydbg та idag.

Зловмисне програмне забезпечення використовує такі імена, як OfficeTemplate.exe та MicrosoftOfficeDashboard.exe, щоб маскуватися під компонент Microsoft Office у зламаній системі.

Його можливості включають наступне:

Прочитайте MachineGuid

Отримайте IP-адресу з https://checkip.amazonaws.com

Отримати ім’я хоста, інформацію про систему та інформацію про користувача

Крадіть дані з Firefox і Thunderbird

Викрасти приватні ключі з MobaXTerm.
Викрасти відомі хости SSH
Викрасти дані з PuTTY
Викрасти збережені паролі
Робіть скріншоти
Створіть каталог
Список каталогу
Виконайте команду оболонки
Викрасти довільний файл

Зловмисне програмне забезпечення використовує наведений нижче код PowerShell, щоб викрасти паролі зі сховища Windows, вбудованого в систему менеджера паролів, де збережені облікові дані зберігаються в зашифрованому вигляді AES-256.

```
[void][Windows.Security.Credentials.PasswordVault,Windows.Securit
y.Credentials,ContentType=WindowsRuntime];$vault = New-Object
Windows.Security.Credentials.PasswordVault;$vault.RetrieveAll() |
% { $_.RetrievePassw

ord();$_} | Select UserName, Resource, Password | Format-Table -
HideTableHeaders
```

Код PowerShell для отримання паролів користувачів

Graphiron використовує шифрування AES із жорстко закодованими ключами для зв'язку із сервером C2 через порт 443, що заслуговує на увагу подібності до старих інструментів Nodaria, таких як GraphSteal і GrimPlant.

Nodaria є тим самим загрозником, який розгорнув підроблене програмне забезпечення-вимагач під назвою «WhisperGate» в українських мережах у січні 2022 року, виконуючи деструктивні атаки знищення даних. Як правило, російські хакери доставляють свою корисну інформацію цілям за допомогою фішингових електронних листів, а війна, що триває, дає багато можливостей для ефективних приманок». ***(Від Володимир. Російські хакери використовують в Україні новий викрадач інформації Graphiron // Український телекомунікаційний портал portaltele (https://portaltele.com.ua/news/cybersecurity/rosijski-hakery-vykorystovuyut-v-ukrayini-novyj-vykradach-informatsiyi-graphiron.html). 08.02.2023).***

***

«…Спустя год после того, как Россия начала прямую захватническую войну на Украине, кибервойна, которую, как многие опасались, развяжет Москва, так и не состоялась. На самом деле, хотя кибероперации были составной частью войны России, а кибербезопасность — необходимостью обороны Украины, кибератаки не сыграли решающей роли.

России явно не удалось захватить контроль над Украиной, понеся при этом огромные потери и вызвав массовый террор, разрушения и смерть. Но использование Россией кибератак является иллюстрацией того, что полезность кибератак в реальной войне ограничена.

Поскольку российские войска в основном зашли в тупик на востоке Украины, кибератаки не дают России волшебной возможности наконец захватить власть. В то же время продолжающееся выживание Украины требует, чтобы она поддерживала надежную киберзащиту, что до сих пор она продолжала делать, отчасти благодаря обширной помощи западных технологических компаний.

«Кибероперации очень трудно интегрировать в обычные военные операции…, но они продолжают функционировать как оружие террора… против гражданского населения», сообщает Джо Словик, менеджер по анализу угроз в Huntress.

Снижение важности кибератак можно проследить по темпу, с которым Россия запускала их для поддержки военных целей. Пик этих так называемых «киберпожаров» пришелся на первую неделю прошлогоднего вторжения, говорит Джон Бейтман, старший научный сотрудник Программы технологий и международных отношений Фонда Карнеги за международный мир, опубликовавший подробный отчет о российских кибероперациях.

Киберпожары «скромно способствовали первоначальному вторжению, но быстро потеряли свою актуальность», — говорит он. Наиболее заметным был взлом Россией модемов, подключенных к сети спутниковой связи Viasat KA-SAT, который начался 24 февраля, примерно в то время, когда российские войска вторглись на границу Украины.

Бейтман говорит, что, хотя эта хакерская атака «вероятно помогла ухудшить» украинское командование, управление, связь, компьютеры, разведку и совместимость, она не помешала защитникам отразить попытку России захватить Киев.

По его словам, с тех пор ни одна кибероперация «не имела сравнимого известного военного воздействия».

Точно так же атаки с использованием вайперов — отличительная черта российской агрессии в киберпространстве — резко возросли в течение первых четырех месяцев 2022 года, но с тех пор пошли на убыль, говорится в отчете, опубликованном на прошлой неделе группой анализа угроз Google совместно с командой реагирования на инциденты Google Mandiant.

Россия, возможно, исчерпала свой арсенал вредоносных программ-вайперов и еще не пополнила запасы. Или, возможно, вредоносное ПО Wiper не оказало должного влияния на военных планировщиков.

Конечно, любое наблюдение за полем боя во время боевых действий вызывает неуверенность. В отчете голландской военной разведки, опубликованном на этой неделе, говорится, что многие атаки еще не стали достоянием общественности…

Относительная неэффективность кибероружия на поле боя не означает, что Москва прекратила его развертывание. Их цель могла сместиться с военного воздействия на подрыв доверия гражданского населения к Киеву путем сеяния террора.

CyberPeace Institute, некоммерческая организация из Женевы, которая отслеживает влияние кибератак на гражданское население, заявляет, что российские атаки нацелены на гражданских лиц в нарушение международного

права. Институт CyberPeace сообщает, что за последние 12 месяцев было зарегистрировано 1100 кибератак и операций, связанных с конфликтом, которые третьи стороны приписывают 80 различным субъектам угроз, включая вредоносные программы, вайперы, кибершпионаж, распределенные атаки типа «отказ в обслуживании», фишинг, программы-вымогатели, порчи веб-сайтов, взлом и утечка, информационные операции и многое другое.

CyberPeace Institute сообщает, что из всех инцидентов, отслеженных им за последние три месяца 2022 года, почти 90% были связаны с DDoS-атаками. Внутри Украины наиболее целевым сектором были финансовые услуги, атаки на которые удвоились в период с июля по сентябрь.

Два непредвиденных события украинского конфликта в киберпространстве — это степень участия хактивистов и важность западных технологических гигантов.

На фронте хактивистов многочисленные союзные России группы продолжают наносить вред Украине и ее союзникам. Воздействие этих усилий представляется минимальным, если не считать пропагандистских целей.

Украина смогла поднять боевой дух, рассчитывая на армию международных добровольцев в сфере информационных технологий. Исследователи обнаружили, что, хотя воины-клавиатурники положительно влияют на боевой дух, их влияние на реальный мир также было минимальным…

Огромное влияние оказала широкая поддержка Украины со стороны Запада, причем не только со стороны спецслужб, но и технологических компаний, таких как Microsoft и Eset, а также сети службы спутниковой связи Starlink компании SpaceX. Западная облачная инфраструктура помогла правительству Украины функционировать, а Россия не смогла разрушить эту онлайн-инфраструктуру и средства защиты — и не из-за отсутствия усилий…

Таково нынешнее состояние российско-украинской войны, которая идет второй год: пока продолжаются кибератаки и операции, они не приведут Россию к победе. В то же время киберзащита остается важной…» ***(Mathew J. Schwartz. Russia-Ukraine War: Cyberattacks Fail to Best Partnerships // Information Security Media Group, Corp. (https://www.govinfosecurity.com/russia-ukraine-war-cyberattacks-fail-to-best-partnerships-a-21291). 24.02.2023).***

***

«Российские атаки на Украину за последний год участились в три раза, сообщает главный украинский центр реагирования на кибербезопасность.

Из 181 миллиона «подозрительных» событий кибербезопасности, зарегистрированных в 2022 году, 415 были событиями высокой степени информационной безопасности, сообщили в Государственной службе специальной связи и защиты информации Государственного центра киберзащиты Украины «Медиагруппа информационной безопасности». Агентство зафиксировало 14 миллионов атак от общего числа в первом квартале…

Атаки вредоносного ПО составили большую часть атак, увеличившись за год в 18 раз. В основном они распространялись с использованием умеренно серьезных уязвимых конечных точек.

Примером этого является эксплуатация CVE-2021-40444, уязвимости нулевого дня Microsoft Windows, которую хакеры использовали для нападения на критически важные украинские объекты. Microsoft исправила ошибку, но хакеры продолжают находить способы ее использования…

Фишинговые атаки были основным источником распространения вредоносного ПО на конечные точки критически важной инфраструктуры. Кампании, нацеленные на Украину, резко возросли в ноябре, а затем в конце года, как и оповещения о безопасности конечных точек в регионе, сообщает охранная фирма Trellix. СКПК подтвердил эту тенденцию.

Помимо приобретения оружия и боеприпасов у западных союзников, Украина получила огромную поддержку в сфере кибербезопасности. Страна углубила свои связи с западными странами, включая США и Польшу.

Союзники оказывали помощь в области кибербезопасности в рамках таких инициатив, как «Совместная помощь в области киберзащиты» — группа компаний и организаций в области кибербезопасности, которые предлагают разведывательные данные, помощь, технологии и услуги по обучению украинским организациям.

По данным Aspen Institute, CDAC помог нескольким украинским организациям смягчить последствия кибератак и выявил ограничения помощи в области киберзащиты. Институт предложил создать хабы для координации деятельности, управления проектами штатной помощи и установления более глубоких контактов между лидерами и операторами.

«CDAC еще не развил способность собирать, объединять и оценивать информацию о киберконфликте в Украине», но это можно сделать, «заимствуя инициативу института войны, которая объединяет общедоступную информацию, чтобы сделать прозрачные, надежные оценки конфликт на Украине», — говорится в сообщении Института Аспена…» ***(Mihir Bagwe. Ukraine Observed 181M Information Security Incidents in 2022 // Information Security Media Group, Corp. (https://www.govinfosecurity.com/ukraine-observed-181m-information-security-incidents-in-2022-a-21237). 17.02.2023).***

***

«…Российские государственные хакеры атаковали Украину в течение первых четырех месяцев 2022 года с более разрушительным вредоносным ПО, чем исследователи безопасности из Google и Mandiant обнаружили за предыдущие восемь лет.

Атаки были попыткой Москвы подорвать доверие к Киеву, и они продолжают происходить, хотя и более медленными темпами и по схеме, которая кажется менее методичной, говорится в отчете исследователей из Google Threat Analysis Group и Mandiant (теперь часть Google). рассмотрение киберпространства в попытке России завоевать Украину.

Сторонние наблюдатели за войной говорят, что центр кибероперацийРоссии в Украине сместился на сбор разведывательных данных, и Google и Mandiant отчасти подтверждают этот вывод. Исследователи из двух подразделений Google

говорят, что они наблюдают всплеск кибер-инцидентов, направленных на достижение нескольких стратегических целей, включая кражу и очистку данных…

В целом волна разрушительных кибератак оказалась не такой эффективной, как предыдущие российские кибератаки. В 2015 и 2016 годах российские хакеры нарушили работу энергосистемы Украины, что обычно приписывают хакерской группе ГРУ, известной как Sandworm.

Google отслеживает Sandworm как FrozenBarents. Группа добилась определенных успехов, говорится в сообщении. В докладе говорится, что он был нацелен на турецкого производителя беспилотников, которые первоначально использовались украинскими военными, но которые внезапно исчезли после того, как Россия вывела из строя беспилотные летательные аппараты.

Фишинг является известным вектором первоначального доступа. В отличие от деструктивных атак, которые, как правило, не имеют побочного эффекта за пределами Украины, число российских фишинговых атак резко возросло внутри Украины и за пределами стран НАТО.

По сравнению с 2020 годом, говорится в отчете, данные за прошлый год показывают увеличение количества фишинговых писем, нацеленных на пользователей в Украине, на 250%, а в странах НАТО — более чем на 300%. В отчет включены фишинговые атаки, совершенные группой, которую Google отслеживает как «Пуща», расположенной в Беларуси, но тесно связанной с Кремлем.

Фишинговая кампания, проведенная группой, известной как ColdDriver, Seaborgium и TA446, была нацелена на учетные записи электронной почты Proton нескольких видных деятелей Соединенного Королевства, и злоумышленники впоследствии слили информацию, пытаясь сформировать общественное мнение. Веб-сайт опубликовал просочившиеся электронные письма от нескольких ведущих сторонников Brexit и предположил, что они тайно принимали решения в Великобритании.

За скачком активности стоит смещение внимания хакеров российской военной разведки на Украину и активизация их усилий там. В отчете говорится, что относительно новая группа ГРУ, отслеживаемая как FrozenVista и также идентифицированная как UNC2589, похоже, начала действовать в Украине весной 2021 года. Когда Россия начала стягивать войска к украинской границе, она разослала фишинговые электронные письма почти 2000 целей в Украине. в основном лица в правительстве или вооруженных силах. В январе он применил очистители данных против украинских государственных органов «что могло быть предварительным ударом», говорится в отчете.

Одним из заметных событий в захватнической войне России стал рост хактивизма с обеих сторон. Большая часть самопровозглашенной прокремлевской или прокиевской активности проявлялась в форме распределенных атак типа «отказ в обслуживании», хотя некоторые группы слили украденные данные. Mandiant оценивает с «умеренной уверенностью», что горстка этих российских групп — XakNet Team, Infocentr и CyberArmyofRussia_Reborn — координирует операции с российской правительственной хакерской группой, которую Google отслеживает как FrozenLake. Группа также известна как Fancy Bear, APT28 и

Strontium…» ***(Anviksha More. Ukraine Withstands Torrent of Russian Cyberattacks // Information Security Media Group, Corp. (https://www.govinfosecurity.com/ukraine-withstands-torrent-russian-cyberattacks-a-21215). 16.02.2023).***

***

«Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, попереджає про нову кібератаку на організації та установи України з використанням програми Remote Utilities.

Про це повідомляє РБК-Україна з посиланням на Telegram-канал Держспецзв'язку…

«Фахівці CERT-UA зафіксували масове розповсюдження небезпечних електронних листів, які надходять начебто від апарату Ради національної безпеки і оборони України. Вони мають тему «RE: Критичне оновлення безпеки» та додаток у вигляді RAR-архіву з назвою "KB5017371 оновлення системи безпеки.rar». Архів містить зображення-приманку «інструкція Важливо прочитати.jpg» та спліт-архів з виконуваним файлом «KB5017371.exe», - попереджають фахівці.

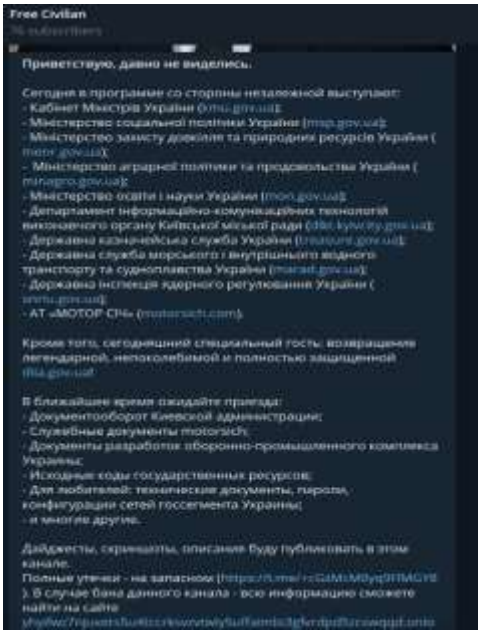
І додають, що у разі завантаження, розпакування та запуску вмісту архіву на комп'ютер буде встановлено легітимну програму Remote Utilities. Вона надає прихований віддалений доступ до пристрою третім особам. Виявлена активність відстежується за ідентифікатором UAC-0096…» ***(Кіберзлочинці вчинили нову атаку на Україну: в е-листах «зашита» програма доступу // Internetua (https://internetua.com/kiberzlocsinci-vcsinili-novu-ataku-na-ukrayinu-v-e-listah-zashita-programa-dostupu). 13.02.2023).***

***

«Невідомі хакери в ніч з 22 на 23 лютого атакували низку українських державних ресурсів. Внаслідок злому не працювали сайти Кабінету Міністрів, Мінсоцполітики, Державної служби морського і річкового транспорту, Держказначейства, АТ «Мотор Січ» та інші. За інформацією видання Фокус, кіберзлочинці обіцяють оприлюднити службові документи держструктур і розробки українського військово-промислового комплексу.

«Черговий український витік. Я був, є і буду», — таке послання залишали хакери на зламаних сайтах.

Анонс кібератаки з'явився напередодні у Telegram-каналі з підозріло малою кількістю підписників Free Civilian. На момент написання новини там всього 76 фолловерів. Українські служби впевнені, що кіберзлочинці мають стосунок до держави-терориста, оскільки у своїх дописах образливо називають Україну «нєзалєжною». Саме таку конотацію часто використовують російські пропагандисти, коли транслюють наративи окупантів на широку аудиторію.



Хакери попереджають про наступні кібератаки на Міністерство зі захисту довкілля та природних ресурсів, Мінагрополітики, Міносвіти, Департамент інформаційних та комунікаційних технологій Київської міськради та Держінспекцію ядерного регулювання. Зловмисники також анонсували оприлюднення документообігу КМДА, розробок оборонно-промислового комплексу України та вихідні коди держресурсів.

«Для любителів: технічні документи, паролі, конфігурації мереж держсегменту України та багато чого ще. Якщо зацікавлені в купівлі повних зливів, звертайтеся в приват», — зазначив адмін телеграм-каналу Free Civilian.

Хакери також «злили» документи «Мотор Січі». Кіберзлочинці стверджують, що підприємство нещодавно відкрило представництво в Туреччині й виробляє двигуни для турецьких БПЛА Bayraktar. «Мабуть, тепер байрактари завдаватимуть ударів по всьому світу й особливо в росії з новою силою. Продовжую стежити за діяльністю цього підприємства і час від часу відправляю їхні напрацювання в руки зацікавлених спільнот», — поінформувало угруповання.

Українські високопосадовці поки ніяк не прокоментували ситуацію…» ***(Хакери з росії зламали урядові сайти України та пообіцяли оприлюднити секретну інформацію // No worries! (https://noworries.news/hakery-z-rosiyi-zlamaly-uryadovi-sajty-ukrayiny-ta-poobiczyaly-oprylyudnyty-sekretnu-informacziyu/). 23.02.2023).***

****

«Українські ІТ-спеціалісти з угрупування HackYourMom зламали навігаційну супутникову систему держави-терориста російської федерації - ГЛОНАСС. Про це на своїй сторінці у Facebook повідомив експерт із кібербезпеки Микита Книш.

Сам Книш докладно не розповідає подробиць зламу і не коментує ситуацію, але радить російським окупантам та злочинним спецслужбам згадувати, як користуватися паперовими картами, «бо ГЛОНАСС — всьо». Також Книш «поставив 2» за «Модель загроз безпеці інформації», яку розробляли у

московському університеті імені Баумана. Документи також стали надбанням хакерів…

ГЛОНАСС — це радянська, а після розвалу срср російська радіонавігаційна супутникова система. Розгортання навігації у космосі зроблено за допомогою супутників «Глонасс-К» та «Глонасс-М». Базу ГЛОНАСС складають 24 космічні об'єкти, які перебувають на земній орбіті на висоті 19,4 тис. км. фіційними даними, у 2015 році після виправлення деяких помилок навігаційну систему здали в експлуатацію міністерству війни рф…

Українське кіберугрупування HackYourMom — результат спільної праці волонтерів-програмістів і команди з кібербезпеки Микити Книша. Фахівці не лише займаються ІТ-діяльністю, але й створили освітню платформу, де консолідується інформація з різних напрямків кібербезпеки. До слова, наприкінці січня хакери HackYourMom злили базу даних найбільшого іранського оператора мобільного інтернету IranCell…» ***(Українські хакери зламали російську супутникову систему навігації // No worries! (https://noworries.news/ukrayinski-hakery-zlamaly-rosijsku-suputnykovu-systemu-navigacziyi/). 06.02.2023).***

***

«Кіберзлочинці створили фейковий сайт Міністерства закордонних справ України для викрадення конфіденційних даних громадян, шляхом поширення шкідливого ПЗ. Сайт, що імітує офіційний вебресурс МЗС, виявили спеціалісти урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

На фейковому сайті користувачам пропонують завантажити програмне забезпечення для виявлення «заражених комп'ютерів». Фішингове посилання містить шкідливе ПЗ, завантаживши яке користувачі ризикують «поділитися» особистою інформацією зі зловмисниками.

На комп'ютер жертви завантажується BAT-файл «Protector.bat» — його відкриття призведе до запуску на комп'ютері PowerShell-скриптів, які здійснюють пошук файлів із розширеннями:.edb,.ems,.eme,.emz,.key,.pem,.ovpn,.bat,.cer,.p12,.cfg,.log,.txt,.pdf,.doc, .docx,.xls,.xlsx,.rdg. У каталозі робочого столу інструменти шкідливого ПЗ роблять знімки екрану та передають дані на сервер зловмисників, які, ймовірно, є росіянами.

Як повідомили спеціалісти урядової команди реагування, у межах співпраці з CERT Polska та CSIRT MON виявлені аналогічні фішингові ресурси, які імітують офіційні вебсторінки МЗС України, Служби безпеки України, а також Поліції Польщі. У червні 2022 року подібна фішингова сторінка імітувала інтерфейс поштового сервера Міністерства оборони України.

Поки представники країни-терориста намагаються отримати доступ до конфіденційних даних користувачів, українські хакери зламали всі 79 сервісів російської ІТ-компанії Yandex. 45 Гб даних Yandex опинились у відкритому доступі. Відтепер у вільному доступі лежить код, який показує як Yandex змінює пошукові алгоритми заради кремлівської пропаганди. А наприкінці 2022 року український ІТ-спеціаліст Алекс Голден та його команда Hold Security зламали

російський даркнет-маркетплейс Solaris та отримали доступ до коштів платформи. Hold Security вдалось переказати 1.6 BTC з криптогаманця Solaris (близько $ 25 000 на момент переказу) українському благодійному фонду «Життєлюб». ***(Хакери створили фейковий сайт одного з Міністерств для викрадення конфіденційних даних українців // No worries! (https://noworries.news/hakery-stvoryly-fejkovyj-sajt-odnogo-z-ministerstv-dlya-vykradennya-konfidenczijnyh-danyh-ukrayinczіv/). 03.02.2023).***

***

«Кремль планує провести весь спектр інформаційних операцій проти України та Європи, а також усередині власної країни, щоб переламати хід війни.

Про це повідомляється у звіті компанії Google, опублікованому напередодні Мюнхенської конференції з безпеки. Група аналізу загроз Google (TAG) повідомила, що ці операції мають три цілі:

Підірвати український уряд,

Зламати міжнародну підтримку України,

Збільшувати внутрішню підтримку війни на території росії.

За даними звіту, зловмисники, які підтримує російський уряд, доклали агресивних зусиль, щоб отримати вирішальну перевагу у воєнний час у кіберпросторі. При цьому хакери, що спонсоруються російською державою, атакували Україну ще за рік до вторгнення. У 2022 році Росія збільшила атаки на Україну 250% порівняно з 2020 роком. За той же період атаки на користувачів у країнах НАТО збільшився більш ніж на 300%.

У Google спостерігали сплески активності, пов'язані з ключовими подіями у війні, такими як нарощування військ, вторгнення та мобілізація військ у росії…» ***(Олег Бесараб. У Google викрили цілі інформаційних спецоперацій рф // UA.NEWS (https://ua.news/ua/war-vs-rf/v-google-razoblachili-tseli-informatsionnyh-spetsoperatsij-rf). 16.02.2023).***

***

«Декілька серверів медіахолдингу Всеросійська державна телевізійна та радіомовна компанія (ВДТРК) були атаковані хакерами при трансляції послання президента Росії Володимира Путіна до Федеральних зборів. В цей час проводяться технічні роботи для нормалізації сервісів, – повідомляє Lenta.Ru.

Згідно з інформацією на сайті ВДТРК, на цю мить ведуться технічні роботи на декількох сервісах медіахолдингу, включаючи телеканали «Росія 1», «Росія 24», «Росія К», «Росія РТР», «Карусель», радіо «Маяк», «Росія», «Вести FM», «Культура» та «Юність».

Сайт «Смотрим.ру», на якому транслюються програми «Росія 24», також припинив роботу.

Згідно з інформацією, що розповсюджується в Telegram-каналах, у зв’язку з атакою, сайт «Першого каналу» також зазнав збою…» ***(Сайти російського медіахолдингу ВДТРК зазнали DDoS-атаки під час виступу Путіна // mediasat***

(https://mediasat.info/uk/2023/02/21/sajty-rosijskogo-mediaholdyngu-vdtrk-zaznaly-ddos-ataky-pid-chas-vystupu-putina/). 21.02.2023).

***

«Українські ІТ-спеціалісти з угрупування HackYourMom зламали навігаційну супутникову систему держави-терориста російської федерації - ГЛОНАСС. Про це на своїй сторінці у Facebook повідомив експерт із кібербезпеки Микита Книш.

Сам Книш докладно не розповідає подробиць зламу і не коментує ситуацію, але радить російським окупантам та злочинним спецслужбам згадувати, як користуватися паперовими картами, «бо ГЛОНАСС — всьо». Також Книш «поставив 2» за «Модель загроз безпеці інформації», яку розробляли у московському університеті імені Баумана. Документи також стали надбанням хакерів.

ГЛОНАСС — це радянська, а після розвалу срср російська радіонавігаційна супутникова система. Розгортання навігації у космосі зроблено за допомогою супутників «Глонасс-К» та «Глонасс-М». Базу ГЛОНАСС складають 24 космічні об'єкти, які перебувають на земній орбіті на висоті 19,4 тис. км. За офіційними даними, у 2015 році після виправлення деяких помилок навігаційну систему здали в експлуатацію міністерству війни рф.

Українське кіберугрупування HackYourMom — результат спільної праці волонтерів-програмістів і команди з кібербезпеки Микити Книша. Фахівці не лише займаються ІТ-діяльністю, але й створили освітню платформу, де консолідується інформація з різних напрямків кібербезпеки. До слова, наприкінці січня хакери HackYourMom злили базу даних найбільшого іранського оператора мобільного інтернету IranCell.

Це далеко не перша перемога наших програмістів у боротьбі з російськими окупантами. Нагадаємо — хакерам з України вдалось зламати всі 79 сервісів російської ІТ-компанії Yandex. 45 Гб даних Yandex опинились у відкритому доступі. У вільному доступі також знаходиться код, який показує як Yandex змінює пошукові алгоритми заради кремлівської пропаганди». ***(Українські хакери зламали російську супутникову систему навігації // No worries! (https://noworries.news/ukrayinski-hakery-zlamaly-rosijsku-suputnykovu-systemu-navigacziyi/). 06.02.2023).***

***

«Спустя год после того, как Россия вторглась в Украину, война продолжается, включая постоянно развивающийся цифровой компонент, который влияет на будущее кибербезопасности во всем мире. Среди прочего, война в Украине перевернула восточноевропейскую киберпреступную экосистему, по словам экспертов по кибербезопасности из Google, в корне изменила ход атак программ-вымогателей.

«Программы-вымогатели по-прежнему приносят прибыль, но финансовые мотивы злоумышленников не застрахованы от геополитических событий», — говорится в новом отчете, составленном Google Threat Analysis Group (TAG),

Mandiant (фирма по кибербезопасности, которая теперь является частью Google Cloud) и Google Доверие и безопасность.

«Границы между злоумышленниками, мотивированными деньгами, и злоумышленниками, поддерживаемыми правительством, в Восточной Европе стираются, — говорится в отчете, — злоумышленники меняют свои цели, чтобы соответствовать региональным геополитическим интересам, а злоумышленники, поддерживаемые правительством, перенимают некоторые тактики и услуги, связанные с финансово мотивированными субъектами».

В отчете отмечается, что по мере изменения альянсов для киберпреступников больше не является табу преследовать российские цели. Между тем, по словам экспертов Google, война также ускорила тенденцию к «специализации» в экосистеме программ-вымогателей, что затрудняет выявление виновных.

Вдобавок ко всему, в докладе отмечается, что «война в Украине также определялась тем, что мы ожидали, но не увидели». В частности, не было всплеска атак на критическую инфраструктуру, что удивительно, учитывая распространенность угроз программ-вымогателей.

Политические расколы

Война расколола восточноевропейскую сеть киберпреступников, говорится в отчете Google. Некоторые группы заявили о своей политической приверженности, в то время как другие работали в геополитическом ключе, а другие известные группы вымогателей закрылись.

Например, в начале войны группа вымогателей Conti заявила о своей поддержке России и пригрозила нанести удар по критически важной инфраструктуре стран, которые предприняли действия против России. По словам Google, такая позиция привела к разногласиям внутри группы, согласно утечкам ее внутренних коммуникаций и исходного кода. Вместо того, чтобы усиливать атаки, когда это угрожало, группа закрылась.

Кроме того, вредоносное ПО для воровства Raccoon приостановило свою деятельность после того, как его подозреваемый разработчик бежал из Украины. Он был арестован в Нидерландах и ожидает экстрадиции в США.

Война также побудила киберпреступников преследовать российские цели.

«До февраля 2022 года создатели программ-вымогателей использовали методы, чтобы избежать нацеливания на Содружество Независимых Государств, включая жесткое кодирование названий стран и проверку языка системы», — говорится в отчете. «После вторжения группа хактивистов NB65 использовала утечку исходного кода Conti для нападения на российские организации. Центральный банк России».

Тем временем так называемая «Украинская ИТ-армия» сотрудничала с министерством обороны Украины, чтобы защитить Украину и атаковать российскую инфраструктуру и веб-сайты.

Изменение тактики

Война также вызвала изменение тактики среди групп вымогателей. Во-первых, кампании программ-вымогателей, связанные с атакующими, поддерживаемыми правительством, используют тактику, обычно связанную с финансово мотивированными хакерами, и наоборот.

Кроме того, в отчете говорится, что злоумышленники с программами-вымогателями все чаще специализируются на одной части «цепочки атак», работая с другими «деловыми партнерами».

Во время войны злоумышленники также больше экспериментировали с новыми методами, такими как новые каналы доставки и нетрадиционные форматы файлов. Злоумышленники с финансовой мотивацией также быстро заимствовали успешные методы других преступников, что затрудняет определение того, кто стоит за атаками.

Возмездие нереализовано

В отчете Google рассматриваются причины, по которым во время войны не было всплеска атак программ-вымогателей на критически важную инфраструктуру, «как можно было ожидать после заявлений в начале конфликта и предыдущей волны таких атак в 2021 году».

Одна из теорий, которую выдвигает Google, заключается в том, что реакция США на атаку Colonial Pipeline в 2021 году и последующий арест в России членов банды вымогателей REvil могли сдержать финансово мотивированные банды вымогателей.

Google также предполагает, что санкции против России могли повлиять на готовность западных организаций платить выкуп». ***(Stephanie Condon. The war in Ukraine has shaken up the cybercriminal ecosystem, Google says // ZDNET (https://www.zdnet.com/article/the-war-in-ukraine-has-shaken-up-the-cybercriminal-ecosystem-google-says/). 16.02.2023).***

***

«Кибернаступление России против Украины оказалось неподготовленным, нескоординированным и неспособным преодолеть хорошо подготовленную и гибкую серию украинских оборонительных действий, которые опирались на опыт и знания и опровергали довоенные прогнозы. По словам экспертов, Киеву активно помогают зарубежные партнеры по информационным технологиям из государственного и частного секторов, а его способность задействовать плотную сеть гражданских специалистов обеспечивает критически важную координацию между гражданскими и военными в кибервойне.

Кибервойна была главной темой обсуждения на крупной конференции по спонсируемым государством угрозам в киберпространстве в южнокорейской столице.

По словам аналитиков, ожидание быстрого краха Киева после его вторжения в феврале прошлого года было ключевой причиной провала российской киберстратегии. План российского вторжения, разработанный небольшим штабом и лишь с опозданием распространенный по российским военным подразделениям, не оставлял времени для координации сетевой борьбы с другими аспектами наступления». ***(Andrew Salmon. Russia's cyber spooks hit hard wall of Ukrainian resilience // The Washington Times, LLC (https://www.washingtontimes.com/news/2023/feb/16/russias-cyber-spooks-hit-hard-wall-ukrainian-resil/?utm_source=RSS_Feed&utm_medium=RSS). 16.02.2023).***

***

«Хакер з Полтави створив шкідливе ПЗ, за допомогою якого він викрадав паролі до акаунтів на криптобіржі Binance та привласнював кошти користувачів. Про інцидент стало відомо завдяки опублікованій постанові суду на сайті Реєстру судових рішень України.

Як тільки користувач відкривав файл зі шкідливим ПЗ та здійснював вхід до акаунту біржі, криптовалюта автоматично відправлялась на гаманець, вказаний в програмному забезпеченні. Повідомляється, що подібним чином зловмисник діяв не лише на Binance, а й на інших криптоплатформах.

Отримуючи цифрові активи, чоловік обмінював їх на фіатну валюту в полтавському пункті обміну. «Дізнатись, які саме криптогаманці користувались послугами обмінного пункту неможливо, адже дана установа здійснює свою фінансову діяльність незаконно», — пояснили правоохоронці. Наразі рішенням Полтавського апеляційного суду майно хакера арештоване.

Якщо мешканець Полтави привласнював чужі цифрові активи, то житель Миколаєва навпаки — втратив 400 000 гривень через криптошахраїв. 35-річний інвестор перейшов за невідомим посиланням в інтернеті, яке закликало користувачів вкладати кошти у криптовалюти. Чоловік переказав на рахунок зловмисників 400 000 гривень, втім обіцяну криптовалюту так і не отримав. У які саме токени хотів вкласти заощадження українець наразі невідомо». ***(Криптовалютний хакер з Полтави привласнював токени користувачів Binance // No worries! (https://noworries.news/kryptovalyutnyj-haker-z-poltavy-pryvlasnyuvav-tokeny-korystuvachiv-binance/). 08.02.2023).***

***

«Правоохоронці Львівської області ліквідували міжнародний конвертаційний центр із щомісячним обігом у 600 млн гривень. Про це пише медіапортал «Твоє місто». Як повідомляють слідчі, група осіб надавала послуги з конвертації віртуальних коштів у готівку та криптовалюту. Також зловмисники пропрацьовували схеми зі зменшення або уникнення оподаткування за транзакції.

«За процесуального керівництва Львівської обласної прокуратури викрито групу осіб на легалізації майна, одержаного злочинним шляхом, та ухиленні від сплати податків (ч. 3 ст. 209, ч. 3 ст. 212 КК України)», — йдеться у повідомленні прокуратури Львівської області.

Загалом таких угруповань нарахували понад 30. У прокуратурі повідомили: клієнтами конвертаційного центру були приватні підприємці, фізичні особи й так звані «транзитні підприємства», які входять до інших конвертаційних груп. Окрім цього, протягом 2020−2022 років на рахунки 20 таких фіктивних осередків переказали понад 2,5 млрд грн.

Під час обшуків офісних приміщень та приватних будинків злочинців поліція виявила та вилучила 165 млн грн готівки, понад 200 печаток фіктивних іноземних офшорних компаній, чернетки фінансових операцій, комп’ютерну техніку та інші

речові докази. Слідчі дії ще тривають — правоохоронці проводять кримінальні експертизи та узгоджують питання щодо конфіскації майна та арешту учасників фінансової афери…» ***(Криптовалютні злочинці на Львівщині проводили махінації на 600 мільйонів гривень щомісяця // No worries! (https://noworries.news/kryptovalyutni-zlochynczi-na-lvivshhyni-provodyly-mahinacziyi-na-600-miljoniv-gryven-shhomisyaczya/). 08.02.2023).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Канадский университет сотрудничает с Украиной в рамках пилотной программы по обучению до 100 украинцев специалистам по кибербезопасности.

Центр обучения, инноваций и сотрудничества в области кибербезопасности Rogers Cybersecure Catalyst из Брэмптона, Онтарио, входящий в состав Университета Торонто Метрополитан, заявил сегодня, что программа будет реализована онлайн в сотрудничестве с Украинскими партнерами по безопасности информационных систем (ISSP), киберкомпания и Министерство цифровой трансформации страны.

Программа обеспечит базовое обучение кибербезопасности для украинцев, которые были уволены с предыдущей работы из-за войны, говорится в пресс-релизе университета. Участники программы получат международно признанный сертификат кибербезопасности.

Набор на программу начнется в ближайшее время. После завершения пилотная программа обучения будет оценена на предмет возможного расширения на большую группу украинских учащихся.

«Мы считаем, что эта программа окажет положительное влияние на украинскую экономику, а также будет способствовать долгосрочному развитию украинского сектора кибербезопасности», — заявил Чарльз Финли, исполнительный директор-основатель Catalyst. «Мы стремимся помочь сделать этот проект успешным и надеемся, что сможем расширить эту программу в будущем».

«Катализатор ответил на призыв поддержать экономическое восстановление Украины благодаря своему опыту и лидерству в обучении кибербезопасности», — сказала министр иностранных дел Канады Мелани Джоли. «Мы все обязаны думать о будущем Украины, и наше правительство с нетерпением ждет успеха этой пилотной программы».

Украина накопила значительный опыт в области кибербезопасности после того, как в течение как минимум восьми лет сталкивалась с российскими кибератаками. В декабре 2015 года и снова почти ровно через год энергосистема страны была временно выведена из строя кибератаками.

Кибератаки на украинские сайты в январе 2022 года стали прелюдией к вторжению российских войск в феврале 2022 года. С тех пор Украине помогает ряд технологических компаний, в том числе Google, Microsoft и SpaceX.

Страна обратилась в Международный уголовный суд с просьбой расследовать, могут ли определенные российские кибератаки считаться военными преступлениями.

Тем не менее, украинские организации ежедневно сталкиваются с кибератаками, многие из которых связаны с программами очистки. Злоумышленники рассылают украинцам заманчивые и зараженные сообщения электронной почты со ссылками на приложения или якобы официальные документы правительства Украины.

В прошлом месяце украинский чиновник по кибербезопасности заявил, что за последний год количество кибератак в стране увеличилось в три раза». ***(Howard Solomon. Toronto university to help train Ukrainians in cybersecurity // ITBusiness.ca (https://www.itbusiness.ca/news/toronto-university-to-help-train-ukrainians-in-cybersecurity/124187). 10.02.2023).***

***

«Вице-премьер – министр цифровой трансформации Михаил Федоров встретился с заместителем главы USAID Изобель Коулман. В ходе встречи обсуждалось дальнейшее сотрудничество Украины с Агентством США по международному развитию. В частности, они укрепляли киберзащиту и поддерживали цифровую трансформацию.

USAID объявило, что выделит 60 миллионов долларов на укрепление кибербезопасности Украины. Это поможет правительству защитить объекты критической инфраструктуры от российских кибератак. В частности, энергетика, телекоммуникации и системы хранения данных.

«USAID — надежный партнер Украины. Благодаря поддержке агентства мы запустили приложение и портал «Дія» и десятки самых популярных сервисов, которые украинцы могут получить в несколько кликов. Команда Министерства цифровой трансформации активно сотрудничает с USAID в сфере цифровой трансформации и кибербезопасности. При поддержке агентства мы создаем максимально удобные сервисы в «Дии» для украинцев и уже делимся своим опытом с миром. Мы благодарны USAID за постоянную помощь, поддержку наших цифровых инициатив и усиление киберзащиты государства», — сказал Михаил Федоров.

Украина сотрудничает с USAID в сфере кибербезопасности с 2020 года и уже имеет ощутимые успехи. В настоящее время агентство расширяет поддержку для усиления возможностей Украины по отражению кибератак и поддержки цифровой трансформации нашей страны. USAID сотрудничает с Министерством цифровой трансформации с первых дней работы министерства. Украина запустила 80% сервисов в «Дии» благодаря поддержке агентства. Они также совместно запустили Реестр поврежденного имущества и другие антикоррупционные проекты.

USAID будет сотрудничать с Новой Зеландией и Данией для укрепления кибербезопасности Украины и поддержки партнерства с другими странами,

которые также помогают Украине. USAID будет способствовать укреплению цифровой инфраструктуры и поддержке частного сектора в сфере информационных и коммуникационных технологий. А также поможет Украине разработать цифровые инструменты для предоставления государственных услуг и снижения коррупции.

С первых дней существования Министерства цифровой трансформации USAID оказывает юридическую, финансовую и техническую помощь в развитии «Діи». В частности, при поддержке партнеров мы реализовали Bug Bounty — лучшее от «Дии». Американское агентство выделило призовой фонд для этичных хакеров, ищущих уязвимости и ошибки в Diia. Во время Bug Bounty критических уязвимостей обнаружено не было. Это позволило еще раз убедиться и подтвердить, что Дийя — безопасное приложение.

Во время Всемирного экономического форума в Давосе USAID сообщило, что планирует выделить около 650 000 долларов на формирование подхода к распространению цифрового опыта Украины и мобильного приложения «Дія» в другие страны». ***(The Ministry of Digital Transformation is expanding cooperation with USAID: the agency will allocate $60 million to strengthen Ukraine's cyber security // Odessa Journal (https://odessa-journal.com/the-ministry-of-digital-transformation-is-expanding-cooperation-with-usaid-the-agency-will-allocate-60-million-to-strengthen-ukraines-cyber-security/). 10.02.2023).***

***

Світові тенденції в галузі кібербезпеки

«Вперше День безпечного інтернету відзначали 7 лютого 2004 року. Цю дату було встановлено європейською мережею інформаційних центрів Insafe, що сприяють безпеці в інтернеті та цифровій грамотності.

Інтернет став вже невіддільною частиною нашого повсякденного життя. Існування без Інтернету здається нам неможливим, тому безпека під час перебування в мережі має першочергове значення. Цього року День безпечного інтернету відзначатиметься так само 7 лютого. Цей день має дати нам розуміння того, яким чином ми можемо безпечно переглядати нескінченні обсяги доступної нам інформації та розваг.

Традиція, що була започаткована у 2004 році як ініціатива проєкту ЄС SafeBorders, наразі знайшла підтримку вже приблизно у 180 країнах світу. День безпечного інтернету також важливий для того, щоб допомогти молодому поколінню визначити для себе кращі моделі використання інтернетом. Ось усе, що вам потрібно знати про цей день.

Всесвітній день безпечного інтернету 2023

Цього року головна тема відзначення Дня безпечного інтернету – «Хочете поговорити про це? Знайдіть місце для обговорення життя в інтернеті». Цьогоріч, як ми вже зазначали, свято відзначають 7 лютого.

У 1990 році вчений-комп'ютерник Тім Бернерс-Лі створив Всесвітню павутину, започаткувавши інтернет, який ми знаємо сьогодні.

Відзначення Дня безпечного інтернету було запропоновано у 2004 році як ініціатива проєкту ЄС SafeBorders. У 2005 році мережа Insafe взяла на себе місію проведення однієї з перших акцій з відзначення цієї дати. Наразі День безпечного інтернету відзначається приблизно в 180 країнах і територіях по всьому світу.

У 2009 році було запроваджено концепцію комітетів Дня безпечного інтернету. Це було зроблено з метою зміцнення зв'язків із країнами за межами мережі. У комітетах також хотіли інвестувати гроші в узгоджену рекламну кампанію по всьому світу. Наразі в рамках Координаційної команди з відзначення Дня безпечного інтернету, яка базується у штаб-квартирі Європейського Союзу в Брюсселі, працюють понад 150 глобальних комітетів Дня безпечного інтернету.

Щодня у всесвітньому павутинні створюються тисячі web-сайтів, на яких мільйони користувачів розміщують свій контент. Бути у курсі головних тенденцій інтернету, який постійно змінюється, дуже важливо. Адже розуміння цих змін дає можливість найкраще підготуватися до всіх останніх оновлень інтернету.

Цей день також відзначають для того, аби зрозуміти важливість безпеки в інтернеті. Перебувати у безпеці під час роботи в інтернеті означає бути захищеним від усіх загроз і ризиків, що існують в онлайн-середовищі. Під загрозами й ризиками слід розуміти все, що може поставити під загрозу безпеку особистої інформації, спричинити небезпечні зв'язки, або вплинути на ваше психічне здоров'я та загальне самопочуття.

День безпечного інтернету відзначається, щоб допомогти поколінню що підростає зрозуміти основи й принципи безпеки в інтернеті. І це стосується не лише питання захисту себе самого, але й усвідомлення власної відповідальності за те, аби не завдавати шкоди іншим – навмисно чи мимохіть». ***(Борис Скуратівський. Сьогодні Всесвітній день безпечного інтернету: що варто знати? // mediasat (https://mediasat.info/uk/2023/02/07/sogodni-vsesvitnij-den-bezpechnogo-internetu-shho-varto-znaty/). 07.02.2023).***

***

«Кибербезопасность — это практика развертывания людей, политик, процессов и технологий для защиты организаций, их критически важных систем и конфиденциальной информации от цифровых атак.

Независимо от того, являетесь ли вы администратором крупной компании или запускаете стартап из своего гаража, защита идентификационных данных пользователей имеет решающее значение.

Проблемы в сегодняшнем быстро меняющемся ландшафте угроз значительны, но защитные стратегии и технологии могут помочь.

Вот несколько шагов, которые Microsoft предприняла, чтобы укрепить ваши усилия по обеспечению безопасности личных данных:

Многофакторная аутентификация: Всегда защищайте всех своих пользователей с помощью многофакторной проверки подлинности, используя Authenticator, Fast Identity Online (FIDO), Windows Hello или СВА.

Условный доступ: Ограниченный доступ означает меньшее воздействие. Применение правил условного доступа к вашим приложениям помогает защититься от атак приложений.

Политики защиты конечных точек: Используйте политики управления мобильными устройствами и защиты конечных точек, особенно запрет запуска от имени администратора на устройствах, для предотвращения атак кражи токенов.

Ограничение воздействия: Ограничьте локальное воздействие и интегрируйте свои SOC и усилия по идентификации, чтобы защитить свою инфраструктуру идентификации.

Переход в облако: Делайте ставку на гибкость благодаря облачному подходу, адаптируемой аутентификации и глубокой приверженности автоматизированному реагированию на распространенные проблемы, чтобы сохранить критически важные ресурсы для настоящих кризисов». ***(How to stay cyber secure at workplaces in 2023: Microsoft // TechGig (https://content.techgig.com/it-security/how-to-stay-cyber-secure-at-workplaces-in-2023-microsoft/amp_articleshow/97573777.cms). 03.02.2023).***

***

«Кибербезопасность быстро становится одним из наиболее значительных драйверов роста для поставщиков управляемых услуг (MSP). Это основной вывод из недавнего исследования Lumu: в Северной Америке более 80% MSP называют кибербезопасность основным фактором роста своего бизнеса. Поставщики услуг имеют огромные возможности для расширения своего бизнеса и привлечения новых клиентов, развивая свои предложения в области кибербезопасности.

В этом нет ничего удивительного, поскольку спрос на кибербезопасность среди малого и среднего бизнеса и крупных предприятий находится в самом разгаре. По данным Gartner, «к 2025 году 60% организаций будут использовать риск кибербезопасности в качестве основного фактора, определяющего при проведении транзакций и деловых операций с третьими сторонами».

Это означает, что восприятие безопасности трансформируется: из ответственности она становится мощным двигателем бизнеса. Конечно, кибербезопасность продолжает развиваться очень быстрыми темпами, угрозы появляются каждый день, а ставки становятся все выше. Уже одно это может усилить восприятие того, что это непосильная и напряженная область, особенно с учетом того, что COVID-19 перетасовал мир (ИТ).

Ускорение внедрения облачных технологий и гибридная работа, мошенничество, фишинговые сообщения и угрозы для конечных точек — все это беспокоит компании, заботящиеся о своих клиентах. Также бесспорно, что кибербезопасность является важнейшим компонентом гибридных рабочих сред. Пандемия сделала службы безопасности более осведомленными о цифровых рисках и важности стратегической защиты, планирования безопасности и управления рисками. Не стоит забывать о сложности найма квалифицированных специалистов по безопасности и сложности многих продуктов для обеспечения безопасности.

Тем не менее, MSP имеют уникальные возможности для процветания на этом новом рынке.

Согласно отчету о состоянии MSP за 2023 год:

«Кибербезопасность по-прежнему является очень большой областью для роста. В то время как услуги по защите от программ-вымогателей и фишинга/электронной почты остаются в центре внимания MSP, другие находят дальнейший рост, предлагая услуги по расширению отчетности, аудиту, обучению и формированию политики для клиентов».

Другими словами, у MSP есть уникальная возможность создать бренд безопасности, лучше удовлетворяя потребности своих клиентов. Это, вероятно, станет ключевым отличием бизнеса в следующем десятилетии.

Но одной только упаковки и перепродажи продуктов безопасности недостаточно. Им нужно превратиться в доверенных советников по безопасности.

Давайте объясним, что потребуется сервисно-ориентированным компаниям, чтобы в полной мере воспользоваться преимуществами этого крупного стратегического изменения.

Создание конкурентного преимущества

MSP — это в первую очередь сервисные компании, стремящиеся помочь своим клиентам в их цифровых операциях. Кибербезопасность — это расширяющаяся область с множеством возможностей для создания ценных услуг.

Переход к облачным и цифровым совместным рабочим процессам привел к значительному пробелу в обеспечении безопасности во многих отраслях, что привело к неэффективным и устаревшим мерам защиты.

Это справедливо даже для компаний, работающих с программным обеспечением: быстрое внедрение практики DevOps привело к появлению множества «серых зон» безопасности, которым не хватает возможностей для мониторинга и аудита.

Не только это, но и за последние несколько лет произошли изменения в том, как киберпреступники действуют во всем мире. Мы наблюдаем, что киберугрозы сосредотачиваются на корпоративном программном обеспечении посредством так называемых атак на цепочку поставок и концентрируют свои усилия на точках входа с высоким уровнем влияния, таких как сотрудники с особыми ИТ-правами, такие как разработчики.

Но создание конкурентного преимущества означает создание ценности для клиентов. В кибербезопасности может быть сложно продемонстрировать такую ценность.

Таким образом, для MSP важно лучше понять, с какими проблемами сегодня сталкиваются лидеры в области безопасности, а затем опираться на это:

— Как я могу получить полное представление о том, что происходит в моем окружении?

— Как я могу обнаружить потенциальные неправильные конфигурации и уязвимости?

— Как мне расставить приоритеты среди постоянно растущего списка приоритетов?

— Как я могу быстро и эффективно реагировать на угрозы в моей организации?

— Какие угрозы уникальны для моей организации?

Затем следует выбрать правильный набор инструментов. Инструменты не являются окончательными ответами на эти вопросы. Это то, что позволит поставщикам услуг получить представление о средах своих клиентов и создать дорожную карту безопасности для снижения рисков.

Работая в масштабе, MSP должны будут доказать, что они могут отделить сигнал от шума (не все уязвимости одинаковы) и что они могут использовать эту информацию для быстрого и точного решения проблем.

Развертывание решений, не обладающих компетенцией для их эксплуатации, только усугубит проблему.

Клиенты, независимо от их размера или отрасли, будут ожидать информации и индивидуального совета.

Это уникальная возможность переосмыслить безопасность как процесс или как услугу.

Теперь главный вопрос: как выделиться?

Принесите пользу, обнаружив утечку учетных данных до хакеров

Масштабируемость, наблюдаемость, автоматизация реагирования и образовательная ценность позволят поставщикам услуг предоставить своим клиентам максимальную пользу. Продвижение в области кибербезопасности путем предоставления исключительной ценности — это путь.

GitGuardian — это платформа безопасности кода, специализирующаяся на обнаружении утечек учетных данных (секретов) в исходном коде. Мы предоставляем решение для мониторинга внутренних репозиториев исходного кода, которое изначально интегрируется с GitHub, GitLab, BitBucket и Azure Repos.

Жестко закодированные секреты — это острая проблема практически для любой компании, занимающейся программным обеспечением: они копируются и передаются в разных средах практически без контроля, и они представляют серьезную угрозу для компаний. мы узнали, что в прошлом году что инженеры по безопасности приложений совершенно ошеломлены огромным количеством учетных данных, найденных в кодовых базах: в среднем 3,4 тыс. секретов на одного инженера.

Опираясь на эти возможности аудита, чтобы предоставить аналитикам SOC полезную информацию, было бы полезно для любой группы безопасности...

GitGuardian также предлагает возможность публичного мониторинга для определения глобального периметра компании на GitHub. более 6 миллионов секретов Только в 2021 году наша система обнаружения обнаружила, что вдвое больше, чем в предыдущем году. Многие из этих учетных данных являются корпоративной тайной, опубликованной по ошибке.

Эта возможность мониторинга позволяет заблаговременно выявлять угрозы и защищать компании от взлома.

Если вы готовы принять отраслевой подход к консультированию по вопросам безопасности, запросите бесплатную демонстрацию, чтобы начать аудит периметра ваших клиентов на GitHub». ***(The Pivot: How MSPs can Turn a Challenge Into a Once-in-a-Decade Opportunity // The Hacker News (https://amp.thehackernews.com/thn/2023/02/the-pivot-how-msps-can-turn-challenge.html). 03.02.2023).***

***

«Национальная лаборатория возобновляемых источников энергии (NREL) опубликовала отчет, который поможет авиационной отрасли внедрить меры кибербезопасности для электроавиации.

Исследование финансировалось Федеральным авиационным управлением, которое изучает потенциал электрификации аэропортов для достижения целей воздушной мобильности в США, сообщило в понедельник NREL.

Согласно отчету, безопасность должна быть включена на ранних этапах проектирования и закупок производства электрических самолетов. Во время закупки технологий владельцы объектов могут использовать такие оценки, как Модель зрелости возможностей кибербезопасности Министерства энергетики и Структура кибербезопасности распределенных энергетических ресурсов, для выявления потенциальных уязвимостей и защиты энергетических активов.

NREL заявил, что отрасль также должна использовать уроки, извлеченные из киберугроз, при наземной зарядке электромобилей.

Чтобы защитить виртуальную информацию в аэропортах, несколько заинтересованных сторон могут масштабировать системы обнаружения вторжений или использовать лабораторную платформу шифрования операционных технологий Module OT». ***(Jamie Bennet. NREL Report: Cybersecurity Should Be Implemented Early in Aviation Electrification // Executive Mosaic (https://executivegov.com/2023/02/nrel-cybersecurity-should-be-implemented-early-in-aviation-electrification/). 01.02.2023).***

***

«2022 год был годом, когда кибербезопасность повлияла на жизнь и образ жизни каждого человека — она скорректировала цену на бензин для вашего автомобиля, возможность получить стейк в ресторане, возможность и время визита к врачу, а также был ли скомпрометирован ваш любимый игровой сайт. ваши личные финансовые данные. Повышенное давление было оказано на тех, кто является профессионалами и практиками в области кибербезопасности, вызванными более строгим нормативным климатом, и мы, несомненно, увидим, как правительство и органы по стандартизации продолжат преследовать организации, которые пренебрегают или сводят к минимуму их внимание к кибербезопасности.

Все мы знаем заголовки об утечках данных в 2022 году (например, Copper Mountain Mining, Mizuno, Intrado, Rackspace, T-Mobile и обширный глобальный список организаций государственного и частного секторов). Но компании должны задаться вопросом: КАК происходят эти атаки и что мы можем сделать, чтобы

этого избежать? Именно здесь наша работа в качестве менеджеров по бизнес-рискам должна четко сообщать обо всех действиях, предпринятых киберпреступниками для компрометации цифровых активов, и о том, что нам нужно сделать, чтобы защитить наши организации и быть устойчивыми (защищать, обнаруживать и восстанавливать) от атак.

Давайте начнем с использования программ-вымогателей в качестве «измерителя вредоносности» кибербезопасности, то есть использования распространенности и воздействия этого экономического преступления в качестве меры улучшения или снижения эффективности в нашей отрасли. Мы часто не знаем, был ли выплачен выкуп. Есть много случаев, как в случае с Colonial Pipeline в 2021 году, когда мы знаем, что был выплачен выкуп в размере 4,4 миллиона долларов. Плата выкупа свидетельствует о крайнем провале вашей стойкости, подготовленности и готовности. Не будем забывать, что основные деятели угроз очень хорошо финансируются, и во многих случаях злоумышленники проводят серьезные исследования, чтобы понять, сколько организация может заплатить, чтобы увеличить вероятность суммы платежа, требуемой вымогателем.

Мы знаем это. Что число организаций во всем мире, пострадавших от программ-вымогателей, немного выросло до 66% в 2022 году (увеличение на 3% по сравнению с 2021 годом). 68% этих жертв заплатили выкуп в 2022 году, что на 19% меньше, чем в 2021 году. Это важное улучшение, но почти семь из каждых десяти по-прежнему очень высоки.

16% организаций трижды сталкивались с программами-вымогателями, что указывает на отсутствие в этих организациях основ кибербезопасности и гигиены, а также на игнорирование мер по исправлению положения, необходимых для того, чтобы не стать повторной жертвой. 56% подвергшихся атаке потеряли прибыль, 50% потеряли клиентов, а 43% значительно потеряли репутацию и доверие.

То, что мы ясно видим в 2022 году, — это более масштабные индивидуальные атаки, чем когда-либо прежде. В 2022 году в 11% атак программ-вымогателей сумма вымогательства превысила 1 миллион долларов, а общий средний выкуп за весь год составил 220 298 долларов. Однако сумма выкупа ничтожна по сравнению с затратами на восстановление и воздействие в размере 4,54 миллиона долларов в 2022 году, что лишь немного меньше, чем 4,62 миллиона долларов в 2021 году.

Ожидается, что глобальные затраты на ущерб от программ-вымогателей (опять же, не сама сумма выкупа) вырастут до 265 миллиардов долларов к 2031 году, в результате чего программы-вымогатели войдут в число 50 крупнейших по размеру валового национального продукта в мире.

Наконец, по данным Всемирного экономического форума (ВЭФ), «по оценкам, к 2025 году во всем мире будет создаваться 463 экзабайта данных каждый день — это эквивалентно 212 765 957 DVD в день!» Но по мере того, как создается больше данных и ценность данных (часто классифицируемых как «стоимость записи») стремительно растет, мы можем только ожидать, что все больше злоумышленников попытаются успешно использовать новый вектор угроз, вызванный растущими объемами данных. Как однажды заметил миллиардер Уоррен Баффет, данные — это новая нефть.

Хотя некоторые из этих статистических данных движутся в улучшенном направлении, растущая изощренность киберпреступников, добавляющих искусственный интеллект (ИИ) к их бесконечному набору эксплойтов нулевого дня и атак социальной инженерии, просто ужасает. Исследовательская компания Cybersecurity Ventures теперь прогнозирует, что новая атака программ-вымогателей будет происходить каждые 2 секунды (по сравнению с 11 секундами в начале 2022 года), поскольку злоумышленники продолжают совершенствовать свои полезные нагрузки вредоносных программ и связанные с ними действия по вымогательству.

Кроме того, операционные поверхности атак и атаки, направленные на конфиденциальность/PII, увеличиваются в основном по мере того, как миллионы устройств IoT, IoMT, IIoT подключаются к сети, по некоторым оценкам, к 2030 году их будет более 50 миллиардов во всем мире, а также бесчисленное количество организаций, работающих в гибридном режиме (облачные технологии). и локально) с преимущественно удаленной рабочей силой после пандемии 2020–2021 гг.

Теперь давайте посмотрим глубже на то, что мы в Seceon предсказали на 2022 год, а затем давайте посмотрим, что, по нашим прогнозам, произойдет в 2023 году. Спасибо, что присоединились к нам в этом путешествии!

В 2022 году в мировой индустрии кибербезопасности наблюдался резкий рост текучести кадров. Это произошло из-за растущей конкуренции на рынке труда, когда большое количество квалифицированных кандидатов претендовали на одни и те же рабочие места. Компаниям пришлось скорректировать свои стратегии найма, чтобы оставаться впереди конкурентов и нанимать лучших специалистов. В настоящее время ISC2 оценивает нехватку рабочей силы в 3,1 миллиона специалистов по всему миру. Похоже, что пути входа для тех, кто новичок в кибербезопасности, изменились. 26% профессионалов с опытом работы менее 3 лет начали работать в сфере, отличной от ИТ или киберпространства, тогда как только 1 из 5, 20% с 8 и более годами опыта работы в киберпространстве начинали работу в сфере, отличной от ИТ или киберпространства.

Более того, у нас есть разрыв в рабочей силе в области кибербезопасности: большинство выпускников колледжей и университетов переходят к техническим областям кибербезопасности, и очень немногие в области управления, рисков и соответствия (GRC), в то время, когда самая большая потребность в GRC. Это значительный риск. Таланта мало. Если вы не можете получить навыки, необходимые для эффективного управления кибер-рисками, то ваш кибер-риск останется без изменений, что приведет к разоблачениям, высокой стоимости страховки (или утрате страховки) и оставит вас уязвимыми для атак, вымогательства и утечки данных. По данным ISC2, 57% организаций имеют незанятые должности и не могут найти подходящего пула кандидатов.

Кроме того, появление облачных технологий и автоматизации означало, что многие из традиционных ролей в кибербезопасности должны были развиваться, и только некоторые из существующих сотрудников отправлялись в путешествие, а другие покидали свои должности в поисках новых возможностей. Несмотря на эти сдвиги, спрос на специалистов по кибербезопасности продолжал расти, и эта

отрасль оставалась одним из самых востребованных секторов в технологической отрасли с нулевым процентом безработицы среди ищущих работу.

Компании по всему миру стали уделять больше внимания соблюдению требований в разных отраслях. Это включало более строгие требования к безопасности данных, конфиденциальности и соблюдению ряда законов, правил и стандартов. Организации всех размеров, от малого бизнеса до крупных корпораций, должны были придерживаться все более сложных правил и политик, касающихся защиты персональных данных и обращения с конфиденциальной информацией. Компании также должны были принять дополнительные меры для защиты своих систем от кибератак и других вредоносных действий. В свою очередь, специалисты по кибербезопасности должны были быть в курсе последних стандартов и технологий безопасности, а также следить за тем, чтобы их системы соответствовали новым и существующим нормам. Предприятиям пришлось инвестировать в новые технологии и стратегии, чтобы соответствовать новым требованиям, таким как облачные вычисления, анализ угроз и искусственный интеллект. В целом, акцент на соблюдении требований в 2022 году привел к повышению осведомленности об угрозах кибербезопасности и усилению чувства ответственности среди всех заинтересованных сторон. Советы директоров в настоящее время задают вопросы о киберугрозах, возможностях и о том, что они могут сделать, чтобы помочь компаниям, входящим в их состав, особенно в этой области, которую мы называем управлением рисками и установлением того факта, что соответствие не подлежит обсуждению. Распоряжение 14028, недавние поправки к Правилам защиты Федеральной торговой комиссии, принятие нескольких инициатив штатов в отношении конфиденциальности (California CPRA, Colorado, Connecticut, Utah Virginia) и недавние директивы CISA — все это свидетельствует о усилении контроля и принятии законодательных мер, требующих соблюдения разумная практика кибербезопасности и конфиденциальности.

Технология кибербезопасности на основе искусственного интеллекта продолжала развиваться быстрыми темпами и становилась все более централизованной. Это позволило организациям лучше обнаруживать угрозы безопасности и реагировать на них. Автоматизированные инструменты безопасности, такие как машинное обучение и прогнозная аналитика, использовались для более эффективного выявления и блокировки вредоносных действий. В то же время получили дальнейшее развитие и внедрение облачные решения для обеспечения безопасности, позволяющие организациям лучше защищать свои данные и системы. Облачные решения упростили обнаружение и сдерживание угроз, а также быстрое реагирование на инциденты. Внедрение моделей безопасности с нулевым доверием также вызвало всплеск популярности в 2022 году. Эта модель основана на постоянной проверке личности пользователя и прав доступа, а не на доверии пользователям, которые уже находятся в системе. Это помогло организациям обеспечить безопасность своих данных и систем, даже когда к ним обращались из-за пределов их сетей. Наконец, использование шифрования и токенизации также стало более распространенным в 2022 году. Эти меры безопасности помогают защитить данные от доступа или кражи, даже если

данные перехвачены. Кроме того, математика, примененная к вариантам использования, должна привести к более эффективному и действенному SOC с меньшим количеством предупреждений и шума. ИИ также предлагает преимущество предоставления системы измерения с использованием аналитики безопасности для вероятностного измерения риска, преодолевая проблему невозможности количественно оценить вероятность и влияние угрозы на окружающую среду…» ***(Cybersecurity 2022: The Year in Review by Seceon Thought Leadership // Seceon Inc (https://www.seceon.com/cybersecurity-2022-the-year-in-review-by-seceon-thought-leadership/). 02.02.2023).***

***

«Недавний отчет, опубликованный компанией-разработчиком программного обеспечения Splunk, показал, что организациям государственного сектора часто не хватает информации о кибербезопасности, необходимой для эффективного реагирования, и они борются больше, чем частный сектор, в использовании данных для обнаружения и предотвращения угроз.

На основе опроса более 200 менеджеров по ИТ и безопасности данных, проведенного Foundry Research, в декабрьском отчете сравнивается состояние федеральной защиты кибербезопасности с состоянием частного сектора. Цель состояла в том, чтобы определить, как организации используют данные для решения приоритетных задач кибербезопасности, и выявить препятствия для действий на основе этих данных. В ходе опроса также оценивалась степень обмена информацией об угрозах внутри обоих секторов и за их пределами.

«Кибербезопасность стоит недешево, а федеральные агентства огромны», — говорит Райан Ковар, выдающийся стратег безопасности в Splunk. Ковар также является руководителем SURGe, синей исследовательской группы Splunk по безопасности, которая выступает в качестве технического связующего звена между государственными и частными партнерствами в организации. Ковар сказал, что проблемы государственного сектора связаны с огромным размером правительства, даже по сравнению с крупнейшими частными организациями, такими как Google и Microsoft, в которых работают сотни тысяч сотрудников.

«Почтовая служба насчитывает более 500 000 сотрудников; Минобороны – более миллиона», — сказал Ковар. «Когда вы размером с федеральное правительство, хранение данных — это проблема физики, а не просто проблема затрат».

Среди респондентов из государственного сектора 63 процента заявили, что им сложно использовать данные для обнаружения и предотвращения угроз, по сравнению с 49 процентами респондентов из частного сектора. Государственный сектор также с большей вероятностью столкнулся с проблемами, связанными с кибербезопасностью (66% респондентов из государственного сектора по сравнению с 56% респондентов из частного сектора).

Респонденты из государственного сектора назвали несколько причин этих недостатков, включая пробелы в навыках, нехватку ресурсов и недостаточное понимание ландшафта угроз.

Опрос показал, что самым большим препятствием для государственного сектора в решении приоритетов и задач в области кибербезопасности является бюджет. Почти 80 процентов респондентов из государственного сектора заявили, что бюджет ограничивает их возможности в решении этих вопросов. недавно Сводный пакет расходов на 2023 год, подписанный президентом Джо Байденом, показал значительное увеличение финансирования кибербезопасности, в том числе 1,3 миллиарда долларов на программы кибербезопасности в Агентстве кибербезопасности и безопасности инфраструктуры (CISA), что на 230 миллионов долларов больше, чем в прошлом году, согласно данным. FedScoop.

Что касается информации об угрозах, 44 процента респондентов из государственного сектора заявили, что доступная им общая информация о кибербезопасности недостаточна для их нужд, по сравнению с 29 процентами респондентов из частного сектора. Ковар, который работал как в государственном, так и в частном секторе, утверждает, что эти цифры могут быть результатом того, что государственный сектор знает, чего ему не хватает, а частный сектор не знает обо всех возможностях.

«Когда я работал в государственном секторе, у меня было значительно больше интеллекта, чем в частном», — говорит Ковар. «Мне интересно, часть этого заключается в том, что люди знают, сколько они могли бы иметь, но не могут это сделать из-за нехватки ресурсов. И сколько из этого частный сектор не знает, что он может иметь?»

В ноябре Управление общих служб признало это и предприняло шаги для решения этой проблемы. От имени CISA GSA подал запрос на предоставление информации о доступности корпоративных услуг Threat Intelligence, чтобы помочь агентству в развитии возможностей анализа угроз. CISA назвала фрагментированную информацию об угрозах одним из существующих барьеров в федеральной киберэкосистеме, встречающихся на протяжении всего жизненного цикла анализа угроз.

Как ограничения данных увеличивают разрыв между публичным и частным секторами

Согласно отчету, эти проблемы с данными ограничивают возможности обоих секторов обмениваться информацией друг с другом, препятствуя сотрудничеству между государственными и частными организациями. Результаты опроса показывают, что организации в обоих секторах гораздо чаще делятся информацией внутри своего сектора, чем между секторами.

Тем не менее, два сектора были согласованы в отношении того, какими знаниями и информацией важно делиться:

Информация об угрозах и действующие лица (69 % общедоступных и 63 % частных)

Информация о событиях безопасности в режиме реального времени (60% общедоступных и 69% частных)

Учебные материалы и лучшие практики по кибербезопасности (79 % общедоступных и 68 % частных)

Сравнительные данные (36% общедоступных и 31% частных)

Ковар сказал, что разрыв происходит из-за того, что у двух секторов разные задачи и возможности, поэтому у каждой стороны разные представления об исполнении.

«Мы увидим, как люди соглашаются с целями, но то, как вы их реализуете и выполняете в государственном и частном секторах, будет отличаться», — говорит он. «Во-вторых, у государственного сектора есть мандат помогать гражданам, а не извлекать прибыль. Там очень большая разница».

Забегая вперед, наиболее распространенные инвестиции в кибербезопасность среди респондентов из государственного сектора включали мониторинг/оповещение, анализ угроз и оценку безопасности». ***(Michael Hickey. Federal Cybersecurity vs. Private: How Do Agencies Stack Up? // FedTech (https://fedtechmagazine.com/article/2023/02/federal-cybersecurity-vs-private-how-do-agencies-stack?amp). 02.2023).***

***

«Согласно новому отчету, когда дело доходит до обеспечения безопасности помещений, большинство предприятий отдают приоритет предотвращению, а не обнаружению, расследованию и реагированию. Однако в результате большое количество фирм страдает от утечек данных или других атак, причем инциденты постоянно усугубляются.

Исследователи из Exabeam опросили 500 специалистов по ИТ-безопасности и пришли к выводу, что примерно две трети респондентов (65%) считают предотвращение угроз своей главной задачей (открывается в новой вкладке).

Для третьего (33%) - обнаружение было наивысшим приоритетом.

Что еще хуже, предприятия на самом деле действуют в соответствии с этим мышлением. Почти три четверти (71%) тратят от 21% до 50% своего бюджета на ИТ-безопасность на предотвращение, а 59% инвестируют столько же, сколько и на обнаружение, расследование и реагирование.

Проблема с этим подходом, по словам главного специалиста по безопасности Exabeam Стива Мура, заключается в том, что фирмы сосредотачиваются на предотвращении, когда мошенники уже находятся внутри стен, что делает их усилия тщетными.

«Как известно, настоящий вопрос заключается не в том, находятся ли злоумышленники в сети, а в том, сколько их, как долго они имеют доступ и как далеко они зашли», — говорит Мур. «Команды должны обнародовать этот вопрос и относиться к нему как к неписаному ожиданию перераспределения своих инвестиций и действий, уделяя необходимое внимание согласованию действий злоумышленников и реагированию на инциденты. Профилактика не удалась».

На вопрос, уверены ли они, что смогут предотвратить нападения, большинство респондентов ответили положительно. На самом деле, 97% сказали, что они уверены в своих инструментах и процессах для предотвращения и выявления вторжений и утечек данных.

Однако, когда их спросили, легко ли они скажут своему боссу, что их сети в то время не были взломаны, только 62% ответили утвердительно, а это означает, что более трети сомневаются.

Другими словами, говорит Exabeam, команды безопасности слишком самоуверенны и имеют данные, подтверждающие это. Ссылаясь на отраслевые отчеты, компания утверждает, что в прошлом году 83% организаций столкнулись с более чем одной утечкой данных». ***(Sead Fadilpašić. Many security teams are prioritizing prevention over detection, with disastrous results // Future US, Inc (https://www.techradar.com/news/many-security-teams-are-prioritizing-prevention-over-detection-with-disastrous-results). 03.02.2023).***

***

«Кибербезопасность уже давно имеет жизненно важное значение для бизнеса и в последние годы стала еще более важной статьей расходов. Как склонны признавать большинство технических экспертов, ни одна система не может быть спроектирована так, чтобы быть абсолютно безопасной или абсолютно надежной.

В мире, который все больше зависит от данных, предприятия должны сосредоточиться на сохранении своих ценных и в равной степени уязвимых цифровых активов в неприкосновенности. Кибератака может быстро и существенно снизить стоимость сделки и, если ее вовремя не выявить, может привести к увеличению рисков и заражению систем покупателя.

Так же, как он берет на себя долги и обязательства, покупатель, желающий приобрести акции, унаследует все кибер-уязвимости бизнеса. Следовательно, покупатель должен опасаться не только того, что ему не удастся получить полную стоимость того, что он ищет, но и того, что он запоздало обнаружит, что цель обременена недостатками кибербезопасности, которые создают риски для покупателя.

Кибер-должная осмотрительность

Учитывая риск, связанный с кибератаками, безопасность следует учитывать на всех этапах процесса. Проверка готовности цели к кибербезопасности должна быть такой же обычной, как и оценка финансовых, правовых, операционных или репутационных рисков цели.

Если комплексная проверка выявляет уязвимости, предыдущие инциденты или в целом устаревшие системы, покупатель должен предвидеть необходимость выделения дополнительных расходов на цель для улучшения ее систем безопасности. Это может побудить покупателя договориться о более низкой покупной цене или установить механизм удержания/депонирования части цены, чтобы обеспечить защиту от киберугроз после завершения.

Кибератака, происходящая между подписанием и закрытием, может представлять собой существенное неблагоприятное изменение в соответствующем бизнесе, что должно позволить покупателю пересмотреть условия сделки или даже отказаться от нее.

Но даже самый тщательный due diligence может не подтвердить соответствие цели требованию отсутствия инцидентов, ставящих под угрозу безопасность данных. Следовательно, покупатели могут также искать защиту от киберугроз с помощью заявлений и гарантий. Поскольку заверения и гарантии в конечном счете связаны с распределением рисков, продавцы захотят ограничить свой риск

нарушения гарантий путем введения квалификаторов, таких как их знания (т. е. предоставление гарантии на основе знаний определенной группы лиц) или «существенных» квалификаторов (т. е. ограничить гарантию вопросами, существенными для стоимости сделки), или вообще ограничить гарантии определенным ретроспективным периодом.

Независимо от тактики ведения переговоров, предусмотрительный покупатель цифровых активов будет запрашивать заявления и гарантии, охватывающие как минимум наличие и соблюдение политик безопасности данных, соблюдение договорных обязательств в отношении безопасности данных, отсутствие несанкционированного доступа к данным цели, отсутствие инцидентов, связанных с безопасностью, и наличие мер безопасности для защиты систем и информации.

Заключение

Кибербезопасность — это не просто технический термин. Это юридическое обязательство для компаний, и, когда на карту поставлены дорогостоящие цифровые активы, это может быть фактором, который делает или срывает сделку по слиянию и поглощению. Таким образом, кибербезопасность должна быть постоянной заботой на протяжении всей сделки по слиянию и поглощению, от ранних стадий должной осмотрительности до окончательного соглашения, содержащего заверения, гарантии и компенсации, направленные на покрытие возможных киберрисков, и, в конечном итоге, до полномасштабной безопасной интеграции бизнеса». ***(Madalina Neagu. Cybersecurity in M&A transactions: common representations & warranties // Schönherr Rechtsanwälte GmbH (https://www.schoenherr.eu/content/cybersecurity-in-m-a-transactions-common-representations-warranties/). 01.02.2023).***

***

«…Согласно отчету Всемирного экономического форума Global Cybersecurity Outlook 23 Insight Report (опубликованному в сотрудничестве с Accenture), хотя бизнес-лидеры лучше осведомлены о риске киберпроблем для своих организаций, остаются проблемы, связанные с тем, как организации решают и снижают этот риск.

Согласно отчету, «лидеры бизнеса и киберпространства считают, что глобальная геополитическая нестабильность с умеренной или высокой вероятностью может привести к катастрофическим кибер-событиям в ближайшие два года». Респонденты понимают меняющуюся картину кибератак и «теперь считают, что кибератаки, скорее всего, сосредоточатся на подрыве бизнеса и репутационном ущербе. Это две главные проблемы среди респондентов».

Кроме того, 43 процента респондентов считают, что «вероятно, что в ближайшие два года кибератака существенно затронет их собственную организацию». Они также признают, что риск кибербезопасности их организации связан с состоянием безопасности их партнеров по цепочке поставок. Руководители «рассматривают законы о конфиденциальности данных и правила кибербезопасности как эффективный инструмент для снижения киберрисков в отрасли». Не то чтобы они хотели видеть больше правил, но они признают, что

такие правила могут стимулировать организации к внедрению основных мер кибербезопасности. Хотя новости о том, что изощренные атаки в области кибербезопасности будут увеличиваться и становиться все более разрушительными, неутешительны, похоже, что организации все больше осознают риск, пытаются создать более надежную систему кибербезопасности и ищут способы более четкого общения внутри организации. Все эти меры являются положительными, но сложными, особенно в условиях нехватки специалистов по кибербезопасности во всем мире». ***(Linn Foster Freedman. World Economic Forum's Global Cybersecurity Outlook for 2023 Is Bleak // Robinson & Cole LLP. (https://www.dataprivacyandsecurityinsider.com/2023/02/world-economic-forums-global-cybersecurity-outlook-for-2023-is-bleak/). 02.02.2023).***

***

«Как специалист по безопасности, вы знаете, что, хотя технология является важным инструментом для предотвращения превращения вредоносной деятельности в реальную проблему в вашей среде, это только часть уравнения. Хорошо спроектированный центр управления безопасностью (SOC) необходим для защиты вашего предприятия от постоянно меняющихся рисков, связанных с современными технологиями…

Следуйте этим семи рекомендациям, которые помогут вам создать SOC и обеспечить его успех.

1. Поймите осуществимость вашего проекта до того, как вы начнете строить SOC.

Создание успешного Центра операций по обеспечению безопасности (SOC) начинается с углубленной оценки осуществимости, которую следует провести на раннем этапе. Такие оценки должны учитывать все обычные переменные, такие как бюджет и кадровый потенциал, а также включать различные другие факторы, которые могут повлиять на общий результат.

Например, надлежащее укомплектование персоналом является ключевым фактором эффективности любого центра обеспечения безопасности. Наличие нужного количества персонала напрямую влияет на производительность — если круглосуточный мониторинг невозможен, то он может создать среду, в которой успех недостижим.

Не уверены, что у вас есть возможности для создания или управления SOC самостоятельно? Откройте для себя преимущества поставщика управляемых услуг безопасности и узнайте, почему это необходимо для обеспечения круглосуточной безопасности — все это подробно описано в нашей соответствующей публикации в блоге.

2. Определите, какие услуги желательны.

Основная функциональность SOC заключается в обеспечении мониторинга и реагирования на инциденты. Однако SOC может предоставлять дополнительные услуги в зависимости от уникальных потребностей организации. Эти услуги могут включать анализ вредоносного ПО, управление уязвимостями и цифровую криминалистику.

Важно обеспечить желаемые ожидания от SOC, создавая большую ясность в отношении ожиданий и обязанностей, которые будет выполнять эффективный SOC.

3. Разработайте варианты использования и источники данных.

Сценарии, подлежащие мониторингу, называемые вариантами использования, должны быть разработаны. Эти варианты использования должны иметь отношение к организации и должны быть достойны внимания. Знание среды организации может улучшить это, так что критически важные активы будут расставлены по приоритетам.

Вы захотите:

Определите источники данных для ваших вариантов использования,

Рассмотрите соответствующие угрозы и инциденты для отслеживания.

В зависимости от целей организации могут быть разработаны определенные варианты использования для соблюдения требований. Если эти оповещения о соответствии не требуют тщательного анализа, то автоматизация, которая может поддерживаться SOAR, может сделать их более эффективными и снизить нагрузку на SOC.

4. Выбирайте связные, гибкие технологии.

SOC может использовать множество технологий для своих услуг. Эти технологии должны быть выбраны с умом, чтобы гарантировать, что SOC выполняет свои задачи.

Решения SIEM и SOAR часто используются вместе для мониторинга и реагирования на инциденты. Выбранные технологии должны быть адаптированы к среде и потребностям организации.

5. Выберите предпочитаемую модель SOC.

Существует три модели SOC, которые следует рассматривать в зависимости от потребностей и желаний организации: специализированные, аутсорсинговые и гибридные решения.

Выделенный SOC обеспечивает максимальный контроль и прозрачность, но может иметь повышенную стоимость.

Аутсорсинг SOC третьей стороне, такой как MSSP, может быть дешевле, чем создание выделенного SOC.

В гибридном решении некоторые обязанности SOC будут переданы третьей стороне.

6. Определите метрики, относящиеся к организации.

Организация может использовать метрики, собранные для SOC, для определения областей, требующих улучшения, и принятия обоснованных решений. Эти показатели должны быть измеримыми и релевантными, чтобы быть полезными. Метрики также могут использоваться для определения того, насколько успешно SOC работает в настоящее время и где он должен быть в будущем.

7. Интегрируйте методы документирования в процесс.

Процесс документирования важен для многих функций информационных технологий, и SOC интенсивно использует документацию. Политики, процедуры, проблемы, исключения и другая информация должны быть тщательно задокументированы, чтобы гарантировать их четкое определение и доступность

информации для будущего использования. В частности, аналитики SOC могут использовать множество задокументированных сценариев для различных вариантов использования…» ***(Cameron Krivanek. Building a SOC: 7 Best Practices to Consider // Hurricane Labs, LLC. (https://hurricanelabs.com/blog/7-considerations-for-establishing-an-effective-soc/). 03.02.2023).***

***

«Кибербезопасность становится все более изощренной с помощью передовых инструментов и технологий безопасности. Следовательно, инструменты и технологии безопасности должны быть более предсказуемыми, а лидеры в области безопасности должны быть более активными и инновационными, чтобы иметь возможность отстаивать свои позиции. Для обеспечения безопасности им необходимо иметь больше информации о своей распределенной бизнес-среде. Им необходимо предпринять серьезные шаги в области кибербезопасности, чтобы получить целостное представление о функциях кибербезопасности, развернутых в отделах, для сохранения больших данных и других активов компании.

Организации должны попытаться создать упреждающие стратегии кибербезопасности, чтобы заполнить пробел в рабочей силе на основе мер безопасности. Разработка и внедрение единых стратегий должны включать следующие аспекты:

Показатели кибербезопасности и оценки в рабочей силе

Непрерывные инновации для поощрения новых способов борьбы с киберугрозами

Образовательная программа по кибербезопасности

Масштабные ИТ-трансформации

С помощью этих параметров директора по информационной безопасности должны поощрять интегрированную координацию и совместную работу руководителей ИТ и службы безопасности, чтобы добиться успеха в предотвращении кибератак. Это особенно связано с острой необходимостью использовать и развертывать режим быстрого реагирования, чтобы помочь организациям смягчить последствия атак программ-вымогателей и восстановиться до того, как они создадут сбои. Глядя на неиспользованные области новых кибер-талантов, организациям следует поощрять учебные материалы для развития навыков у сотрудников. Делая это, организации могут получить преимущество более квалифицированной рабочей силы экспертов по безопасности.

Сегодня организациям необходимо расширить свои усилия по развитию персонала в области кибербезопасности за счет прозрачного представления соответствующих данных, которые помогут оценить влияние мер безопасности и эффективность инициатив по развитию персонала.

По мере того, как предприятия переходят на цифровые технологии, угроза для данных, сетей и приложений возрастает из-за увеличения количества точек входа, которые теперь доступны в Интернете. С другой стороны, преимуществом цифровых инфраструктур является гораздо более совершенный механизм сопоставления данных, благодаря которому лидеры в области безопасности получают гораздо большую прозрачность своих инициатив в области безопасности.

Это может стать основой для будущей дорожной карты безопасности, а поддержание будущих планов кибербезопасности может быть построено на прочной основе данных о развертывании и надежности системы. Надлежащее представление о кибербезопасности с помощью данных даст представление о том, как организации могут наилучшим образом смягчить последствия дефицита кибернетической рабочей силы, и может даже предоставить прогнозную информацию, которая может помочь уменьшить количество атак с течением времени.

Навыки, но и социальные навыки. Мягкие навыки в общении, поощрение гибкости и лидерство представляют собой наиболее важные атрибуты, определенные для улучшения развертывания кибербезопасности в рабочей силе.

Дорожные карты по улучшению развертывания кибербезопасности в рабочей силе побуждают организации создавать соответствующий конвейер с участием экспертов по безопасности в качестве дополнительного преимущества. Организации могут находить и удерживать более разнообразные наборы экспертов с помощью стратегий привлечения талантов для выявления потенциальных сотрудников, создания более инклюзивной рабочей культуры путем обучения руководителей и сотрудников службы безопасности совместному решению проблем и пересмотру политики в отношении существующей инфраструктуры кибербезопасности. Это может включать в себя инструменты, технологии и методологии, чтобы обеспечить лучшее и продвижение для устранения традиционных барьеров.

Неудивительно, что организации должны сосредоточиться на долгосрочных планах кибербезопасности, что является важным усилием для повышения кибербезопасности в организациях. Безопасность не должна достигаться за счет инноваций, поэтому организации должны оставаться инновационными и гибкими. Благоприятные правила кибербезопасности и развертывание могут заставить рабочее место выполнять функции и операции кибербезопасности на должном уровне. Такие развертывания, вероятно, будут управлять производительностью сотрудников и сбалансировать подходы к кибербезопасности в соответствии с бизнес-требованиями.

Учитывая значительный рост числа кибератак, организациям может быть сложно найти адекватные решения. К счастью, имея четкую дорожную карту политики кибербезопасности, организации могут найти правильные цели кибербезопасности, которые помогут эффективно улучшить все аспекты, что приведет к эффективной инфраструктуре кибербезопасности». ***(Anushree Bhattacharya. Major Attempts to Improve Cybersecurity Workforce Across Organizations // ITSecurityWire (https://itsecuritywire.com/featured/attempts-to-improve-cybersecurity-workforce-across-organizations/amp/). 08.02.2023).***

***

«Каждая новая многомиллионная утечка или изощренный изощренный взлом побуждает бесчисленное количество организаций тяготеть к новым кибербезопасности инструментам, которые они считают еще более

изощренными. Простое вбрасывание денег в проблему не решит более крупную проблему.

Чтобы понять суть этой проблемы, ключевым моментом является моделирование угроз. Это не какое-то новое программное обеспечение на основе подписки, которое обеспечивает вашу безопасность; это практика переворачивания уравнения с ног на голову, чтобы вы видели вещи так же, как хакер.

Что такое моделирование угроз?

Моделирование угроз, обычная практика в разработке приложений, по сути то же самое, что в страховом мире называют «анализом рисков». Он предлагает лучшее понимание того, откуда исходят угрозы, и позволяет размещать смягчающие элементы управления в нужных местах. Это приводит не только к повышению безопасности, но и потенциально к снижению затрат.

Например, если вы установили брандмауэр веб-приложений (WAF) за критически важными приложениями, возможно, вы добавили некоторую защиту. Однако для правильной работы WAF его необходимо настроить, и сотрудник должен поддерживать его, что увеличивает расходы.

Чего вы не получите в этом сценарии, так это какой-либо информации о дверях, которые вы могли непреднамеренно оставить открытыми на поверхности атаки. По данным ESG Research, 69% организаций столкнулись с тем или иным типом кибератаки, которая началась с использования неизвестного, неуправляемого или плохо управляемого цифрового актива, подключенного к Интернету.

Прохождение упражнения по моделированию угроз может оказать огромное влияние на всю организацию. Это не просто техническая практика, применимая к разработчикам. Директора по информационной безопасности (CISO) и директора по технологиям (CTO) должны использовать это с подходом «сверху вниз» во всех отделах, за которыми они наблюдают.

Есть четыре основных вопроса, которые следует задать себе при выполнении упражнения по моделированию угроз, чтобы лучше защитить свою организацию. Давайте погрузимся в каждый и поместим их в более широкий контекст.

На что нацелятся хакеры?

Чтобы победить хакеров, вам нужно знать, что вы должны защищать. Для этого требуется видимость, которую вы можете получить с помощью анализа вашей поверхности атаки — не только ваших внешних ресурсов, но и ваших внутренних. Эта полная картина вашей организации позволяет вам моделировать угрозы.

Когда организации проводят эту оценку, они часто обнаруживают забытые активы или ресурсы, которые, как они думали, были размещены временно, например, промежуточную среду, сторонние активы или активы клиентов, которые они забыли развернуть.

Рассмотрите риск через триаду ЦРУ: конфиденциальность, честность и доступность. Если конфиденциальность базы данных раскрыта, какому риску вы подвергаетесь? Даже если она не раскрыта — скажем, кто-то подделал базу данных — как ее отсутствие целостности влияет на организацию? Каковы последствия,

если распределенная атака типа «отказ в обслуживании» (DDoS) выводит базу данных из строя и она становится недоступной?

Когда этот риск становится очевидным, практикующие могут начать защищаться и попытаться преуменьшить опасность. Не делайте это упражнение на обвинение! Чтобы повысить уровень безопасности, вам нужно признать этот риск, а затем действовать в соответствии с ним.

Что может пойти не так?

Хакеры пытаются нанести максимально возможный ущерб. Они будут считать, что ваши наиболее важные бизнес-активы хорошо защищены, и вместо этого попытаются нацелиться на то, на что вы не обращаете внимания. Именно эти белые пятна часто вызывают у организаций самые большие головные боли.

Подумайте об этом в более ощутимом масштабе. Скажем, на задней двери вашего дома есть засов и замок на ручке, но у вас также есть собачья дверь. Возможно, это не то, как вы попадаете в дом, но вам лучше поверить, что если кто-то попытается проникнуть в дом, он воспользуется этим. То же самое касается поверхности атаки вашей организации.

Если у вас неправильно настроен веб-сервер или вы забыли, что у вас все еще есть активные ресурсы из вашей старой облачной инфраструктуры, именно так хакеры могут получить доступ и начать перемещаться. Именно здесь можно быстро экстраполировать данные на третьи стороны и цепочки поставок. По данным ESG, восемь из 10 организаций столкнулись с нарушением цепочки поставок, но только 22,5% контролируют всю свою цепочку поставок.

Что мы делаем по этому поводу?

При построении модели угроз необходимо расставить приоритеты вероятности событий. Возможно, хакер не найдет ваши старые облачные ресурсы, но более правдоподобно ли, что ваш домен написан с ошибкой? Какова вероятность того, что клиент введет это и подвергнется спуфинговой атаке?

Вам необходимо установить средства управления для смягчения угроз, которые вы считаете наиболее вероятными после того, как вы их все обнаружите. Отправной точкой для элементов управления обычно являются брандмауэры, потому что они охватывают то, о чем знает организация. Также распространены системы обнаружения и предотвращения вторжений, а также сети доставки контента. Но ни один из этих элементов управления не влияет на неизвестные, о которых организация не знает.

Достаточно ли хорошо мы работаем?

Поскольку организации обычно не имеют полного представления о своих поверхностях атаки, обычно можно сделать больше, чтобы защитить их. Моделирование угроз заставляет всех мыслить более творчески. Как только вы узнаете, как выглядит эта поверхность атаки, как вы можете ограничить угрозы? Одно дело признать стратегию, другое — внедрить ее в своей организации.

Быстрый способ снизить риск — снять активы, которые не используются. Они представляют угрозу только в том случае, если для них нет бизнес-логики, чтобы они все еще находились в вашей сети. Без них вы отсекаете пути, по которым хакер может скомпрометировать вашу организацию.

Вместо того, чтобы тратить бюджет на безопасность, бросая деньги на потенциальный риск взлома, моделирование угроз может показать вам, где находятся ваши уязвимости. Это напоминает вам, что эти забытые ресурсы все еще существуют и представляют потенциальную угрозу. Наличие этого уровня видимости дает вам лучший шанс победить хакеров, прежде чем они смогут получить доступ к вашей сети». ***(Marcos Lira. Why threat modeling can reduce your cybersecurity risk // VentureBeat (https://venturebeat.com/security/why-threat-modeling-can-reduce-your-cybersecurity-risk/). 10.02.2023).***

***

«…По данным французской компании-разработчика программного обеспечения IS Decisions, с начала века было подано около 2270 патентов, связанных с кибербезопасностью. Почти все — около 97% — были поданы с 2010 года, года, когда произошел огромный всплеск глобальных кибератак.

Согласно отчету «Лаборатории Касперского», общее количество кибератак в том году увеличилось примерно в восемь раз, в то время как Stuxnet, вредоносный компьютерный червь, саботировавший иранскую программу создания ядерного оружия, положил начало десятилетию громких киберинцидентов, таких как взлом Sony Pictures, совершенный Норт. Корейская Lazarus Group и ликвидация рынка наркотиков в даркнете Silk Road.

Сталкиваясь с растущими угрозами, страны соревнуются в поиске новых инновационных способов предотвращения кибератак, и данные показывают, что есть явные победители, когда речь идет о ведомствах, получающих наибольшее количество патентных заявок в области кибербезопасности.

Ведомство США по патентам и товарным знакам возглавляет список с 1087 патентными заявками, связанными с кибербезопасностью, поданными в период с 2000 по 2022 год. По словам исследователей, с самой большой в мире рабочей силой в области кибербезопасности, насчитывающей около 1,1 миллиона человек, неудивительно, что США лидируют в киберинновациях.

Среди 10 самых активных компаний, подающих заявки на патенты в области кибербезопасности, пять базируются в США, включая IBM, Boeing, Microsoft, Honeywell и Qomplx.

Международные заявки, поданные в соответствии с Договором о патентной кооперации, составляют следующий по величине объем заявок, связанных с кибербезопасностью: с 2000 года было подано 326 заявок. Международные патентообладатели могут защищать и охранять свою интеллектуальную собственность во всех 156 государствах-членах Всемирной организации интеллектуальной собственности.

Китай, мировой лидер по общему количеству патентных заявок, подал только около 13% глобальных патентов в области кибербезопасности и занимает третье место. Исследование, проведенное в 2014 году, показало, что качество патентных заявок в Китае было неудовлетворительным, и правительство Китая поставило перед собой задачу улучшить его…» ***(Daryna Antoniuk. More than 2,000 cybersecurity patent applications filed since 2010: report // The Record from Recorded***

Future News (https://therecord.media/more-than-2000-cybersecurity-patent-applications-filed-since-2010-report/). 07.02.2023).

***

«Международное арбитражное сообщество уделяет все больше внимания вопросам защиты данных и кибербезопасности. Учитывая судебный и межюрисдикционный характер международного арбитража в сочетании с крайне конфиденциальным характером информации, обычно обрабатываемой в международных арбитражах, важно, чтобы пользователи арбитража оценивали, как на них могут повлиять законы и правила о защите данных и какие типы информационной безопасности меры подходят для конкретного арбитража. Ряд организаций сотрудничали, чтобы опубликовать Протокол о кибербезопасности в международном арбитраже («Протокол кибербезопасности») и Дорожную карту защиты данных в международном арбитраже («Дорожная карта защиты данных»), чтобы предоставить практическое руководство для пользователей международного арбитража…

Протокол кибербезопасности

Протокол, который был недавно обновлен, содержит рекомендации по снижению рисков информационной безопасности в арбитраже. Признавая возросшее количество киберугроз, Протокол предоставляет образец протокола утечки персональных данных для нарушений, которые могут произойти в ходе судебного разбирательства (см. Приложение D-1). Протокол характеризует это дополнение как признание «важности наличия плана реагирования на инциденты, если инцидент безопасности произойдет во время арбитража».

Протокол содержит четырнадцать руководящих принципов. Основные выводы следующие:

Протокол предлагает образцы базовых методов обеспечения безопасности (Приложение A), но подчеркивает, что меры информационной безопасности в арбитраже не являются «универсальными» — не только потому, что могут существовать разные применимые правила защиты данных, требующие соблюдения различных обязательств, но также и потому, что каждый арбитраж является самостоятельным созданием (Принцип 1). Протокол рекомендует «разумный в данных обстоятельствах» стандарт для определения надлежащих мер, которые должны применяться в арбитраже (Принцип 5).

Принципы содержат руководство для пользователей арбитража в отношении того, как определить разумные меры кибербезопасности, в том числе путем описания и объяснения: (i) характеристик арбитража, которые стороны и трибуналы должны учитывать при реализации мер безопасности (например, «профиль риска арбитража », ресурсы участников арбитража и «эффективность арбитражного процесса») (принцип 6); (ii) категории мер, которые могут быть приняты в арбитраже (которые охватывают различные категории мер, такие как управление активами, контроль доступа и шифрование) (Принцип 7); и (iii) руководство о том, как конкретные обстоятельства или этапы арбитражного разбирательства могут потребовать специальных мер (например, слушаний и

конференций, обмена информацией и политики хранения и уничтожения после арбитража) (Принцип 8).

Протокол признает, что многие лица, помимо арбитров, сторон и арбитражных учреждений, могут нуждаться в доступе к информации, предоставленной в ходе арбитражного разбирательства. Таким образом, Принцип 3 рекомендует трибуналам, сторонам и арбитражным учреждениям обеспечить, чтобы все лица, участвующие в арбитраже, были осведомлены и соблюдали меры информационной безопасности, которые были приняты для этого арбитража.

Принципы отдают предпочтение соглашению сторон и рекомендуют оперативное внимание к вопросам информационной безопасности, как правило, на конференции по управлению делами (Принципы 9-10). Они отмечают, что трибуналы имеют право определять или изменять меры информационной безопасности, применимые в арбитраже (Принципы 11-12). И в случае нарушения этих мер или в случае инцидента информационной безопасности Протокол отмечает, что трибуналы могут распределять расходы и налагать санкции на стороны (Принцип 13). Однако в Протоколе отмечается, что он не устанавливает «какой-либо ответственности или стандарта ответственности для любых целей» (Принцип 14). Аналогичным образом Протокол признает, что он не заменяет применимые законы, правила арбитража, профессиональные или этические обязательства или другие обязательные обязательства. (Принцип 4)

Дорожная карта защиты данных

Дорожная карта представляет собой обновленную и доработанную версию проекта, опубликованного для общественного обсуждения в 2020 году, включая измененные формулировки и новые приложения. Дорожная карта адресована «участникам арбитража», которая ограничена «сторонами, их юрисконсультами, арбитрами и арбитражными учреждениями». Однако его руководство также применимо к другим лицам, «работающим на [а]рбитражного [п]рбитра или с ним во время арбитража».

Дорожная карта начинается с изложения ключевых понятий, касающихся защиты данных, включая «персональные данные», «субъект данных» и «обработка», а также понятий «контролеров» и «обработчиков данных» на основе принципов, установленных в правилах ЕС. Затем в дорожной карте описываются (в том числе со ссылками на примеры и гипотезы в контексте арбитража) девять общих принципов защиты данных, включенных в большинство правил защиты данных в стиле ЕС, которые включают принципы:

Справедливая и законная обработка при условии, что данные должны обрабатываться, если для этого есть законное основание.

Соразмерность, требующая принятия мер по защите данных для учета интересов субъектов данных, а также интересов и прав третьих лиц.

Минимизация данных, требующая, чтобы «количество [производимых] персональных данных было ограничено для достижения цели обработки этих данных».

Ограничение цели, ограничение сбора персональных данных только для выполнения «конкретной и законной цели» и ограничение обработки персональных данных любым другим способом, который может быть несовместим с этой целью.

Права субъекта данных, указывающие на то, что «лица, чьи персональные данные собираются и обрабатываются», имеют право на получение доступа к этим данным.

Точность, гарантирующая, что собираемые и обрабатываемые персональные данные должны быть «действительными, актуальными и полными» для цели их сбора, и требование их обновления по мере необходимости.

Безопасность данных, требующая от контроллеров данных принятия соответствующих «технических и организационных мер безопасности для защиты персональных данных», чтобы избежать рисков утечки данных.

Прозрачность, требующая, чтобы меры, принятые для защиты данных, были известны субъектам данных.

Подотчетность, требующая от контроллеров данных вести «учет своих усилий по обеспечению соблюдения требований по защите данных».

Затем в дорожной карте рассматривается, как соблюдение требований по защите данных может повлиять на различные этапы арбитражного разбирательства, включая этапы до и после арбитража, а также все промежуточные этапы.

Дорожная карта также включает одиннадцать приложений с контрольными списками вопросов для рассмотрения, примерами уведомлений о конфиденциальности для учреждений, арбитров и адвокатов, а также примерами положений о защите данных для первого процессуального постановления или круга ведения. В одном из приложений, добавленных к недавно выпущенной версии Дорожной карты, содержится контрольный список для соблюдения требований по защите данных при использовании онлайн-платформ управления делами. Как и Протокол, «Дорожная карта» представляет собой руководство, не имеющее обязательной силы, и не отменяет обязательств участника арбитража в соответствии с применимыми законами о защите данных…» (***Lee Rovinescu, Christine Lyon, Maria Paz Lestido. Updated Data Protection and Cybersecurity Guidelines for International Arbitration // TOO Freshfields Bruckhaus Deringer (https://riskandcompliance.freshfields.com/post/102i752/updated-data-protection-and-cybersecurity-guidelines-for-international-arbitratio). 06.02.2023).***

***

«…Тенденции, определяющие ландшафт киберугроз в 2022 году

1 Угрозы национальным государствам продолжали расти наряду с геополитическими потрясениями.

Крупные геополитические события 2022 года привели к резкому изменению сторон угроз кибербезопасности и способов защиты конфиденциальности данных. В частности, злонамеренная активность во всем мире высветила необходимость усиления мер безопасности для защиты от угроз со стороны национальных государств, что побудило правительства во всем мире ввести новые правила кибербезопасности. Ниже приведены наиболее примечательные действующие лица, представляющие угрозу национальному государству в 2022 году:

Россия увеличила свою активность, но стала более оппортунистической и менее скоординированной в своих кибератаках на Украину. Российская Федерация

выделялась как крупный субъект киберугроз из-за проведенных ею кибератак. Значительная часть активности угроз, базирующихся в России, была направлена против базирующихся в Украине организаций и их союзников. Были взломаны несколько государственных учреждений в Коста-Рике, а кампании программ-вымогателей и утечки данных нацелены на компании и организации здравоохранения по всему миру. Американские компании сообщили о 16-процентном увеличении числа кибератак, приписываемых России, после вторжения в Украину. Однако когда дело доходит до атак на украинскую инфраструктуру, оппортунистические действия российских хакеров стали более распространенными, в отличие от начала войны, когда атаки были гораздо более изощренными и скоординированными. Тем не менее, по крайней мере, с мая 2022 года пророссийские группы, такие как Killnet и Sandworm, проводят целенаправленные атаки в поддержку интересов России, начиная с литовских и заканчивая веб-сайтами правительства США.

Китай провел кибератаки и создал арсенал уязвимостей нулевого дня. Китайская Народная Республика также была основным действующим лицом угроз в 2022 году, о чем свидетельствует кампания Billbug (также известная как Thrip, Lotus Blossom, Spring Dragon), нацеленная на центры сертификации, правительственные учреждения и оборонные организации во многих странах. Кроме того, способность Китая выявлять и накапливать уязвимости нулевого дня раньше, чем другие страны, была подкреплена законом, принятым в 2021 году, который требует, чтобы все китайские организации сообщали правительству об обнаруженных уязвимостях до того, как будут раскрыты какие-либо другие сведения. Об успехе этого закона свидетельствует тот факт, что в 2022 году уровень публичного раскрытия уязвимостей кибербезопасности, исходящих из Китая, снизился по сравнению с предыдущими годами, и в то же время увеличилось количество анонимных сообщений. Все это указывает на арсенал незарегистрированных уязвимостей программного обеспечения, находящихся в распоряжении правительства Китая.

Иран был особенно агрессивен, совершив ряд разрушительных атак. Иран представлял собой актуальную киберугрозу в 2022 году, учитывая его агрессивное поведение после смены президента. Иран продемонстрировал свою способность проводить разрушительные атаки, включив сирены аварийных ракет в Израиле. Кроме того, иранские субъекты участвовали в атаках программ-вымогателей на цели национальных государств без намерения когда-либо предоставлять ключ, что предполагает намерение нанести ущерб, а не получить финансовую выгоду от атаки. Об этой деятельности стало известно, когда правительство Албании разорвало дипломатические отношения с Ираном после атаки программы-вымогателя 15 июля, в результате которой были временно закрыты многочисленные правительственные цифровые службы и веб-сайты Албании. Изощренность и агрессивность этих действий показывают, почему Иран считался серьезной угрозой кибербезопасности в 2022 году.

Северная Корея продолжает атаковать критически важные отрасли с помощью программ-вымогателей. Корейская Народно-Демократическая Республика занималась киберактивностью, используя свою самую известную

группу угроз Lazarus. Целевые фишинговые кампании использовали поддельные предложения о работе от таких компаний, как Amazon и Coinbase, в попытке скомпрометировать конфиденциальные данные. Спонсируемые государством субъекты использовали различные типы вредоносных программ и программ-вымогателей для нанесения ударов по критически важным отраслям, таким как здравоохранение, энергетика, аэрокосмическая промышленность и оборона. Например, двум поставщикам медицинских услуг в США пришлось заплатить выкуп, чтобы расшифровать свои системы. В целом, эти инциденты служат напоминанием для организаций о необходимости принимать активные меры для защиты своих данных от киберугроз, исходящих от северокорейских субъектов.

2 Риски цепочки поставок стали более опасными благодаря целенаправленным атакам на критически важную инфраструктуру.

Серьезные сбои в цепочке поставок были вызваны кибератаками: NotPetya проник в системы Maersk после того, как один компьютер был заражен вредоносным ПО в 2017 году, а хакеры взломали Colonial Pipeline в 2021 году, используя скомпрометированные учетные данные. В 2020 году SolarWinds также подверглась крупной кибератаке, связанной с компрометацией учетных данных и/или доступа третьих лиц. Совсем недавно, в 2022 году, Okta была атакована LAPSUS$, злоумышленник проник на GitHub, используя украденные токены приложений OAuth, а инфраструктура Comm100 была взломана, а в установщике чата был спрятан бэкдор. Такие события служили напоминанием о важности бдительности в отношении различных субъектов угроз и соблюдения протоколов для защиты цепочек поставок, а также информировали компании о рисках, связанных с атаками на цепочки поставок программного обеспечения в 2022 году: исследование, проведенное ReversingLabs, показало, что кибербезопасность цепочек поставок находится на высоком уровне. список приоритетов специалистов по безопасности: 98% опрошенных согласились с тем, что использование открытого исходного кода и стороннего программного обеспечения в сочетании с потенциальными угрозами от взлома программного обеспечения существенно повышает их риски безопасности. Кроме того, 87% знают, что такой вид вмешательства может привести к серьезным проблемам с безопасностью в их бизнесе. Кроме того, поставщики ИКТ-инфраструктуры все чаще становятся объектами угроз кибербезопасности, поскольку они предоставляют платформу для воспроизведения вредоносных атак, а пророссийская хакерская группа Killnet даже нацелилась на конкурс песни «Евровидение» в этом году, хотя и безуспешно. Как следствие, глобальное законодательство и правила, касающиеся конфиденциальности данных и безопасности цепочки поставок, также стали более строгими, часто с различными требованиями в разных юрисдикциях, а спрос клиентов на надежные решения для обеспечения безопасности также быстро растет.

Некоторые решили предпринять шаги для устранения этих рисков: 53% организаций планируют увеличить свои расходы на кибербезопасность к 2023 году. Согласно исследованию, проведенному Verizon DBIR, в 2022 году количество атак на цепочки поставок резко увеличилось. сложным из-за взаимосвязанного характера глобальных сред. В результате 90% руководителей цепочек поставок

заявили о планах по регионализации, чтобы снизить эти потенциальные риски для третьих сторон.

Несмотря на инициативы по обеспечению безопасности систем, атаки на цепочки поставок не показывают признаков снижения, учитывая тенденции последних лет. Таким образом, специалисты считают, что количество и изощренность кибератак на цепочки поставок будет расти.

#3 Продолжается переход от «предотвращения» к «обнаружению и реагированию».

Продолжающаяся с 2021 года тенденция смещения акцента в области кибербезопасности с предотвращения на обнаружение и реагирование сохранялась в полном разгаре в течение 2022 года. Организации все больше осознавали необходимость упреждающего и эффективного поиска угроз, реагирования на инциденты, защиты конфиденциальности данных и более продвинутых возможностей аналитики безопасности. Появление новых субъектов угроз, особенно тех, кто использует тактику искусственного интеллекта (ИИ), держало организации в напряжении, поскольку злоумышленники воспользовались уязвимостями, которые ранее упускались из виду или оставались незащищенными. В этом сдвиге, который продолжится до 2023 года, следует отметить распространение следующих событий:

Системы управляемого обнаружения и реагирования (MDR): в 2022 г. системы управляемого обнаружения и реагирования (MDR) быстро росли и внедрялись на рынке кибербезопасности. Это в значительной степени связано с увеличением как сложности угроз кибербезопасности, так и числа субъектов угроз, нацеленных на организации. Способность решений MDR быстро обнаруживать такие угрозы и реагировать на них становится все более привлекательной, поскольку организации стремятся сократить время обнаружения и, таким образом, смягчить воздействие этих событий. В использовании MDR также наблюдался сдвиг от ограничения более крупными организациями с обширными ресурсами к организациям всех размеров, полагающимся на него, благодаря его доступности, масштабируемости и гибкости. По мере того, как вводится все больше правил конфиденциальности данных, все больше внимания уделяется защите данных и соответствию требованиям, включая необходимость обнаружения и быстрого реагирования на любые потенциальные инциденты безопасности. Это ускорило спрос на решения MDR в 2022 году.

Антивирусы следующего поколения (NGAV): в 2022 году антивирусы нового поколения (NGAV) стали занимать центральное место в кибербезопасности из-за растущей сложности субъектов угроз и появления бесфайловых атак. Таким образом, организации поняли, что устаревшие антивирусы больше не способны предотвращать кибератаки, поскольку злоумышленники нашли способы обойти эту защиту. Для борьбы с этим стал необходим NGAV, поскольку он обеспечивает упреждающую, а не реактивную защиту как от известных, так и от неизвестных угроз. NGAV основан на облаке, а это означает, что развертывание может быть выполнено в течение нескольких часов, а не месяцев, без необходимости в дополнительном оборудовании или программном обеспечении. Также снимается бремя обслуживания программного обеспечения, управления инфраструктурой и

обновления баз данных сигнатур. Кроме того, теперь клиенты могут устанавливать до 70 000 агентов за один день.

Аналитика угроз. Аналитика угроз — это использование данных, аналитики и идей для выявления, оценки и реагирования на киберугрозы. Это упреждающий подход к кибербезопасности, который позволяет организациям опережать быстро меняющийся ландшафт угроз. В 2022 году мировой рынок Threat Intelligence оценивался в 7,3 миллиарда долларов США и, по прогнозам, достигнет пересмотренного размера в 20,6 миллиарда долларов США к 2027 году, увеличившись в среднем на 16% за период 2020–2027 годов. Этот быстрый рост можно объяснить изменениями в законах и правилах о конфиденциальности данных, повышенным вниманием организаций по всему миру к безопасности данных и появлением новых сложных субъектов угроз, действующих в глобальном масштабе. Правоохранительные органы теперь также используют информацию об угрозах в режиме реального времени для активной борьбы с торговлей людьми.

Глядя в горизонт: тенденции, которые определят 2023 год

№1 Переход к гибридным или полностью облачным средам ускорится.

Переход к гибридным или полностью облачным инфраструктурам — это устойчивая тенденция, о которой следует помнить организациям при инвестировании в защиту данных. Компании среднего размера, в частности, обращаются к партнерам по безопасности, которые предлагают широкий спектр услуг, а не полагаются на точечные решения и нишевых поставщиков. По мере того, как инфраструктура перемещается в облако, локальное пространство уменьшается, что может привести к снижению уязвимости системы безопасности; однако это также увеличивает уязвимость к облачным технологиям и методам, которые требуют специальных навыков и стратегий для эффективного внедрения. Организации должны помнить об этих изменениях и обеспечивать наличие надежных тенденций в области кибербезопасности, субъектов угроз и мер по обеспечению конфиденциальности данных, поскольку они продолжают переход к гибридным или полностью облачным средам. Крайне важно быть в курсе последних тенденций и угроз в области кибербезопасности, чтобы защитить конфиденциальные данные и конфиденциальную информацию.

Организации должны уделять первоочередное внимание конфиденциальности данных при переходе к облачной инфраструктуре, поскольку это имеет решающее значение для постоянного соответствия требованиям, надежности и удовлетворенности клиентов. Применяя упреждающий подход к кибербезопасности, организации могут обеспечить успешный и безопасный дальнейший переход к гибридным или полностью облачным средам.

2 Экономика разработки внутренней службы кибербезопасности будет продолжать меняться.

Экономика разработки внутренней функции кибербезопасности была серьезной проблемой для многих предприятий в течение последних нескольких лет. В 2022 году ситуация ничем не отличалась: стоимость киберзащиты по-прежнему в значительной степени перевешивала стоимость атаки.

Поскольку правила конфиденциальности данных становятся все более жесткими, а кибератаки — все более изощренными, вполне вероятно, что

внутренние функции кибербезопасности будут по-прежнему обходиться многим компаниям дорого. Чтобы свести к минимуму расходы, некоторые организации могут рассмотреть возможность передачи части или всех своих операций по кибербезопасности на аутсорсинг сторонним поставщикам. В то же время существует риск того, что эти поставщики могут быть не такими безопасными и надежными, как внутренняя команда.

Организации, стремящиеся построить собственную защиту от киберугроз, также должны взвесить ценность инвестиций в новые технологии, такие как искусственный интеллект (ИИ) и машинное обучение (МО). Благодаря автоматизации и расширенной аналитике команды могут быстро выявлять злоумышленников и защищаться от атак более эффективно, чем когда-либо прежде. Однако стоимость внедрения новых инструментов может быть высокой, особенно для небольших предприятий с ограниченными ресурсами.

Поскольку такие тенденции, как AI, ML и регулирование конфиденциальности данных, продолжают формировать ландшафт кибербезопасности в 2023 году, компании, заботящиеся о бюджете, должны помнить о компромиссах, на которые они идут, решая инвестировать в кибербезопасность. Правильный баланс между стоимостью и безопасностью имеет важное значение для организаций, стремящихся обеспечить безопасное будущее.

3 Инструменты автоматизации на основе искусственного интеллекта станут более эффективными, но для их использования потребуется больше опыта.

По мере того, как изощренность киберугроз продолжает расти, растет и спрос на более совершенные решения в области кибербезопасности. Искусственный интеллект (ИИ) и инструменты автоматизации стали важной частью ландшафта кибербезопасности в 2022 году. Инструменты автоматизации на основе ИИ становятся все более эффективными для смягчения угроз безопасности и могут выявлять потенциальные угрозы до того, как они станут проблемой. Однако для использования этих автоматизированных решений требуется больший опыт, чем когда-либо прежде.

Хотя организациям рекомендуется адаптироваться, чтобы опережать своих противников, используя инструменты на основе ИИ, они также должны осознавать эту новую потребность в более опытных и специально обученных специалистах; организациям нужен доступ к кадровому резерву опытных аналитиков, которые понимают, как и когда эффективно использовать эти инструменты. Например, новые технологии, такие как машинное обучение, могут автоматизировать процесс выявления злоумышленников, но аналитики по-прежнему должны иметь возможность точно интерпретировать данные и понимать, когда атака неизбежна. Автоматизированные инструменты на основе передового ИИ стали более мощными, чем когда-либо, но по-прежнему требуют постоянного управления и обслуживания, чтобы оставаться эффективными. По мере того, как рынок свыкается с этой реальностью, также вероятно, что появятся возможности для гибких поставщиков управляемых услуг.

Следовательно, в 2023 году будет расти спрос на специалистов по кибербезопасности, имеющих опыт использования инструментов автоматизации на основе ИИ, поскольку организации стремятся опередить своих противников.

Вполне вероятно, что эта тенденция сохранится в течение следующего года и далее.

4 Регулирование и контроль со стороны регулирующих органов будут продолжать усиливаться.

Регулирование и контроль со стороны регулирующих органов приобретают все большее значение в индустрии кибербезопасности из-за распространенности киберугроз. Это привело к расширению законодательства, предназначенного для защиты компаний и частных лиц от кибератак, защиты их данных и конфиденциальности. Регуляторный надзор в отрасли будет усиливаться по мере того, как организации все больше осознают необходимость безопасных методов работы с особо конфиденциальной информацией. Теперь компании должны внедрять строгие меры безопасности, такие как методы шифрования и многоуровневый контроль доступа, иначе в случае нарушения безопасности им придется столкнуться со значительными финансовыми и репутационными санкциями. В будущем организации должны стремиться быть в курсе текущих правил, инвестировать в технологии, которые могут помочь соответствовать требованиям соответствия, и применять упреждающий подход к кибербезопасности, делая все возможное для защиты информации своих клиентов от злоумышленников…» ***(Ander Ugalde and Hunter Voegele. Cybersecurity: Trends and Moments that Defined 2022 & Predictions for 2023 // Ankura Consulting Group, LLC. (https://angle.ankura.com/post/102i7dr/cybersecurity-trends-and-moments-that-defined-2022-predictions-for-2023). 09.02.2023).***

***

«…Согласно отчету Deloitte Opens a new window, доля ранее невиданных кибератак выросла с 20% до пандемии до более чем 35% после COVID-19. Заметно возросло количество изощренных форм фишинга и атак на основе машинного обучения.

Из-за высокой зависимости людей и организаций от киберинфраструктуры и воздействия на материальные активы убытки страховых компаний могут стать чрезвычайно большими, и страховые компании не смогут их компенсировать. Следовательно, страховые компании теперь требуют положений, исключающих ответственность за убытки, понесенные в результате нападений на государство.

Кибербезопасность стала тесно связана с геополитикой

В последние месяцы организации по всей Украине стали жертвами фишинга, DDoS-атак, дезинформации и киберфизических атак. Воздействие кибератак известно тем, что они легко выходят за пределы географических границ.

Кроме того, другие организации в Европе также подверглись атакам со стороны злоумышленников, базирующихся в Китае после начала вторжения. Проблема усугубляется участием негосударственных игроков, таких как группы хактивистов.

Кибератаки с участием национальных государств, скорее всего, будут продолжаться в обозримом будущем, с многочисленными потенциальными физическими горячими точками между странами. Напряженность обстановки,

напоминающей войну, негативно влияет на ситуационную осведомленность компаний и усугубляет панику в глобальном масштабе.

Проблемы исключения атак национального государства

Хотя уклонение от покрытия атак национального государства может показаться очевидным решением для андеррайтеров, этот подход не обходится без проблем.

Страховым компаниям сложно надлежащим образом доказать, что кибератака является атакой государства. Большинство участников масштабных событий стараются скрыть свои следы и происхождение. Следовательно, трудно понять, мотивирована ли кибератака государственными или частными мотивами.

Кроме того, настоящие атаки на национальные государства осуществляются сторонними субъектами, а не реальными государственными органами. Эти третьи стороны часто осуществляют свои собственные частные атаки. Таким образом, для страховой компании всегда будет сложно установить, была ли атака подкреплена мотивами национального государства. Бремя доказывания в таких случаях часто ложится на страховщиков, что является немалым подарком для компаний, стремящихся получить страховое покрытие.

Суды и правоохранительные органы будут играть решающую роль

Хотя это и не является обязательным, но основным решающим фактором в том, что кибератаку приписывают национальным государствам, являются расследования, проводимые правительственными разведывательными службами и службами безопасности. Таким образом, такие органы, как Федеральное бюро расследований, скорее всего, обратятся за заявлениями о нападениях на национальные государства, которые в дальнейшем должны быть доказаны в судах, что позволит страховщикам отказать в покрытии таких атак.

В тех случаях, когда правоохранительные органы и суды не могут предоставить убедительных доказательств, бремя доказывания, скорее всего, ляжет на страховщика, располагающего ресурсами для отказа в покрытии.

Однако, несмотря на все это, быстро растущее число атак на уровне государства поднимает вопросы о целесообразности приобретения полисов киберстрахования, если не покрывается все более распространенная проблема безопасности.

Раннее обнаружение и оперативная разведка могут решить проблему

По мере увеличения числа кибератак будет увеличиваться и количество компаний, обращающихся за страховкой. Количество полисов киберстрахования увеличилось на 90% в период с 2016 по 2020 год.

Однако теперь компаниям потребуются подробные стратегии кибербезопасности, чтобы претендовать на страхование. Получение дешевой страховки с минимальной инфраструктурой безопасности, скорее всего, уйдет в прошлое. Общая стоимость страховых полисов выросла на 60% за последние годы.

Рост Интернета вещей не создает новых угроз, когда ожидается, что атаки смогут перемещаться между подключенными устройствами, используя обширный обмен данными и возможности подключения. Традиционные инструменты безопасности, такие как индивидуальные пароли, также, вероятно, потеряют

популярность в ближайшем будущем. Биометрия, EDR и MFA — вот некоторые технологии, которые вместо этого будут набирать обороты.

В будущем атаки национальных государств смогут затронуть самые разные цели, помимо бизнеса, включая энергетическую инфраструктуру и автоматизированные электромобили. Ожидается, что в связи с крупномасштабными последствиями атак со стороны государства превентивные меры будут приобретать ценность во всех отраслях. Это может включать использование поведенческой аналитики для обнаружения аномальных действий в системе или сети, включая потенциальную кражу учетных данных. Такие шаги позволят службе безопасности организации предпринять быстрые шаги, чтобы помешать будущим действиям злоумышленников.

Использование такой информации в режиме реального времени в нескольких организациях может даже помочь правительствам принять своевременные меры против атак со стороны государства, защищая критически важную инфраструктуру, многие из которых принадлежат и контролируются частным сектором страны. Такой подход изменит инфраструктуру безопасности с реактивной на проактивную». ***(Anuj Mudaliar. Will Cyber Insurance Cover Nation-State Attacks in 2023? // Spiceworks Inc. (https://www.spiceworks.com/it-security/cyber-risk-management/articles/insurance-nation-state-attacks/)ю 15.02.2023).***

***

«С самого начала промышленной революции владельцы бизнеса и операторы должны были управлять бизнес-рисками, а также рисками для здоровья и безопасности своих работников и их сообществ. На протяжении веков это была ручная задача по защите в первую очередь физических помещений и процессов. С приходом информационной революции правила игры и ставки изменились. Сегодняшняя цифровая среда создает новый спектр рисков и ответственности в обеспечении физической безопасности.

Интеграция информационных технологий (ИТ) с операционными технологиями (ОТ) означает, что системы и процессы, которые когда-то были логически изолированы, теперь подвергаются тем же киберугрозам, что и мир ИТ. Предприятия больше не являются автономными операциями; они являются компонентами критически важных инфраструктур и цепочек поставок, что значительно увеличивает их подверженность рискам.

Необходимость интеграции ОТ и ИТ-безопасности для управления рисками очевидна, но ОТ и ИТ-безопасность разрабатывались отдельно, создавая рискованные и дорогостоящие хранилища безопасности.

Несмотря на необходимость скоординированной безопасности, менее половины компаний, включенных в исследование Ponemon, заявили, что их процедуры и политики кибербезопасности в области ИТ и ОТ согласованы. Основными причинами этого разрыва являются культурные различия между ИТ- и ОТ-командами, а также технические различия между их соответствующими передовыми практиками и тем, что возможно в ОТ-средах — короче говоря, культурный разрыв.

ОТ включает в себя системы, которые контролируют и управляют физическими активами и процессами. Предприятия полагаются на эти критически важные системы во всем: от управления производственными линиями и распределительными сетями до эксплуатации систем отопления, вентиляции и кондиционирования воздуха. Первоначально спроектированные и спроектированные как проприетарные автономные системы, теперь они часто используют готовое оборудование с IP-адресацией, связанное с традиционными ИТ-системами. Та же самая технология, которая позволяет администраторам удаленно управлять системами ОТ, также позволяет злоумышленникам их скомпрометировать.

Системы ИТ и ОТ развивались с разными миссиями. ИТ стали стандартизированным и интероперабельным средством обеспечения бизнеса. Системы ОТ исторически были изолированы и построены с использованием проприетарных протоколов и оборудования. Первоначально практически не предпринималось усилий для их интеграции, а логическая изоляция систем ОТ обеспечивала определенный уровень безопасности. Системы, которые не были доступны через Интернет, не были открыты для удаленных угроз. Однако растущая взаимосвязь систем ОТ и ИТ стирает эти различия. Теперь даже к системам ОТ, не имеющим прямого подключения к Интернету, часто можно получить косвенный доступ через бизнес-сети организации, подвергая ОТ новым угрозам.

Несмотря на их растущие связи, сохраняются критические различия в том, как управляются эти два типа технологий. Поскольку ОТ работает с физическими операциями, основная цель ОТ состоит в том, чтобы продолжать работать. Однако, поскольку ОТ-угрозы могут представлять значительный риск для бизнес-операций, а также для здоровья и безопасности людей, обеспечение бесперебойной работы любой ценой не является достижимой целью в сетевой среде.

Требования физической безопасности при эксплуатации и управлении ОТ иногда противоречат традиционным процессам кибербезопасности. В отличие от ИТ-систем, которые часто обновляются с точки зрения функциональности и безопасности, в ОТ изменения рассматриваются как враги. Системы ОТ, которые сейчас используют то же аппаратное и программное обеспечение, что и ИТ-системы, обычно не находятся под контролем ИТ-администраторов и не подчиняются их протоколам безопасности. Это означает, что системы ОТ не заменяются и не обновляются регулярно.

Отношение к киберриску как к бизнес-риску

Кибербезопасность — это общая ответственность ОТ и ИТ, и устранение бизнес-рисков, связанных с угрозами кибербезопасности, требует преодоления культурных и операционных различий между ними. В этой общей модели безопасности каждая сторона использует весь спектр доступных ресурсов. ИТ-специалисты традиционно оттачивали навыки кибербезопасности, в то время как ОТ занимается проектированием и физическими системами. Эффективное управление рисками требует от ОТ развития навыков кибербезопасности, а от ИТ — лучшего понимания потребностей ОТ. Директор по информационной безопасности должен обеспечить обучение, инструменты и поддержку как ОТ- так и ИТ-команд, чтобы они могли сотрудничать в борьбе с киберугрозами и вызовами.

Возможность травм, гибели людей и интеллектуальной собственности, а также сбоев в работе необходимо контролировать для защиты основного бизнеса организации. Это требует согласования групп и руководителей по безопасности ИТ и ОТ, чтобы обеспечить связь и укрепить отношения.

Организации должны иметь четкое представление о промышленных активах, чтобы принимать обоснованные решения о безопасности; разработать и задокументировать план реагирования на инциденты и постоянно оценивать его эффективность; и узнайте, как эффективно снижать риски, сокращать время простоя и распределять ресурсы кибербезопасности.

Зрелость вашего бизнеса

Первым шагом в эффективном бизнес-риске является оценка текущего состояния вашей программы. Организации безопасности ОТ должны задать себе следующие вопросы при рассмотрении управления рисками.

• Какие сценарии риска ОТ наиболее важны для ваших операций, безопасности и других критериев воздействия риска? Соответствует ли ваш план реагирования на инциденты этим сценариям?

• Есть ли у вас защищенная архитектура, основанная на этих сценариях?

• Можете ли вы обнаружить поведение, связанное с этими сценариями риска?

• Есть ли у вас надежные средства управления удаленным доступом для смягчения этих сценариев риска?

• Устранены ли ключевые уязвимости в ваших сетях ОТ, связанные с этими сценариями?

Как только организация поймет, на каком этапе процесса управления рисками она находится, она сможет начать использовать доступные профессиональные услуги для защиты всех областей бизнеса». ***(Jason Christopher. Industrial Cyber Risk Management: Integrating IT And OT Security To Fully Address Business Risk // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/02/13/industrial-cyber-risk-management-integrating-it-and-ot-security-to-fully-address-business-risk/?sh=e110ad935691). 13.02.2023).***

***

Сполучені Штати Америки

«В четвертой части рекомендаций по кибербезопасности Консультативного комитета по телекоммуникациям национальной безопасности выдвигаются более общие требования для укрепления национальной системы кибербезопасности.

Последовательные стандарты кибербезопасности и действия президента — это две из нескольких рекомендаций, опубликованных сегодня Консультативным комитетом Белого дома по национальной безопасности по телекоммуникациям в рабочем проекте документа, направленного на усиление кибербезопасности индустрии связи США перед лицом усиливающихся цифровых атак.

Как впервые сообщило Washington Post, NSTAC разработал серию проектов рекомендаций по запросу исполнительной власти еще в мае 2021 года, чтобы помочь создать более прочную национальную основу для обеспечения готовности к кибербезопасности. В этом последнем отчете основное внимание уделяется ключевым выводам, сделанным в первых трех отчетах, и освещаются проблемы, с которыми сталкиваются организации при адаптации к ужесточающимся федеральным нормам в области кибербезопасности.

Основной темой итогового отчета NSTAC является единообразие стандартов кибербезопасности и требований к критически важным инфраструктурным технологиям.

«Стандарты ИКТ [информационно-коммуникационных технологий] для требований безопасности и подходов к обеспечению, разработанные совместно с промышленностью, регулирующими органами и другими экспертами, сотрудничающими в разных секторах и регионах, отражают лучшие мировые практики», — говорится в отчете. «Приведение в соответствие с согласованными стандартами устранит конфликты, упростит и согласует разработанные на региональном уровне решения по обеспечению соответствия, чтобы действия по обеспечению безопасности можно было эффективно выполнить один раз и повторно использовать во всем мире».

Отраслевые нормативные акты, различные общие виды использования и ограничения ресурсов являются основными проблемами при установлении универсальных требований безопасности для систем ИКТ.

«Эти требования часто приводят к тому, что организациям все чаще приходится доказывать, что они выполняют свои требования к кибербезопасности с помощью различных программ обеспечения или сертификации, но эти программы часто расходятся по секторам или странам, что приводит к дополнительным затратам без повышения безопасности», — говорится в отчете. состояния.

Основные рекомендации по борьбе с разнообразием стандартов кибербезопасности включают в себя более заметные и решительные действия по продвижению требований Белого дома в области кибербезопасности, а также сотрудничество между промышленностью и правительством. Коммуникация между правительственными агентствами также была указана как область, в которой консенсус по требованиям кибербезопасности может пошатнуться.

Чтобы помочь в борьбе с этими нормативными несоответствиями, NSTAC рекомендовал создать новое правительственное учреждение в рамках CISA, получившее название Управление по гармонизации регулирования кибербезопасности, основной функцией которого будет накопление опыта в области регулирования кибербезопасности и содействие единообразию регулирования в разработке и принятии стандартов.

«Для CISA существует возможность создать и предоставить ресурсы офису, основной задачей которого является продвижение гармонизации нормативных требований в области кибербезопасности, и поручить ему изучение существующих нормативных актов и разработку ресурсов, которые могли бы определить, как создавать согласованные нормативные акты», — отмечается в отчете.

Консультативный комитет также отметил важность сохранения постквантовой криптографии в качестве приоритетной области требований кибербезопасности.

«Президент должен поручить CISA и NIST сформировать крупномасштабное партнерство с участием частного сектора, государственного сектора и академических кругов, сосредоточив внимание на переходе к постквантовой криптографии… с целью ускорения принятия и развертывания PQC», — говорится в отчете. Он также пояснил, что постквантовые криптографические стандарты должны быть основаны на процессе разработки криптографических стандартов и руководств NIST, и конкретно назвал Министерство торговли и Министерство внутренней безопасности двумя агентствами, которым следует поручить создание стимулов для массового внедрения квантовых технологий. - устойчивая криптография.

Укрепление национальной системы кибербезопасности было приоритетом для администрации Байдена, особенно на фоне натиска иностранных и внутренних кибератак, нацеленных на критически важные инфраструктурные сети в таких секторах, как энергетика и здравоохранение…

Ожидается также, что Белый дом опубликует новую Национальную киберстратегию в связи с эскалацией кибератак и угроз со стороны новых технологий». ***(Alexandra Kelley. White House Committee Advocates Collaboration, Consensus in Cybersecurity Standards // Nextgov (https://www.nextgov.com/cybersecurity/2023/02/white-house-committee-advocates-collaboration-consensus-cybersecurity-standards/383209/). 22.02.2023).***

***

«…Директор по информационным технологиям министерства обороны Джон Шерман выпустил Руководство Министерства обороны США 8140.03, Программу квалификации и управления персоналом в киберпространстве — третий выпуск этой серии политик, который последний раз обновлялся в декабре 2021 года, — чтобы обеспечить более целенаправленный и гибкий подход к жизненному циклу персонала в киберпространстве.

В частности, программа Министерства обороны США по квалификации и управлению персоналом в киберпространстве устанавливает ряд базовых требований по ролям и уровням квалификации «для повышения готовности Министерства обороны к выполнению миссий в киберпространстве». В руководстве отмечено, что стандарты и требования должны использоваться совместно с квалификационными стандартами Управления кадров. Кроме того, будет принято все обучение, соответствующее требованиям DOD Cyberspace Operations Forces.

Кроме того, программа направлена на развитие рабочей силы киберпространства «с общим пониманием концепций, принципов и приложений функций киберпространства для улучшения взаимодействия между организациями и наборами задач», говорится в плане.

Руководство 8140 заменяет Руководство Министерства обороны США 8570 «Программа повышения квалификации персонала по обеспечению безопасности

информации» (последнее обновление в 2015 г.), в котором основное внимание уделялось квалификации части персонала по кибербезопасности в области обеспечения безопасности информации и специалистов по защите компьютерных сетей. Предыдущая итерация плана — 8140.02 — детализировала рабочие роли и описала структуру рабочей силы в киберпространстве Министерства обороны США. Согласно объявлению, новое руководство 8140.03 предоставит широкий набор опций для компонентов DOD для управления и обеспечения квалифицированной рабочей силы в области ИТ, кибербезопасности, кибер-эффектов, кибер-разведки и кибер-активаторов.

Во время выступления в Сенатском комитете по вооруженным силам в апреле 2021 года Шерман отметил, что серия политик в большей степени ориентирована на навыки и профессиональное развитие…

Согласно плану, знания, навыки и способности в области кибербезопасности будут включены в квалификационные требования для каждой роли в области кибербезопасности. Программа имеет три квалификационные области…

Квалификация на рабочем месте, а также требования к образованию, обучению, сертификации или опыту работы также должны быть выполнены. Однако опыт может служить альтернативой базовым направлениям образования, обучения и аттестации персонала. Кроме того, требования к непрерывному профессиональному развитию начинаются после выполнения базовых и жилых квалификационных требований.

Кроме того, в обновленном плане также излагаются требования к управлению информацией о персонале в киберпространстве.

Обновленный план появился, когда агентство собирается опубликовать свою новую стратегию кибер-кадровых ресурсов, чтобы направлять общие усилия по укомплектованию персоналом и найму в ближайшем будущем». ***(Kirsten Errick. DOD Unveils Updates to its Cyber Workforce Job Qualifications // Nextgov (https://www.nextgov.com/cybersecurity/2023/02/dod-unveils-updates-its-cyber-workforce-job-qualifications/383052/). 16.02.2023).***

***

«В преддверии долгожданного выпуска первой Национальной стратегии кибербезопасности, которая должна быть выпущена офисом Национального директора по кибербезопасности Белого дома, Дилан Пресман, директор офиса по бюджету и оценке, подтвердил, что структура будет включать руководство по постквантовой криптография.

Обсуждая планы Белого дома по защите классических цифровых сетей от появления мощных алгоритмов квантовых вычислений, Пресман сказал, что готовящаяся Национальная киберструктура «займет твердую позицию в отношении квантов, особенно в отношении перехода к постквантовой криптографии».

Квантовые компьютеры, которые используют принципы квантовой физики для быстрой и точной обработки больших объемов данных, скорее всего, откроют новую эру кибербезопасности, поскольку обработка информации классическими компьютерами и безопасность данных будут отставать по сравнению с ними.

«Это будет иметь удивительные трансформационные качества для нашего общества и удивительные возможности, но нам также необходимо предпринять эти шаги, чтобы обезопасить себя от противников», — сказал он.

Пресман рассказал об этой функции разрабатываемой киберинфраструктуры во время обсуждения в Центре передовых технологий академического исследования. Он объяснил, что, поскольку технологии, основанные на принципах квантовой физики, а именно квантовые вычисления и квантовое зондирование, в ближайшие годы будут расширяться, и правительству, и промышленности необходимо защищать свои конфиденциальные данные уже сейчас…» ***(Alexandra Kelley. Pending National Cyber Strategy to Feature 'Strong Stand' on Quantum Cryptography // Nextgov (https://www.nextgov.com/cybersecurity/2023/02/pending-national-cyber-strategy-feature-strong-stand-quantum-cryptography/383010/). 15.02.2023).***

***

«Растущая геополитическая напряженность, уязвимости в критически важной инфраструктуре и набор необходимых правил — вот некоторые из факторов, способствующих множеству угроз кибербезопасности, с которыми столкнется государственный и частный секторы в новом году, заявила группа экспертов во время мероприятия, организованного двухпартийной политикой. Центр в понедельник.

Панельная дискуссия была проведена в ознаменование публикации нового отчета базирующегося в Вашингтоне аналитического центра, в котором были рассмотрены некоторые из основных рисков кибербезопасности, с которыми столкнутся отдельные лица, компании и правительство в 2023 году. В отчете определены восемь «макрорисков», которые могут представлять собой самые большие угрозы в киберпространстве в этом году, в том числе: развивающаяся геополитическая среда; глобальная гонка кибервооружений; уязвимая критическая инфраструктура; отсутствие необходимых инвестиций в киберподготовку; регуляторная неопределенность; нехватка кибер-талантов; недостаточное корпоративное управление; и экономическая неопределенность.

Доклад был составлен рабочей группой, состоящей из государственных чиновников, бывших федеральных чиновников и законодателей, а также представителей компаний и правозащитных групп. Агентство кредитной информации Equifax, которое в 2017 году столкнулось с собственной громкой утечкой данных, сотрудничало с Двухпартийным политическим центром для подготовки отчета.

Джамиль Фарщи, исполнительный вице-президент и директор по информационной безопасности в Equifax, сказал, что «примерно 85% вещей, которые включены в [отчет], не являются чем-то новым» — например, постоянные риски для критически важной инфраструктуры и отстающие проблемы управления, — но добавил, что невозможность исправить эти проблемы остается постоянным источником беспокойства для государственного и частного секторов…

Некоторые из этих существующих рисков еще больше усугубились усилением геополитической напряженности, которая проявилась в форме

спонсируемых государством программ-вымогателей и кибератак на критически важные службы инфраструктуры, а также онлайн-кампаний по дезинформации и дезинформации.

«Хотя эти конфликты могут быть локальными, киберугрозы могут иметь далеко идущие последствия, учитывая глобальный характер Интернета», — говорится в отчете. «Интернет и другие технологии позволили актерам выполнять эти действия удаленно и почти мгновенно».

Кристофер Пейнтер, занимавший должность координатора Госдепартамента по вопросам кибербезопасности в администрациях Обамы и Трампа, назвал обострение напряженности в отношениях США с Китаем и вторжение России в Украину одними из глобальных факторов, потенциально усугубляющих системные киберриски. Но он добавил, что растущая осведомленность о потенциальных субъектах угроз в сочетании с увеличением числа громких кибер-инцидентов также помогает подчеркнуть важность усиленных мер кибербезопасности…

Хотя в отчете говорится, что ключевые факторы риска, такие как уязвимые операционные системы, устаревший код и нехватка обученных специалистов по кибербезопасности, остаются серьезной проблемой в течение 2023 года, в нем также отмечается, что «совпадающие, противоречивые и субъективные правила» создают свои собственные проблемы, связанные с кибербезопасностью. В отчете упоминается принятие универсальных правил кибербезопасности и «балканизация законов о конфиденциальности данных и раскрытии информации о нарушениях» в качестве некоторых проблем, затрагивающих государственный и частный секторы.

Участники дискуссии заявили, что прогресс на некоторых смежных направлениях, таких как возобновление интереса Конгресса к принятию федеральной системы конфиденциальности данных, также поможет снять некоторые опасения по поводу нечеткой картины киберполитики…» ***(Edward Graham. Report Reveals How US Has 'Not Advanced the Ball' on Top Cyber Risks // Nextgov (https://www.nextgov.com/cybersecurity/2023/02/report-reveals-how-us-has-not-advanced-ball-top-cyber-risks/382906/). 13.02.2023).***

***

«Ни одно агентство еще не требовало SBOM в какой-либо серьезной форме.

Мы впервые услышали о термине SBOM, или спецификации программного обеспечения, еще в мае 2021 года, когда президент Джо Байден издал распоряжение, которое в конечном итоге потребует от поставщиков программного обеспечения, работающих с федеральным правительством, поставлять SBOM вместе со всем своим программным обеспечением. продукты. С тех пор Министерство торговли помогло определить, что необходимо включить в SBOM. И агентства, которым была предоставлена решать, когда и как начать требовать их, начали исследовать, как они будут работать.

Идея создания SBOM интересна, но за последние два года, с тех пор как они были введены в действие указом, ни одно ведомство не потребовало от них каких-либо существенных требований. Многие поставщики относятся к этой идее прохладно, и также, похоже, отсутствует понимание того, зачем они нужны, как их

создавать и что на самом деле может сделать SBOM для защиты цепочки поставок программного обеспечения.

Несколько сбивающие с толку факторы, связанные с SBOM, послужили идеальным фоном для видеовебинара, который недавно меня попросили модерировать на эту тему. Вебинар был организован FedInsider, и в нем приняли участие некоторые ведущие эксперты в этой области, работающие в промышленности и правительстве, в том числе те, кто активно разрабатывает стандарты SBOM или пытается внедрить их в своих агентствах. За время работы с этими экспертами я многому научился и хотел поделиться некоторыми из этих знаний, чтобы попытаться развеять большую часть продолжающейся путаницы в отношении того, что в конечном итоге может стать очень полезным инструментом, который правительство может использовать для защиты своей цепочки поставок программного обеспечения.

…По словам Боба Мартина, старшего главного инженера по обеспечению качества программного обеспечения и цепочек поставок в MITRE, за последние два десятилетия характер создания программного обеспечения изменился до такой степени, что требуется что-то вроде SBOM, чтобы агентство знало, что оно на самом деле получает, приобретая новое программное обеспечение.

«В прошлом у нас был образ кого-то, кто сидит буквально с чистым листом бумаги и пишет программу с нуля», — сказал он. Но сегодня «никто не пишет большую часть кода. Они используют компоненты и фреймворки других людей и собирают их вместе, чтобы выполнять большую часть работы, которую должно выполнять приложение, добавляя специфику того, что они пытаются выполнить. Сегодня это норма, потому что каждый из нас, кто делает модули, делает в основном одно и то же».

Таким образом, по словам Мартина, если агентство в прошлом получало модуль или программу от поставщика, то оно могло быть достаточно уверенным в том, что один программист или небольшая группа написали весь код, из которого они состоят. Но сегодня ведущие программисты могут заимствовать код из любого количества библиотек, фреймворков и репозиториев кода, потому что нет необходимости изобретать велосипед каждый раз при создании модуля. Вместо этого большинство основных программных функций создаются из повторно используемого предыдущего кода, и программист добавляет только последнюю часть уникальной функциональности.

Затем могут возникнуть проблемы, если позже будет обнаружена уязвимость в некоторых из тех библиотек или сред, которые составляют компонент миллионов программ и модулей, используемых правительством. Без SBOM для активных программ у агентств нет быстрого способа узнать, затронуты ли они недавно обнаруженными уязвимостями, потому что они не знают, что было в коде и программном обеспечении, которое они используют.

Хотя были написаны статьи о надлежащих компонентах SBOM, до сих пор существует много путаницы в отношении того, что они собой представляют на самом деле. Чтобы помочь в этом, Сэм Кинч, директор по управлению техническими счетами в Tanium Federal, придумал умный способ думать о них.

«Мне нравится думать о SBOM как о списке ингредиентов на упаковке с едой», — сказал Кинч во время вебинара. «С большинством упакованных продуктов вы получите список ингредиентов, которые компания использовала для создания этой еды, и точно так же вы можете думать о SBOM как о списке ингредиентов на стороне — или как части — программного пакета, который вы получать. Он предоставляет вам подробную информацию о том, какие компоненты использовались разработчиком для создания программного пакета».

Думать о SBOM как о списке ингредиентов для упакованных продуктов — отличный способ помочь визуализировать концепцию, но Кинч отмечает, что есть одно важное отличие. В отличие от упаковки макарон с сыром, которая остается неизменной до тех пор, пока кто-нибудь не сварит и не съест ее, SBOM для программного обеспечения может меняться со временем, даже после того, как программное обеспечение было доставлено в агентство.

«Если вы выполняете обновление или исправление программного обеспечения, это может изменить SBOM, потому что могут быть добавлены новые элементы», — сказал Кинч. Точно так же SBOM также может меняться в зависимости от того, на какой платформе установлено программное обеспечение или как оно используется. Из-за этого агентствам нужно не только требовать SBOM от поставщиков программного обеспечения, но и поддерживать их активность и обновлять по мере использования этого программного обеспечения в агентстве.

После создания SBOM представители федерального правительства рассказали о трех сценариях, в которых их использование было бы чрезвычайно полезным. Во-первых, их было бы неплохо иметь во время кризиса, например, когда была обнаружена уязвимость Log4j.

«Вместо того, чтобы выполнять всю эту «загрузку на месте», когда произойдет следующий Log4j, вы можете вместо этого иметь базу данных или репозиторий происхождения SBOM, к которому можно обратиться», — сказал Джейсон Маллинз, руководитель цепочки поставок из Министерства образования. «Я мог бы просто найти это и посмотреть, где я пострадал, откуда взялись мои плохие ингредиенты и куда они попали, и где эта часть программного обеспечения подключена к моим системам. Тогда я смогу начать действовать правильно».

Пэт Салливан, старший советник директора по управлению цепочками поставок в Командовании материальных средств армии, добавил, что SBOM помогут не только во время кризиса, но и для повседневного мониторинга сетей как ключевого компонента кибербезопасности.

«Это ценный инструмент, который помогает не только в момент кризиса, но и в нашей ежедневной работе по обнаружению и пресечению выявленных злонамеренных намерений», — сказал Салливан. «Интересно, что мы ведем это обсуждение сейчас, потому что совсем недавно, в октябре, наш заместитель секретаря по закупкам поделился, что армия с головой уходит в SBOM, поэтому, хотя анализ состава продолжается уже много лет, пришло время перейти к следующему шагу».

Наличие SBOM может даже повысить безопасность процесса приобретения программного обеспечения, что становится все более сложным для многих

агентств». ***(John Breeden II. How SBOMs Can Eventually Help to Secure Government's Software Supply Chain // Nextgov (https://www.nextgov.com/cybersecurity/2023/02/how-sboms-can-eventually-help-secure-governments-software-supply-chain/382835/). 10.02.2023).***

***

«Новые федеральные требования регистрировать каждый пакет данных, проходящий через сети агентства (так называемый захват пакетов или PCAP), вызвали обеспокоенность у экспертов по кибербезопасности в правительстве и за его пределами, которые говорят, что новое правило неясно, ресурсоемко и малоценно в реальных условиях. расследование нарушений.

Требования PCAP стали прямым результатом ряда нарушений, обнаруженных в конце 2020 года, в том числе инцидента SUNBURST, который вызвал общегосударственные усилия по исправлению положения и ряд новых мандатов для агентств.

К августу 2021 года Административно-бюджетное управление выпустило служебную записку «Совершенствование возможностей федерального правительства по расследованию и устранению последствий инцидентов в области кибербезопасности», в которой были указаны новые требования к агентствам по созданию и хранению определенных данных для использования в криминалистике после взлома. Эти элементы данных включали «полный захват пакетов», а также более простые журналы кибербезопасности.

За этим требованием в прошлом месяце последовало новое руководство от Национального управления архивов и документации — его первое обновление правил записей кибербезопасности с 2014 года — которое официально установило правила хранения: 30 месяцев для журналов кибербезопасности и 72 часа для данных PCAP.

Но широкий характер требования PCAP оказался запутанным для некоторых федеральных чиновников по кибербезопасности, которые поставили под сомнение ценность выполнения PCAP в современных сетях и стоимость, связанную с хранением больших наборов данных. Специфика политики — в частности, короткое 72-часовое окно — еще больше снижает ценность перехвата пакетов для криминалистических целей.

Например, один федеральный чиновник по кибербезопасности, который попросил остаться анонимным, поскольку его агентство не разрешило ему выступать публично, сказал, что служебной записки 2021 года и обновления NARA недостаточно, чтобы помочь агентствам определить свои процедуры PCAP, и, похоже, не предлагает свобода действий для тех, кто пытается создать аналогичную систему кибербезопасности без PCAP.

Роберт Грэм, консультант по кибербезопасности и эксперт по PCAP, а также известный «случайный парень в Интернете», согласился, что самая большая проблема правительственной политики PCAP — это двусмысленность.

«Я недостаточно понимаю это, чтобы судить», — сказал он Nextgo. «Одна интерпретация кажется приемлемой; другая интерпретация — дурацкая».

В ответ на просьбу о разъяснениях представитель ОМБ, говоря по бэкграунду, лишь подтвердил официальную политику правительства: «Хранение ПКП в течение 72 часов требуется для M-21-31; CISA и OMB сотрудничают с агентствами, чтобы предоставить техническую помощь по хранению журналов и управлению ими».

Представитель Агентства кибербезопасности и безопасности инфраструктуры отказался комментировать, как агентства должны выполнять это требование, и направил Nextgov обратно в NARA по поводу правил хранения записей.

Но реализация будет эффективной только в том случае, если агентства установят PCAP в правильных частях сети, сказал Грэм.

«В сети нет места, куда можно было бы подключиться и увидеть весь трафик. Сеть представляет собой своего рода ячеистую сеть — именно поэтому мы называем ее сетью — и поэтому вам нужно задействовать множество точек. В некоторых из этих точек будет много трафика — больше, чем вы хотите захватить. Другие части будут видеть только тот трафик, который вы хотите захватить», — сказал он. «Где они на самом деле означают, что эти PCAP должны происходить?»

Например, связь между основными серверами и резервным сервером, собирающим данные исключительно для избыточности, не требует захвата пакетов, поскольку эти данные PCAP были бы избыточными и дорогостоящими для хранения.

«Означает ли это, что сетевой трафик идет в Интернет? Или это означает весь сетевой трафик где угодно, в том числе между двумя серверами?» он сказал. «Два сервера могут, например, обмениваться резервными копиями, что быстро приведет к перегрузке. Я не могу представить, что они намерены делать».

Проблема усугубляется, когда агентства шифруют сетевой трафик, как это требуется в соответствии с мандатом OMB от января 2022 года «Нулевое доверие». Расследователи инцидентов кибербезопасности могут собрать некоторые данные из зашифрованного пакета, например его размер, но получить мало дополнительной информации без расшифровки пакета, что невозможно при большинстве настроек безопасности.

«Учитывая, что большая часть трафика зашифрована без возможности расшифровки, журналы потоков мало что дают. Пассивный сбор сертификатов мог бы помочь вместе с пассивным DNS, но помимо этого я не могу представить, какую пользу это принесет», — сказал Грэм.

Из-за небольшой добавленной стоимости и высоких затрат на хранение некоторые сомневаются в том, что PCAP действительно стоит того.

Грэм согласился с тем, что люди, беспокоящиеся о соблюдении требований, особенно в правительстве, могут склоняться к «дурацкой стороне», чтобы быть в безопасности, либо перебарщивать и тратить гораздо больше денег и ресурсов, чем необходимо, либо делать достаточно захвата пакетов, чтобы соответствовать небольшим требованиям. никак не влияет на состояние кибербезопасности агентства.

Даже если в данных PCAP содержится полезная информация, данные PCAP, вероятно, редко будут ценными в течение 72-часового окна.

Различные источники предлагают разные статистические данные о том, как долго в среднем нарушение остается незамеченным.

Согласно отчету IBM Cost of a Data Breach Report 2022, среднее время, затрачиваемое организацией на обнаружение утечки, составляет более 200 дней, и за последние шесть лет оно незначительно изменилось.

Данные компаний по кибербезопасности Mandiant и Sophos показывают гораздо более радужную картину: среднее время пребывания, определяемое как «количество дней, в течение которых злоумышленник находится в среде жертвы до того, как его обнаружат», составляет 24 дня и 15 дней, согласно данным в их соответствующие отчеты за 2021 год.

В отчете Sophos отмечается, что время ожидания намного выше для инцидентов, не связанных с программами-вымогателями, для которых злоумышленники обычно отправляют заметки о выкупе, информируя жертв об утечке, более чем вдвое до среднего значения 34 дней.

Хотя эти сроки намного короче, чем 200 дней, они все еще далеко за пределами 72-часового окна, предписанного OMB и NARA.

«Нарушение произошло задолго до 72 часов», — согласился Грэм. Однако он отметил, что даже если нарушение будет обнаружено в течение 72-часового окна и уникальный PCAP будет потенциально полезен, агентствам все равно будет сложно эффективно использовать данные PCAP для судебной экспертизы из-за одной из самых постоянных проблем. в федеральном управлении ИТ: наличие достаточного количества квалифицированных сотрудников в области кибербезопасности.

По словам Грэма, PCAP могут быть полезны для определения того, является ли потенциальный инцидент реальной проблемой или просто ложным срабатыванием, но «такой анализ PCAP — это особый навык, которого нет у среднего работника [центра операций по обеспечению безопасности]…». ***(Aaron Boyd. Experts Question Value of Federal Cybersecurity Data Capture Mandate // Nextgov (https://www.nextgov.com/cybersecurity/2023/02/experts-question-value-federal-cybersecurity-data-capture-mandate/382738/). 08.02.2023).***

***

«Согласно отчету, опубликованному наблюдательным органом во вторник, более половины рекомендаций Счетной палаты правительства (GAO) по защите критически важных инфраструктурных услуг от киберугроз не выполнялись с 2010 года, что может поставить под угрозу безопасность национальной энергосистемы и других жизненно важных услуг.

В отчете указано, что из 106 общедоступных рекомендаций по укреплению критически важной киберинфраструктуры, которые были выпущены агентством с 2010 года, по состоянию на декабрь 2022 года были реализованы только 46.

«Пока они не будут полностью реализованы, ключевые критически важные инфраструктуры будут по-прежнему подвергаться повышенным рискам кибербезопасности для своих систем и данных», — предупредил GAO.

В отчете говорится, что агентствам необходимо сосредоточиться на «укреплении роли федерального правительства в кибербезопасности критически важной инфраструктуры», в том числе уделять больше внимания

совершенствованию своих методов кибербезопасности с учетом меняющихся киберугроз.

GAO процитировал отчет за март 2021 года, в котором говорится, что Министерство энергетики «разработало планы по борьбе с этими угрозами и реализации национальной стратегии кибербезопасности для сети», но не «устранило уязвимости распределительных систем, связанные с цепочками поставок».

«В результате эти планы, вероятно, будут иметь ограниченное применение при определении приоритетов федеральной поддержки штатов в решении проблемы кибербезопасности распределительных сетей», — говорится в отчете.

Хотя GAO рекомендовало Energy «координировать свои действия с Министерством внутренней безопасности, штатами и отраслью для более полного устранения рисков для распределительных систем сети от кибератак» в своих планах по реализации национальной стратегии кибербезопасности, наблюдательный орган заявил, что агентство до сих пор не сделало этого. Итак, по состоянию на декабрь 2022 г.

«Распределительные системы США, которые передают электроэнергию от систем передачи к потребителям и регулируются в основном штатами, все чаще подвергаются риску кибератак», — отмечается в отчете. «Распределительные системы становятся все более уязвимыми, отчасти из-за расширения возможностей подключения промышленных систем управления. В результате злоумышленники могут использовать несколько методов для доступа к этим системам и потенциально нарушить работу».

GAO также заявило, что Агентству кибербезопасности и безопасности инфраструктуры «необходимо оценить эффективность своих программ и услуг для поддержки сектора связи», который сталкивается с целым рядом человеческих, физических и киберугроз.

GAO ранее выпустило отчет за ноябрь 2021 года, в котором предупреждалось, что CISA «не оценивала эффективность своих программ и услуг, поддерживающих безопасность и устойчивость сектора связи», и «не обновляла свой план для сектора связи на 2015 год». Хотя наблюдательный орган рекомендовал CISA «оценить эффективность своих программ и услуг для поддержки сектора связи» и подготовить пересмотренный план, к концу 2022 года агентство не выполнило ни одну из рекомендаций.

Кроме того, GAO заявило, что рост числа атак программ-вымогателей, особенно направленных на критически важные службы инфраструктуры, требует усиления межведомственной координации между Министерством внутренней безопасности и Министерством юстиции.

В отчете GAO за сентябрь 2022 года описывалось, как CISA, ФБР и Секретная служба работали вместе, чтобы «оказать помощь в предотвращении и реагировании на атаки программ-вымогателей на племенные, государственные, местные и территориальные правительственные организации», но выявил пробелы в «аспектах шести из семи». ключевые практики межведомственного сотрудничества», а также опасения респондентов по поводу «проблем, связанных с осведомленностью, информированием и коммуникацией».

Хотя в отчете DHS и Министерству юстиции рекомендовалось «решить выявленные проблемы и внедрить ключевые методы сотрудничества при предоставлении услуг правительствам племен, штатов, местных и территорий», по состоянию на декабрь 2022 года рекомендации надзорного органа оставались без внимания.

Обзор, представленный во вторник, — это третий отчет GAO из серии из четырех статей о проблемах кибербезопасности с высоким риском, которые федеральное правительство должно немедленно решить. В предыдущих двух отчетах, выпущенных GAO в своей серии, также было обнаружено, что федеральные агентства не делают достаточно, чтобы реагировать на выявленные уязвимости и операционные недостатки…» ***(Edward Graham. GAO's Critical Infrastructure Cyber Recommendations Go Largely Unaddressed // Nextgov (https://www.nextgov.com/cybersecurity/2023/02/gaos-critical-infrastructure-cyber-recommendations-go-largely-unaddressed/382733/). 08.02.2023).***

****

«…Президент Джо Байден обратился к нации во вторник вечером, приветствуя двухпартийные усилия по производству и инновациям в области технологий…

В своем втором обращении к Конгрессу Байден высоко оценил принятый в прошлом году Закон о ЧИПС и науке, который предусматривает финансирование в размере 52 миллиардов долларов для субсидирования производства полупроводников в США и дополнительные миллиарды долларов для исследований и разработок в области новых технологий. Использование таких микрочипов распространилось на предметы повседневного обихода, такие как автомобили и смартфоны, на передовые технологии…

Байден также призвал обуздать Big Tech из-за его практики конфиденциальности данных и наблюдения.

Президент выразил обеспокоенность по поводу чрезмерного сбора данных платформами и попросил двухпартийную поддержку запретить таргетированную онлайн-рекламу для детей и подростков и обеспечить надежную защиту конфиденциальности, данных, здоровья и онлайн-безопасности. Он призвал законодателей ввести более строгие ограничения на использование компаниями персональных данных.

«Мы должны, наконец, призвать социальные сети к ответу за эксперимент, который они проводят над нашими детьми с целью получения прибыли», — сказал Байден.

Замечания президента прозвучали после того, как Федеральная торговая комиссия рассмотрела более широкие методы регулирования конфиденциальности в Интернете.

В преддверии выступления группа по защите цифровых прав «Борьба за будущее» подчеркнула необходимость принятия законов о конфиденциальности, которые выходят за рамки защиты детей.

«Позволение таким компаниям, как Meta и Google, работать на полную катушку с их рекламной бизнес-моделью наблюдения, но с некоторыми

косметическими ограждениями для несовершеннолетних пользователей, на самом деле не делает мир лучше или безопаснее для наших детей». Об этом заявил режиссер «Борьбы за будущее» Эван Грир. «Лучший способ защитить наших детей в Интернете — защитить всех в Интернете. Мы должны начать с запрета вредных и хищнических методов коммерческой слежки, которые лежат в основе вреда больших технологий»…» ***(Kirsten Errick. Biden's State of the Union Highlights Semiconductor Success and Big Tech Privacy Concerns // Nextgov (https://www.nextgov.com/technology-news/2023/02/bidens-state-union-highlights-semiconductor-success-and-big-tech-privacy-concerns/382704/). 07.02.2023).***

***

«Глава Бюро киберпространства и цифровой политики Госдепартамента заявил, что более заметное внимание США к технологической политике требует более активного международного участия.

Иностранная дипломатия, сосредоточенная вокруг киберпространства и технологий, имеет решающее значение для обеспечения глобального лидерства США и противодействия враждебным странам, заявил посол Госдепартамента по вопросам кибербезопасности на мероприятии, организованном немецким фондом Маршалла в четверг.

Натаниэль Фик, посол США по особым поручениям в области киберпространства и цифровой политики, заявил, что приоритетом для правительства США должно быть «укрепление американской внешней политики в отношении технологических тем», особенно с учетом того, что эти вопросы приобретают все более ведущую роль в международных делах.

«По сути, это означает сохранение американского преимущества и преимущества единомышленников в тех областях, где у нас есть сильные технологические лидеры», — добавил он. «Это означает вернуть наши зацепки в тех местах, где мы их потеряли. И это означает закрытие путей к преимуществам для противников и конкурентов».

Фик возглавляет Государственное бюро киберпространства и цифровой политики, которое департамент запустил в апреле 2022 года в рамках усилий по «решению проблем национальной безопасности, экономических возможностей и последствий для ценностей США, связанных с киберпространством, цифровыми технологиями и цифровой политикой». Сенат единогласно утвердил Фика на посту главы киберкосмического бюро штата в сентябре.

Фик сказал, что успешные усилия по продвижению голоса США в международных организациях, связанных с технологиями, такие как избрание в сентябре прошлого года кандидата США Дорин Богдан-Мартин на пост Генерального секретаря Международного союза электросвязи Организации Объединенных Наций, а не российского оппонента, помогают обеспечить необходимый являются противовесом враждебным странам и символизируют «повторное участие Соединенных Штатов и, надеюсь, переломный момент».

«Природа не терпит пустоты, и другие заполняют пустоту, когда мы уходим, и двигают эти тела в направлениях, которые в конечном итоге в корне расходятся с

технологическим будущим, которое, я думаю, мы все хотим видеть», — добавил Фик.

Он сказал, что такой тип расширенного участия на мировой арене также влечет за собой укрепление партнерских отношений между правительством и компаниями частного сектора — усилия, которые значительно увеличились за последний год, в значительной степени из-за вторжения России в Украину. Фик сказал, что эти государственно-частные партнерства оказались особенно эффективными, когда речь идет о поддержке цели государства «гарантировать, что вторжение России в Украину приведет к стратегическому поражению России».

«Люди задавались вопросом, почему российские кибератаки кажутся неэффективными или столь же эффективными в Украине или в Европе», — сказал Фик. «Одна из причин заключается в том, что Microsoft и другие компании смогли выпускать масштабные обновления практически в режиме реального времени благодаря сотрудничеству с разведывательным сообществом США, которое позволило им отразить эти атаки. Дело не в том, что атак не было, а в том, что они были неэффективны».

В дополнение к более эффективному продвижению технологических и кибер-интересов Соединенных Штатов во всем мире и поддержке американских союзников в поддержку общих дипломатических интересов, Фик сказал, что для официальных лиц также важно взаимодействовать с неприсоединившимися или «средними странами», особенно по вопросам управления Интернетом.

«Это не должно быть все антироссийское или антикитайское, потому что в мире есть много средних государств», — сказал Фик, отметив, что США должны работать над тем, чтобы «все наши политики — в первую очередь — были утверждены, позитивные, привлекательные, убедительные термины, рассказывающие очень реальную историю о хороших вещах, которые технологии могут принести в наше будущее».

Вопросы внутренней политики, связанные с технологиями и кибербезопасностью, также стали играть более заметную роль во внешней политике. Фик сослался на статью президента Джо Байдена от 11 января в Wall Street Journal, в которой частично содержится призыв к США принять федеральные меры по защите конфиденциальности данных, и добавил, что «это укрепит нашу внешнюю политику, укрепит нашу торговую политику [и] это поможет нам создать более крупные и крепкие союзы».

По мере того, как США пытаются позиционировать себя в качестве ведущего регулирующего органа в области технологий и политики кибербезопасности — вопрос, который законодатели Конгресса назвали важным для борьбы с растущим глобальным влиянием Китая, — роль чиновников, ориентированных на цифровую политику, таких как Фик, стала более заметной. в иностранных делах.

«Одна из неудобных реалий дипломатии заключается в том, что иногда внутренняя политика вашей страны не обязательно укрепляет вашу внешнюю политику», — сказал Фик, отметив, что вопросы конфиденциальности и технологий являются постоянной «темой для обсуждения с нашими европейскими коллегами».

Союзники США, например, не согласны с некоторыми положениями, включенными в прошлогодний Закон о снижении инфляции (или IRA), который некоторые европейские официальные лица считают слишком протекционистскими, когда речь идет о предоставлении субсидий и налоговых льгот американским компаниям и производителям. И США все еще взаимодействуют с международными союзниками, чтобы прийти к соглашению об экспортном контроле, призванном ограничить доступ Китая к передовым полупроводникам и связанному с ними оборудованию.

Фик признал, что некоторые положения IRA «вызвали негативную реакцию в Европе», но сказал, что официальные лица США продолжают переговоры с европейскими коллегами, чтобы сгладить любые разногласия…» ***(Edward Graham. US Cyber Diplomat Calls for Bolstering American Advantage in Global Tech Policy // Nextgov (https://www.nextgov.com/policy/2023/02/us-cyber-diplomat-calls-bolstering-american-advantage-global-tech-policy/382526/). 02.02.2023).***

***

«Атаки, предположительно совершенные базирующимися в России противниками, произошли в августе и сентябре 2022 года и могут привести к разоблачению конфиденциальных научных исследований США.

После серии кибератак, направленных на три национальные лаборатории, находящиеся в ведении Министерства энергетики США, законодатели Палаты представителей запрашивают доступ к соответствующей документации о хакерских инцидентах, чтобы исследовать их масштабы и текущую позицию агентства в области кибербезопасности.

Атаки были осуществлены хакерской группой, известной как Cold River, которая, как отмечают законодатели, «причастна» к операциям в интересах российского правительства. Хакерская тактика, используемая Cold River, заключалась в создании ложных страниц входа в систему для трех целевых лабораторий и отправке их соответствующим ученым, у которых затем запрашивалась информация о пароле.

В письме, направленном министру энергетики Дженнифер Грэнхольм, руководство Комитета Палаты представителей по надзору и подотчетности и Комитета по науке, космосу и технологиям упомянуло три отдельные кибератаки в период с августа по сентябрь 2022 года как нацеленные на информацию, связанную с национальной безопасностью США и научной конкурентоспособностью. Сообщается, что атаки произошли в Брукхейвенской национальной лаборатории, Аргоннской национальной лаборатории и Ливерморской национальной лаборатории Лоуренса.

«Хотя неясно, были ли попытки вторжения успешными, вызывает тревогу тот факт, что враждебный иностранный противник нацелился на правительственные лаборатории, занимающиеся научными исследованиями, имеющими решающее значение для национальной безопасности и конкурентоспособности Соединенных Штатов», — говорится в письме. «Комитеты запрашивают документы и информацию, связанные с этими инцидентами, чтобы определить последствия попыток вторжений и оценить, что делает Министерство

энергетики для обеспечения постоянной безопасности конфиденциальных научных исследований и разработок в своих национальных лабораториях».

Законодатели ищут подробную информацию о сообщениях каждой лаборатории о попытках взлома в период с июля 2022 года по сегодняшний день. Это включает в себя общение между подрядчиками и субподрядчиками, поддерживающими Energy, по поводу взломов, а также с другими федеральными агентствами.

Чиновники в сфере энергетики намерены сотрудничать с законодателями Палаты представителей, а представитель агентства подтвердил Nextgov, что агентство серьезно рассматривает свою киберзащиту.

«В рамках нашей текущей проверки Министерство энергетики не обнаружило доказательств того, что информация была скомпрометирована. Министерство энергетики будет продолжать работать с нашими федеральными партнерами, чтобы реагировать на любые потенциальные угрозы и нарушения и расследовать их, обеспечивая безопасность научных исследований, проводимых в национальных лабораториях Америки», — сказал представитель.

Кибератаки происходят на фоне геополитического конфликта между Россией и США — наряду с другими странами, входящими в двустороннюю Организацию Североатлантического договора — в результате продолжающейся войны между Россией и Украиной…» ***(Alexandra Kelley. Cyberattacks on Energy's National Labs Draw Lawmaker Scrutiny // Nextgov (https://www.nextgov.com/cybersecurity/2023/02/cyberattacks-energys-national-labs-draw-lawmaker-scrutiny/382503/). 02.02.2023).***

***

«Согласно новому отчету Центра двухпартийной политики, основные риски кибербезопасности в 2023 году включают нехватку обученных кибер-специалистов, международные конфликты и сохраняющиеся уязвимости в службах критической инфраструктуры.

Растущая геополитическая напряженность, уязвимости в критически важной инфраструктуре и набор необходимых правил — вот некоторые из факторов, способствующих множеству угроз кибербезопасности, с которыми столкнется государственный и частный секторы в новом году, заявила группа экспертов во время мероприятия…

Панельная дискуссия была проведена в ознаменование публикации нового отчета базирующегося в Вашингтоне аналитического центра, в котором были рассмотрены некоторые из основных рисков кибербезопасности, с которыми столкнутся отдельные лица, компании и правительство в 2023 году. В отчете определены восемь «макрорисков», которые могут представлять собой самые большие угрозы в киберпространстве в этом году, в том числе: развивающаяся геополитическая среда; глобальная гонка кибервооружений; уязвимая критическая инфраструктура; отсутствие необходимых инвестиций в киберподготовку; регуляторная неопределенность; нехватка кибер-талантов; недостаточное корпоративное управление; и экономическая неопределенность.

Доклад был составлен рабочей группой, состоящей из государственных чиновников, бывших федеральных чиновников и законодателей, а также представителей компаний и правозащитных групп. Агентство кредитной информации Equifax, которое в 2017 году столкнулось с собственной громкой утечкой данных, сотрудничало с Двухпартийным политическим центром для подготовки отчета.

Джамиль Фарщи, исполнительный вице-президент и директор по информационной безопасности в Equifax, сказал, что «примерно 85% вещей, которые включены в [отчет], не являются чем-то новым» — например, постоянные риски для критически важной инфраструктуры и отстающие проблемы управления, — но добавил, что невозможность исправить эти проблемы остается постоянным источником беспокойства для государственного и частного секторов.

«Самое удивительное для меня то, что многие риски, которые мы здесь выделили, — это те же самые риски, которые, я думаю, могли бы быть в этом списке, если бы мы сделали это пять лет назад или, может быть, даже 10 лет назад. — сказал Фарщи. «Итак, в некотором смысле это предсказуемо, в некотором роде. Но с другой стороны, это обескураживает, потому что мы, как сообщество, как страна, недостаточно эффективно продвигаем мяч, чтобы иметь возможность смягчить или даже снизить некоторые из рисков, которые мы выделили».

Некоторые из этих существующих рисков еще больше усугубились усилением геополитической напряженности, которая проявилась в форме спонсируемых государством программ-вымогателей и кибератак на критически важные службы инфраструктуры, а также онлайн-кампаний по дезинформации и дезинформации.

«Хотя эти конфликты могут быть локальными, киберугрозы могут иметь далеко идущие последствия, учитывая глобальный характер Интернета», — говорится в отчете…

Кристофер Пейнтер, занимавший должность координатора Госдепартамента по вопросам кибербезопасности в администрациях Обамы и Трампа, назвал обострение напряженности в отношениях США с Китаем и вторжение России в Украину одними из глобальных факторов, потенциально усугубляющих системные киберриски. Но он добавил, что растущая осведомленность о потенциальных субъектах угроз в сочетании с увеличением числа громких кибер-инцидентов также помогает подчеркнуть важность усиленных мер кибербезопасности.

«Из-за пандемии программ-вымогателей, которую мы наблюдали в течение последних нескольких лет, осведомленность стала гораздо выше, чем раньше», — сказал Пейнтер. «И поэтому привлечение внимания к этим рискам, я думаю, действительно важно, и попытка каталогизировать их действительно важна».

Хотя в отчете говорится, что ключевые факторы риска, такие как уязвимые операционные системы, устаревший код и нехватка обученных специалистов по кибербезопасности, остаются серьезной проблемой в течение 2023 года, в нем также отмечается, что «совпадающие, противоречивые и субъективные правила» создают свои собственные проблемы, связанные с кибербезопасностью. В отчете упоминается принятие универсальных правил кибербезопасности и «балканизация

законов о конфиденциальности данных и раскрытии информации о нарушениях» в качестве некоторых проблем, затрагивающих государственный и частный секторы.

Участники дискуссии заявили, что прогресс на некоторых смежных направлениях, таких как возобновление интереса Конгресса к принятию федеральной системы конфиденциальности данных, также поможет снять некоторые опасения по поводу нечеткой картины киберполитики.

«Я думаю, что больше всего действий в области регулирования мы наблюдаем через призму конфиденциальности», — сказал Ноопур Дэвис, исполнительный вице-президент и главный специалист по информационной безопасности и конфиденциальности продуктов в Comcast. «Но линза конфиденциальности, конечно же, влияет на линзу безопасности. Так что внимание к конфиденциальности также смещается в киберпространство. И я думаю, что сейчас это ощущается иначе, чем пять лет назад — в 2023 году это кажется более актуальным». ***(Edward Graham. Report Reveals How US Has 'Not Advanced the Ball' on Top Cyber Risks // Nextgov (https://www.nextgov.com/cybersecurity/2023/02/report-reveals-how-us-has-not-advanced-ball-top-cyber-risks/382906/). 13.02.2023).***

***

«По данным Layoffs.fyi, с начала 2022 года увольнения в крупных технологических компаниях вызвали беспорядки для почти 250 000 рабочих в США и привели к тому, что было названо великой перестановкой рабочих мест в сфере технологий. Некоторые пострадавшие работники обратились к LinkedIn и другим доскам объявлений о вакансиях, требуя новой работы, в то время как другие поняли, что «их навыки по-прежнему пользуются спросом», как показывают недавние отчеты Fortune.

Увольнения в значительной степени коснулись работников, занимающихся управлением продуктами, разработкой продуктов, маркетингом, продажами и подбором персонала. Одна группа сотрудников, которых почти не трогали? Те, кто работает в сфере кибербезопасности.

Увольнения в сфере кибербезопасности были «нечастыми и редкими», говорит Дэн Уолш, директор по информационной безопасности в VillageMD, компании первичной медико-санитарной помощи, контрольный пакет акций которой принадлежит из списка Fortune 500 компании Walgreens Boots Alliance. VillageMD планирует IPO. Некоторые инженеры-программисты, уволенные в компании, отказались от целой функции или линейки программного обеспечения, но в сфере кибербезопасности было меньше увольнений.

В целом, технологические «увольнения ничтожны по сравнению с количеством наймов во время пандемии», — говорит Уолш. Тем не менее, кибербезопасность по-прежнему пользуется большим спросом. «Вакансий по-прежнему больше, чем людей, которые могут их заполнить».

«Есть только некоторые основные и стратегические роли в области безопасности, которые необходимо заполнить», — добавляет Уолш.

Проблемы для новых специалистов по кибербезопасности

Вместо риска увольнения есть другая проблема для работников кибербезопасности, которые являются новичками в отрасли. На фоне новостей об

увольнениях в крупных технологических компаниях Уолш в посте на LinkedIn предложил провести имитационные собеседования с работниками кибербезопасности, которые искали работу. До сих пор он в основном разговаривал с профессионалами в области кибербезопасности, которые только начинают свою карьеру или уже сменили ее…

При этом открытых вакансий в области кибербезопасности по-прежнему больше, чем заполненных, при этом, по некоторым прогнозам, в США открыто 700 000 вакансий в области кибербезопасности. их бюджет на кибербезопасность.

«Безопасность всегда нуждается в ресурсах, — говорит Уолш. «Как руководитель службы безопасности я хотел бы устранить все риски. Но деловая реальность такова, что [наем талантов] обходится чрезвычайно дорого».

С этой целью компаниям часто проще нанять более опытных специалистов, потому что «безопасность — это, по сути, дело доверия», — объясняет Уолш.

«Хочу ли я рискнуть с этим человеком, когда мои ресурсы уже ограничены?» Вопросы Уолша. «Иногда да, а иногда нет».

При этом Уолш прогнозирует, что. в конце этого года откроется больше новых вакансий в области кибербезопасности, потому что кибербезопасность вызывает серьезную озабоченность во время экономического спада Именно в эти периоды предприятия могут стать более уязвимыми для злоумышленников и кибератак.

Профессионалам, которые хотят пробиться в отрасль, Уолш предлагает начинать со смежных ролей, например, работать в ИТ-отделе, чтобы получить соответствующий опыт. Более того, люди могут проявлять инициативу, занимаясь самообучением и даже добровольно предлагая услуги кибербезопасности, чтобы показать работодателям, что они проделали свою работу.

«За последние несколько лет дипломы по безопасности стали популярными и тяжелыми, но мы все начинали с чего-то другого, — говорит Уолш. «Некоторые из нас были инженерами-программистами, некоторые из нас были аудиторами в «Большой четверке», другие начинали в службе поддержки или были системными администраторами. Это по-прежнему отличные способы попасть в систему безопасности».

Заработная плата в сфере кибербезопасности

Хотя работа в службе поддержки может быть одним из способов начать путь к работе в области кибербезопасности, она оплачивается примерно вдвое меньше, чем другие роли. Аналитики по кибербезопасности могут зарабатывать более 80 000 долларов, в то время как тот же человек, работающий в службе поддержки, может зарабатывать только около 40 000 долларов, объясняет Уолш.

«Это еще одно препятствие, с которым, я думаю, индустрии придется как-то разобраться», — говорит он. «Но если люди готовы делать это в течение определенного периода времени и получить немного больше опыта, стать ближе к действию, это лучший способ».

Штатные специалисты по кибербезопасности также находятся на пути к еще большему заработку. Когда Уолш получил свою первую должность директора по информационным технологиям в Rally Health, инженеры по безопасности зарабатывали около 120 000 долларов. сегодня те же самые инженеры сразу же

зарабатывают По словам Уолша, от 180 000 до 200 000 долларов. Это примерно на 40% больше, чем за шесть лет.

«Рынок труда по-прежнему чрезвычайно силен для специалистов по кибербезопасности, — говорит Уолш. «Я думаю, что заработная плата будет продолжать расти». ***(Sydney Lake. Amid Big Tech layoffs, cybersecurity job losses have been 'few and far between,' industry leader says // Fortune Media IP Limited (https://fortune.com/education/articles/amid-big-tech-layoffs-cybersecurity-job-losses-have-been-few-and-far-between-industry-leader-says/). 03.02.2023).***

***

«Натаниэль Фик, посол США по особым поручениям в области киберпространства и цифровой политики, заявил в четверг, что российско-украинская война побудила правительство значительно расширить партнерство с частным сектором, что было менее распространено в предыдущие годы.

Фик, который Госдепартамента в августе был утвержден главой нового кибербюро, сказал, что за последний год он стал свидетелем фундаментальных изменений в том, как правительство и частный сектор сотрудничают по вопросам кибербезопасности.

«Когда я был генеральным директором по кибербезопасности, государственно-частное партнерство было модным термином, — сказал он. «Обычно это означало, что я поделился своими данными с правительством, правительство засекретило их, и я ничего не получил взамен».

«Это категорически больше не так», — добавил он.

Фик сделал свое заявление во время мероприятия, организованного немецким фондом Маршалла, где он отвечал на вопрос о том, как российско-украинская война изменила правила игры в киберпространстве.

Фик также отметил, как государственно-частное партнерство в киберпространстве помогло Украине противостоять российским кибератакам.

«В Украине… Microsoft и другие компании смогли выпускать масштабные обновления в режиме реального времени благодаря сотрудничеству с разведывательным сообществом США, что позволило им отразить эти атаки», — сказал Фик.

«Дело не в том, что атак не было, а в том, что они были неэффективными», — добавил он.

В прошлом году Microsoft объявила, что предотвратила российские кибератаки, направленные против Украины и организаций в США и Европейском союзе.

Том Берт, корпоративный вице-президент Microsoft по безопасности и доверию клиентов, сказал, что атаки были организованы российской хакерской группой Strontium, которая, как сообщается, связана с ГРУ, российской военной разведкой.

Берт сказал, что Microsoft смогла помешать кибератакам со стороны Strontium после того, как технический гигант получил постановление суда, позволяющее ему захватить онлайн-домены, используемые группой.

С началом войны правительство США также активизировало свои усилия по оказанию помощи Украине и другим странам Восточной Европы в укреплении их киберзащиты, что помогло противостоять российским кибератакам и смягчить их воздействие.

Замечания Фика также совпадают с комментариями, сделанными в прошлом году министром внутренней безопасности Алехандро Майоркасом.

Давая показания перед слушаниями в комитете Палаты представителей в ноябре, Майоркас сказал законодателям, что его агентство сосредоточено на укреплении государственно-частного партнерства и сотрудничества с иностранными партнерами. Он добавил, что эти партнерские отношения становятся «все более важными», поскольку враждебные страны расширяют свои кибервозможности и все чаще стремятся атаковать критически важную инфраструктуру в США.

Во время слушаний по утверждению Фик пообещал создать в своем бюро и во всем агентстве культуру, в которой обязательным является наличие опыта в области кибер- и цифровых технологий. Он также пообещал сосредоточиться на внешних угрозах, включая российские кибератаки и цифровую конкуренцию США с Китаем.

Фик ранее был генеральным директором технологической фирмы Elastic. До этого он был генеральным директором Endgame, компании по разработке программного обеспечения для кибербезопасности. Фик также служил в морской пехоте, побывав в боевых действиях в Афганистане и Ираке». ***(Ines Kagubare. Russia-Ukraine war has improved US cyber cooperation, says key official // Nexstar Media Inc. (https://thehill.com/policy/cybersecurity/3841444-russia-ukraine-war-has-improved-us-cyber-cooperation-says-key-official/). 02.02.2023).***

***

«ФБР пытается улучшить отношения с компаниями для устранения текущих угроз кибербезопасности.

Есть опасения относительно того, насколько компании могут доверять ФБР. Есть опасения по поводу коррупции, инсайдерской торговли и доступа к информации, возникающей в результате предоставления государственному органу доступа к частной информации частной компании.

И все же есть причины, по которым им следует подумать о том, чтобы стать более открытыми для рабочих отношений. Как отмечает The Wall Street Journal, необходимо решить проблемы с инфраструктурой и интеллектуальной собственностью. Многие крупные корпорации пострадали больше, чем нужно, потому что они не обратились в ФБР со своими проблемами кибербезопасности достаточно рано.

Резервное копирование

Когда Equifax был взломан в 2015 году, компания начала нервничать, работая с ФБР из-за опасений по поводу масштабного характера процесса и доступа правительства к ее информации. В качестве альтернативы, технологическая компания WatchGuard Technologies работала напрямую с ФБР, чтобы исправить устройства, пострадавшие от вредоносного ПО, распространяемого российским

государством после начала войны в Украине. «Если бы мы работали независимо, ни одна из сторон не смогла бы добиться таких же результатов так быстро», — говорит бывший представитель компании Суджит Раман.

Однако, учитывая доказанные злоупотребления со стороны правительственных групп, таких как ФБР, у компаний есть основания опасаться того, как используется доступ к их материалам. Apple в этом отношении особенно не сотрудничала, отказавшись разблокировать iPhone, который использовался подозреваемыми в терроризме в Сан-Бернардино в 2015 году намного сложнее…» ***(Tyler Hummel. Companies Don't Trust the FBI With Cybersecurity // Leaders.com (https://leaders.com/news/public-policy/companies-dont-trust-the-fbi-with-cybersecurity/). 11.02.2023).***

***

«…Управление транспортной безопасности (TSA) 18 октября 2022 года выпустило новую директиву по безопасности (SD) для повышения готовности к кибербезопасности и устойчивости определенных пассажирских и грузовых железных дорог. SD был разработан при активном участии заинтересованных сторон отрасли и федеральных агентств, включая Агентство кибербезопасности и безопасности инфраструктуры Министерства внутренней безопасности США (CISA) и Федеральное управление железных дорог (FRA). Он использует многоуровневый подход к глубокоэшелонированной защите.

SD поддерживает усилия администрации Байдена по защите необходимой инфраструктуры от кибератак и обновляет предыдущие требования. В декабре 2021 года TSA выпустило два SD, которые требуют от определенных организаций наземного транспорта принять срочно необходимые меры для немедленного повышения кибербезопасности сектора наземного транспорта. В июле 2022 года, после атаки программы-вымогателя Colonial Pipeline в 2021 году, TSA выпустило пересмотренные требования к кибербезопасности для операторов трубопроводов в США с упором на меры, основанные на производительности, для достижения критических результатов кибербезопасности. Совсем недавно, 12 октября 2022 года, TSA объявило о планах выпустить новые требования кибербезопасности для критически важных авиационных систем после того, как веб-сайты нескольких аэропортов США подверглись явно скоординированным атакам типа «отказ в обслуживании». Эти директивы демонстрируют постоянные усилия администрации Байдена по повышению устойчивости национальной инфраструктуры к кибербезопасности, которые мы ожидаем ускорить.

SD применяется ко всем грузовым железнодорожным перевозчикам (владельцам/операторам), подпадающим под действие предыдущей Директивы о безопасности 1580-21-01, а также к другим грузовым и пассажирским железным дорогам, определенным TSA, на основе определения риска. TSA уведомит такого Владельца/Операторов и предоставит конкретные сроки соблюдения требований директивы.

Директива по безопасности 1580/82-2022-01: Действия и тестирование по снижению кибербезопасности на железнодорожном транспорте

SD требует, чтобы указанные TSA пассажирские и грузовые железнодорожные перевозчики принимали меры для предотвращения сбоев и деградации железнодорожной инфраструктуры. SD обязывает этих владельцев/операторов реализовать две всеобъемлющие меры кибербезопасности, предназначенные для предотвращения сбоев в их инфраструктуре и операциях.

Во-первых, SD требует, чтобы владельцы/операторы, на которые распространяется действие страховки, разработали и выполнили одобренный TSA план внедрения кибербезопасности (CIP), в котором описываются конкретные меры кибербезопасности, которые используют пассажирские и грузовые железнодорожные перевозчики, а также устанавливаются определенные стандарты, которые эти перевозчики должны включить в CIP. сделать следующее:

Определите «критические киберсистемы», как это определено в SD.

Внедрите политики и элементы управления сегментации сети, чтобы предотвратить нарушение работы OT, вызванное компрометацией информационных технологий (ИТ), и наоборот.

Создайте и внедрите элементы управления доступом для предотвращения несанкционированного доступа к критически важным киберсистемам.

Убедитесь, что эти критически важные системы охвачены политиками и процедурами непрерывного мониторинга и обнаружения для обнаружения угроз.

Своевременно применяйте исправления и обновления безопасности для операционных систем, приложений, драйверов и микропрограмм в критически важных киберсистемах, используя методологию, основанную на оценке рисков.

CIP, который устанавливает стандарты, которым должны соответствовать организации, требует одобрения TSA. TSA имеет право инспектировать застрахованные организации на соответствие их утвержденным CIP. Требования CIP обширны и подробны и носят более предписывающий характер, чем большинство действующих федеральных правил кибербезопасности.

Во-вторых, владельцы/операторы, на которые распространяется действие программы, должны создать Программу оценки кибербезопасности (CAP) и представить годовой план для CAP. CAP должен активно оценивать и проверять меры кибербезопасности и отслеживать CIP владельца/оператора. CAP также повлечет за собой первоначальный обзор архитектурного проекта, как предписано TSA, и будет включать тестирование на проникновение и другие инструменты оценки.

Новый SD основан на инициативе TSA по обеспечению безопасности, основанной на производительности. Директива по безопасности 1580-2021-01, выпущенная в декабре прошлого года, подробно описывает четыре требования к владельцам/операторам: (1) назначить координатора по кибербезопасности; (2) сообщать об инцидентах кибербезопасности в CISA; (3) реализовать план реагирования на инциденты; и (4) выполнить оценку уязвимости кибербезопасности. Он должен был использовать более гибкий подход к двум более ранним директивам 2021 года и учитывать структуру ИТ, характерную для промышленных систем управления, включая операционные технологии и ИТ. Том ВанНорман, старший вице-президент GRIMM Cyber, специализирующийся на промышленных системах управления (ICS) и OT в критической инфраструктуре,

отмечает, что новый SD устанавливает более конкретные требования, касающиеся инвентаризации сети, видимости и мониторинга активов, а также установки исправлений. В то время как предыдущие SD содержали общие рекомендации по передовым методам кибербезопасности и иногда подвергались критике за то, что они не учитывали особенности OT, новый подход TSA является более целенаправленным, предписывающим и специфичным для набора проблем, но при этом оставляет возможность для владельцев/операторов. разрабатывать программы кибербезопасности, соответствующие их системам и профилям рисков. Новый SD также сигнализирует о повышенном внимании к соответствию требованиям, чем в предыдущих версиях.

В соответствии с SD TSA уведомил или уведомит владельцев/операторов, на которые распространяется действие новых правил. Такие Владелец/Операторы должны немедленно подтвердить получение по электронной почте, как указано в уведомлении. Затем владелец/операторы должны представить CIP на утверждение TSA не позднее 21 февраля 2023 г., то есть через 120 дней после даты вступления в силу SD. Этот жесткий график может быть сложным для владельцев/операторов, у которых еще нет плана, особенно для небольших операторов с ограниченными ресурсами. ВанНорман предлагает уложиться в сроки реализации, а владельцы/операторы должны сосредоточиться на наиболее ценных активах своей организации, расставить приоритеты в мерах защиты, таких как мониторинг и установка исправлений, а также разработать соответствующие политики и меры контроля для снижения рисков, связанных с кибербезопасностью.

Не позднее, чем через 60 дней после утверждения TSA CIP владельца/оператора, владелец/оператор должен представить годовой план с описанием того, как они будут выполнять свой CAP, который измеряет эффективность CIP. Этот годовой план должен включать график конкретных действий и должен ежегодно обновляться.

В последние годы кибербезопасность критической инфраструктуры привлекла к себе внимание в новостях и среди политиков. Он останется в центре внимания специалистов по безопасности и регулирующих органов. Предприятиям в критической инфраструктуре необходимо будет соответствовать различным требованиям и срокам, связанным с этими планами внедрения. TSA также намеревается начать процесс нормотворчества, который установит нормативные требования для железнодорожного сектора после периода общественного обсуждения…» ***(David Aaron, Oviett Worthington Wargula. New TSA Rail Cybersecurity Rule Shows Trend Toward Prescriptive Mandates // Perkins Coie LLP (https://www.perkinscoie.com/en/news-insights/new-tsa-rail-cybersecurity-rule-shows-trend-toward-prescriptive-mandates.html). 10.02.2023).***

***

«Администрация Байдена публикует национальный стратегический план кибербезопасности, чтобы определить, как Соединенные Штаты обеспечивают более безопасную онлайн-сферу. В нем рассказывается о национальной обороне, защите от хакеров предприятий и ключевой инфраструктуры и многом другом…

Многочисленные факторы, несомненно, побудили администрацию Байдена подавить кибербезопасность с помощью этого плана. Один из них, вероятно, заключается в том, что Соединенные Штаты часто являются целью и страной происхождения онлайн-атак.

NordLocker обнаружил, что 46 процентов атак программ-вымогателей происходят в США. Еще одним открытием стало то, что Мичиган больше всего пострадал от таких инцидентов, а Миссури — реже всего. В другом месте исследование CyberProof показало, что Соединенные Штаты занимают второе место в рейтинге стран по происхождению кибератак, и только Китай совершает больше таких преступлений.

Не помогает и то, что необузданные кибератаки могут помешать достижению других целей Байдена в отношении Соединенных Штатов. Например, в 2021 году лидер приказал провести 100-дневное расследование нехватки полупроводников в стране. Наращивание внутреннего производства было одной из широко обсуждаемых возможностей решения этой проблемы. Однако кибератаки серьезно мешают производственным операциям, часто вынуждая пострадавшие компании останавливать производственные линии и отключаться от онлайн-сетей.

В сборнике мнений экспертов от Homeland Security Today люди часто предупреждали о том, что Соединенные Штаты должны серьезно относиться к кибербезопасности и защищать критически важную инфраструктуру.

Эксперты не могут читать мысли президента Байдена, чтобы точно знать, какие факторы вдохновили стратегический план кибербезопасности. Однако наиболее вероятными являются описанные выше движущие силы.

Предыдущие подходы к кибербезопасности на национальном уровне были сосредоточены на государственно-частном партнерстве и практике обмена информацией. Тем не менее, мы можем ожидать сравнительно большего внимания к регулированию.

Washington Post указывает, что страна будет использовать существующие регулирующие органы, где это возможно, а затем использовать Конгресс для устранения пробелов. Однако пока нет ни слова о том, как и когда произойдет необходимая реализация. Освещение также разъясняло, как члены Конгресса должны работать вместе для реализации целей стратегии, потому что исполнительная власть может сделать очень мало. Один эксперт по кибербезопасности, которого цитирует The Post, сомневается, что в следующем году будет достигнут значительный прогресс.

Закон Bloomberg разъяснил, что в стратегии отсутствуют регулирующие зубы сами по себе. Однако содержащиеся в нем детали могут заставить другие агентства принять меры по изменению подхода к кибербезопасности. Одна из предложенных возможностей заключалась в том, что Административно-бюджетное управление могло бы издавать больше правил для организаций, находящихся под его влиянием. Другой вариант заключается в том, что Агентство по кибербезопасности и безопасности инфраструктуры может обеспечить соблюдение обязательных операционных директив, затрагивающих федеральные информационные системы.

В оценке проекта, опубликованной Washington Post, говорится о переносе ответственности на организации, создающие программное обеспечение с

недостатками безопасности. В плане признается, что даже самые передовые меры по обеспечению безопасности программного обеспечения не могут устранить все уязвимости; однако поставщики должны принимать разумные меры для снижения рисков.

Освещение Slate о программе стратегической кибербезопасности также предполагает более надежную защиту от хакеров, стремящихся пожертвовать национальной безопасностью. Национальная объединенная оперативная группа ФБР по расследованию киберугроз будет систематически работать со всеми соответствующими федеральными агентствами, чтобы вмешиваться и уничтожать враждебные киберпреступные сети.

Более того, частные компании также будут играть жизненно важную роль в этих усилиях. Представители этих организаций предупредят соответствующие органы о возможных или подтвержденных нападениях. Они также помогут предотвратить кибер-инциденты. Это не первый акцент на избежание потенциальных угроз в президентстве Байдена. Распоряжение от 2021 года касалось расследования приложений, принадлежащих иностранным противникам, в частности TikTok и WeChat.

Однако стратегия Байдена распространяется только на наступательные действия против сторон, пытающихся проникнуть в сети США. Любой, кто ожидает подробностей об оборонительных усилиях страны в этом отношении, найдет их в плане, опубликованном Пентагоном, который, как сообщается, основан на стратегии администрации Байдена.

Однако в стратегии кибербезопасности Байдена есть 30 страниц, посвященных защите от критически важной инфраструктуры. Это относится к частям экономики, которые считаются важными для современного общества. Существенным изменением в новом плане является то, что защита этих жизненно важных секторов становится обязательной, а не добровольной. Возможно, атака Colonial Pipeline в 2021 году, в ходе которой программа-вымогатель нарушила поставку бензина и авиакеросина из Техаса в юго-восточную часть Америки, послужила тревожным звонком, но это не первая атака на инфраструктуру и уж точно не будет последний.

Но не ждите единых правил для всех компаний, работающих в сфере критической инфраструктуры. Администрация Байдена начала тщательно изучать каждую соответствующую отрасль более чем за год до стратегии кибербезопасности 2023 года. Это говорит о том, что каждому сектору может потребоваться следовать различным передовым методам кибербезопасности в зависимости от наиболее значительных рисков, с которыми он сталкивается.

Даже после публикации стратегического плана кибербезопасности некоторые вещи не изменятся. Естественно, один из них заключается в том, что компании по-прежнему должны поощрять сотрудников к обеспечению безопасности в Интернете. Когда CGS опубликовала советы о том, как заинтересовать сотрудников, она указала, что 99% работников отдают предпочтение удобству, а не обеспечению безопасности на рабочем месте. Привлечение рабочей силы может стать еще более важным со стратегией кибербезопасности.

В обзоре Corporate Compliance Insights предполагается, что его внедрение может привести к тому, что частные организации будут устанавливать стандарты, аналогичные тем, которые применяются к государственным учреждениям или предприятиям в категории критической инфраструктуры. Регулирование и аудиты также могут увеличиться, а это означает, что организация должна убедиться, что она делает все необходимое и возможное для предотвращения кибератак.

Анализ также предупредил, что для удовлетворения ожиданий, изложенных в плане администрации Байдена, потребуются скоординированные усилия, включающие участие правительства. Это говорит о том, что многим компаниям потребуется внести существенные изменения в обеспечение кибербезопасности. Однако лучший вариант — точно подтвердить, что от вас требуется, прежде чем приступить к реализации.

Кибербезопасность — это быстро развивающаяся и постоянно развивающаяся отрасль. Многие, знакомые со стратегией администрации Байдена, считают, что контент в целом подходит для онлайн-безопасности. Но только время покажет, как будет выглядеть его реализация на практике, как долго затронутые организации должны соблюдать требования и что произойдет, если они этого не сделают…» ***(Shannon Flynn. What Is the Biden Administration 2023 National Cybersecurity Strategy? // MUO (https://www.makeuseof.com/biden-2023-national-cybersecurity-strategy/). 15.02.2023).***

***

Країни ЄС та Великобританія

«…Британское правительство предлагает предоставить себе больше полномочий правоохранительных органов против хакеров в ходе публичных консультаций, которые, по словам критиков, омрачены отсутствием конкретных предложений по защите добросовестных исследователей в области безопасности.

Консервативное правительство премьер-министра Риши Сунака в этом месяце представило предложения по обновлению основного закона Великобритании о борьбе с хакерскими атаками, Закона о неправомерном использовании компьютеров 1990 года. для дальнейшей криминализации владения украденными данными. Чиновники Министерства внутренних дел пообещали, что обновленный закон будет включать защиту белых хакеров, но пока не представили никаких конкретных предложений по этому поводу.

Закон 1990 г. предусматривает уголовную ответственность за несанкционированный доступ к компьютерным системам и данным, а также за их повреждение или уничтожение и предназначен для защиты безопасности и целостности систем и информации.

…«В закон было внесено несколько поправок, последняя из которых была в 2015 году, чтобы обеспечить соответствие законодательства Великобритании требованиям Конвенции Совета Европы о киберпреступности — Будапештской конвенции — и другим соответствующим директивам ЕС», — говорится в

сообщении Британского общества компьютеров и права. «Однако эти изменения были относительно ограниченными».

В запросе комментариев от 7 февраля правительство заявило, что оно особенно заинтересовано в получении отзывов о своих предложениях от правоохранительных органов, регистраторов и реестров доменных имен и хостинг-провайдеров. Член парламента от консерваторов Том Тугендхат, занимающий пост государственного министра безопасности, входящего в состав Министерства внутренних дел, говорит, что правительство также хочет получить отзывы по трем конкретным предложенным обновлениям закона:

Изъятие IP-адресов: Должны ли правоохранительные органы иметь право изымать домены и IP-адреса, когда они используются преступниками, например, для взлома или мошенничества? «Мы признаем, что значительная часть средств делается в рамках добровольных соглашений по борьбе с неправомерным использованием доменных имен, и мы не хотели бы, чтобы эти соглашения были подорваны, но я считаю, что нам необходимо обеспечить, чтобы там, где такие соглашения недоступны, правоохранительные органы возможность действовать», — говорит Тугендхат.

Сохранение данных: Должны ли правоохранительные органы иметь возможность требовать сохранения компьютерных данных в случае, если это потребуется в ходе расследования? Предложение не позволит полиции напрямую изымать такие данные — только требовать их сохранения.

Преступления в отношении данных: следует ли криминализировать владение или использование украденных данных, включая информацию, позволяющую установить личность, которая была получена от кого-то другого, который сам нарушил Закон о неправомерном использовании компьютеров?

«Примечательной особенностью предлагаемых изменений является попытка разорвать связь между преступными доменами и доменами-жертвами», — говорит Джулия Варли, сотрудник лондонской юридической фирмы Pinsent Masons, которая специализируется на киберрисках. Помимо изъятия IP-адресов, подозреваемых в использовании преступниками, предлагаемые изменения также дадут полиции «право потребовать от реестра Великобритании не регистрировать доменные имена, которые, по прогнозам, будут использоваться в преступных целях».

Министерство внутренних дел соберет заинтересованные стороны для обсуждения предложений по решению ряда «сложных вопросов» путем внесения изменений в CMA.

К ним относятся «предложения по уровням вынесения приговоров, защите от преступлений CMA, улучшения возможности сообщать об уязвимостях, а также о том, достаточно ли в Великобритании законодательства для покрытия экстерриториальных угроз», — говорит Тугендхат.

В этом заявлении упоминается обещание правительства пересмотреть правовую защиту для исследователей кибербезопасности, которые действуют добросовестно. Внедрение таких мер защиты было широко востребовано поставщиками услуг и членами сообщества кибербезопасности, в том числе Киараном Мартином, бывшим главой Британского национального центра

кибербезопасности. «Правительство не делает ничего плохого. Просто закон 1990 года о неправомерном использовании компьютеров явно устарел», — написал Мартин в Твиттере в сентябре прошлого года.

На данный момент «сохраняющаяся неопределенность» в отношении средств защиты для специалистов по кибербезопасности усложняет задачу защиты британских организаций от онлайн-атак, говорит Кэт Соммер, руководитель группы по стратегии и связям с общественностью в манчестерской консалтинговой компании по кибербезопасности NCC Group.

Соммер спрашивает, почему правительство так долго обновляет CMA. «После 21 месяца консультаций мы надеялись, что 32-летний Закон о неправомерном использовании компьютеров станет еще лучше, чем то, что было объявлено», — говорит она.

Какие бы изменения ни вносились в CMA, у каждого закона есть свои пределы. В данном случае это включает в себя проблему борьбы с киберпреступностью, когда так много преступников проживает не только за пределами Великобритании, но и в России или вокруг нее, которая, как правило, не выдает своих граждан.

«Правительству Великобритании придется полагаться на сотрудничество с правительствами и правоохранительными органами в других юрисдикциях, а также в тех юрисдикциях, которые имеют возможность и законодательство для судебного преследования за экстерриториальную преступность», — говорит Стюарт Дэйви, партнер Pinsent Masons. «Это глобальная проблема, которая требует глобального ответа, и это в какой-то степени признается в ходе консультаций».

Потенциально усугубляет проблему статус отношений Великобритании с Европейским союзом. Несмотря на предложения об обратном со стороны некоторых британских официальных лиц, выступавших за Brexit, после того, как Великобритания вышла из ЕС, ей больше не разрешалось быть членом правоохранительной разведывательной службы ЕС, Европола. Великобритания также потеряла доступ к Шенгенской информационной системе, которая облегчает обмен информацией о границах и безопасности между государствами-членами ЕС.

Быстрый поток информации не был полностью прерван. Согласно отчету Палаты лордов, Великобритания подписала соглашение о торговле и сотрудничестве с ЕС, которое дает ей доступ к некоторым базам данных ЕС. «Например, данные ДНК и отпечатков пальцев могут продолжать обмениваться через систему Prüm при определенных ограничениях и предварительных условиях», — говорится в сообщении.

Кроме того, в соответствии с TCA британским офицерам связи разрешено «присутствовать в штаб-квартире Европола для облегчения трансграничного сотрудничества». Хотя Великобритания потеряла доступ к европейскому ордеру на арест, в соответствии с TCA у нее есть «договоренности об экстрадиции, аналогичные Соглашению ЕС о капитуляции с Норвегией и Исландией».

В соответствии с европейским ордером на арест подозреваемый, арестованный на территории ЕС, должен быть переведен в государство-член ЕС, подавшее ордер, в течение 60 дней. В соответствии с TCA такие переводы могут занимать до 90 дней». ***(Mathew J. Schwartz. Computer Crime: Britain Plans to***

Overhaul 32-Year-Old Law // Information Security Media Group, Corp. (https://www.govinfosecurity.com/computer-crime-britain-plans-to-overhaul-32-year-old-law-a-21229). 17.02.2023).

***

«Чтобы повысить свою кибербезопасность, Совет корпоративного управления Европейской комиссии решил приостановить использование приложения TikTok на своих корпоративных устройствах и на личных устройствах, зарегистрированных в службе мобильных устройств Комиссии.

Эта мера направлена на защиту Комиссии от угроз кибербезопасности и действий, которые могут быть использованы для кибератак на корпоративную среду Комиссии.

Комиссия заявила, что развитие безопасности других платформ социальных сетей также будет находиться под постоянным контролем.

Эта мера соответствует строгой внутренней политике Комиссии в области кибербезопасности в отношении использования мобильных устройств для связи, связанной с работой. Он дополняет давно даваемые Комиссией рекомендации сотрудникам применять передовой опыт при использовании платформ социальных сетей и поддерживать высокий уровень осведомленности о кибербезопасности в своей повседневной работе…» ***(European Commission Bans TikTok on Staff Phones to Increase Cybersecurity // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/european-commission-bans-tiktok-on-staff-phones-to-increase-cybersecurity/). 24.02.2023).***

***

«Национальный центр кибербезопасности, входящий в штаб-квартиру правительственных коммуникаций разведывательного управления Великобритании, является частью растущего числа государственных органов, расследующих кибератаку на ION Trading UK.

NCSC присоединяется к Управлению финансового надзора, Управлению пруденциального регулирования и Федеральному бюро расследований США в поисках информации об инциденте, по словам людей, знакомых с этим вопросом, которые не уполномочены выступать публично.

ION, малоизвестная, но крайне важная компания-разработчик программного обеспечения, которая обеспечивает бесперебойное функционирование рынков акций, облигаций и товаров, во вторник начала сдавать позиции. В среду агентство Bloomberg сообщило, что за инцидентом стоит российская банда вымогателей LockBit.

Ребекка Торп, генеральный директор консалтинговой компании Bovill, заявила, что Банк Англии хотел бы видеть, что у фирм есть надежные планы по предоставлению основных услуг во время сбоев, включая кибератаки.

По ее словам, компании должны определить и установить допуски на воздействие и убедиться, что они могут оставаться в них с помощью тестирования, включая смоделированные кибератаки, предоставляемые Банком Англии». ***(William Shaw. UK's National Cyber Security Center Also Looking Into ION Hack //***

Bloomberg L.P. (https://www.bnnbloomberg.ca/uk-s-national-cyber-security-center-also-looking-into-ion-hack-1.1878921). 03.02.2023).

***

«Чешское национальное агентство по кибербезопасности и информационной безопасности недавно опубликовало законопроект о новом Законе о кибербезопасности, который включает обоснование и правила реализации новой нормативно-правовой базы, и открыло публичные консультации по законопроекту. Заинтересованные стороны и широкая общественность должны до 26 февраля 2023 года ознакомиться с законопроектом и имплементационными постановлениями, а также представить предложения и комментарии по новой предлагаемой нормативно-правовой базе.

Этот законопроект о кибербезопасности был разработан в ответ на принятие 14 декабря 2022 года Директивы (ЕС) 2022/2555 Европейского парламента и Совета о мерах по обеспечению высокого общего уровня кибербезопасности в Союзе (NIS2).

NIS2 направлена на достижение высокого общего уровня кибербезопасности в ЕС и заменяет существующую Директиву (ЕС) 2016/1148 Европейского парламента и Совета от 6 июля 2016 г., касающуюся мер по обеспечению высокого общего уровня безопасности сетей и информационных систем во всех странах Союза (NIS).

NIS2 поддерживает и расширяет NIS.

В Чешской Республике NIS была внедрена с принятием Закона № 181/2014 Coll. по кибербезопасности с поправками. Однако объем изменений, предусмотренных NIS2, побудил чешских законодателей полностью заменить Закон о кибербезопасности и принять новый Закон. Это новое законодательство будет реализовывать NIS2 и принимать дополнительные изменения, основанные на практическом опыте применения первоначального Закона о кибербезопасности». ***(Tomáš Matejovský, Jan Jezek. Czech Republic initiates public consultation on NIS2 implementation // CMS Legal (https://cms-lawnow.com/en/ealerts/2023/01/czech-republic-initiates-public-consultation-on-nis2-implementation). 01.02.2023).***

***

«В сфере кибербезопасности наблюдается кризис, и в этом году государственный сектор, включая государственные учреждения, ощутит кумулятивное воздействие.

Отчет Ipsos для Департамента цифровых технологий, культуры, СМИ и спорта в мае показал, что многим британским предприятиям требуется больше сотрудников с техническими навыками, навыками реагирования на инциденты и управления, необходимыми для управления их кибербезопасностью. Учитывая, что правительство несет ответственность за обеспечение безопасности всей нашей критически важной национальной инфраструктуры, а попытки привлечь квалифицированных специалистов в области кибербезопасности в государственный сектор в последние годы не уменьшили разрыв в навыках, необходимо принять меры, чтобы противостоять растущему ландшафту угроз.

Насколько распространены нарушения безопасности в правительстве?

Заголовки, касающиеся нарушений государственной безопасности, похоже, часто появляются в СМИ. В ноябре 2022 года FT сообщила, что регулятор защиты данных объявил Министерству образования выговор за предоставление неправомерного доступа к идентифицирующей информации о 28 миллионах детей; В апреле 2022 года визовая служба Министерства внутренних дел Великобритании непреднамеренно скопировала 170 адресов электронной почты клиентов в электронное письмо, а в декабре прошлого года Кабинет министров был оштрафован на 500000 фунтов стерлингов Управлением уполномоченного по информации после того, как почтовые адреса получателей новогодних наград 2020 года просочились в сеть.

Похоже, что по крайней мере в двух из этих инцидентов была замешана рука злонамеренных инсайдеров, что отражает внутренние опасности, которые таятся во многих правительственных ведомствах. Вот почему так важно иметь строгие внутренние меры безопасности, а также важно следить за подозрительной активностью в режиме реального времени или по мере ее возникновения. Если правительственные службы безопасности могут создавать интеллектуальные показатели киберугроз, фиксировать и выявлять активные киберугрозы и сводить к минимуму количество ложных срабатываний, они лучше справляются с атаками.

Больше данных может привести к большему пониманию угроз

Распространение данных лежит в основе как проблемы, так и решения, когда речь идет о кибербезопасности. Имея в своем распоряжении больше данных в режиме реального времени, тем лучше информированы государственные учреждения и тем больше информации они могут применить к основным государственным услугам. Однако огромный объем и скорость передачи данных усложняют управление и создают проблемы при внедрении системы обнаружения вторжений.

Цель всех специалистов по кибербезопасности — заставить данные работать в борьбе с угрозами, в идеале путем объединения данных, требующих немедленного действия, с исторически значимыми данными, чтобы можно было получить ценную информацию за миллисекунды. Это приводит к информированным ответам, когда начинает проявляться атака или угроза атаки.

Проблема, однако, заключается в том, что современные подходы к кибербезопасности должны реагировать на поток угроз, связанных с удаленной и гибридной работой, а также с увеличением использования мобильных устройств, социальных каналов и виртуализированных облачных сетей. Традиционные механизмы безопасности не могут использовать огромный массив источников данных, которые могут пролить свет на то, где развиваются риски и как ими можно управлять.

Правительственным ведомствам необходим доступ к инструментам, которые минимизируют эффективное время реакции между выявлением атаки, устранением активной атаки и устранением будущих атак. Без этого существует опасность значительных финансовых последствий, репутационного ущерба, потери секретных или личных данных и даже риска для национальной безопасности.

Вот почему скорость и экстремальная масштабируемость инфраструктуры данных так важны для специалистов по кибербезопасности в государственном и государственном секторах. Это позволяет им преодолеть разрыв между анализом ландшафта угроз и реагированием на угрозы в реальном времени по мере их возникновения. Лучший способ понять современный развивающийся ландшафт угроз в режиме реального времени — получить немедленный доступ к огромным объемам данных, которые могут использовать адаптивные, самообучающиеся алгоритмы.

Платформы данных в режиме реального времени могут восполнить пробел в уязвимости

В нынешних условиях государственные ведомства выиграют от тех же платформ реального времени, которые развертывают частные предприятия, чтобы выйти за рамки типичных методов обнаружения угроз на основе сигнатур. Эти платформы могут принимать интеллектуальные данные и доставлять их быстро и в больших количествах, чтобы вычислительные механизмы, работающие с алгоритмами самообучения, могли обнаруживать закономерности подозрительного поведения в сети. Наши собственные клиенты используют нашу многооблачную платформу базы данных для ежедневного анализа миллиардов событий, что намного превышает возможности любой устаревшей системы.

Принимая и сохраняя петабайты данных из нескольких различных источников, можно проводить анализ для защиты не только сетей государственного сектора и правительства, но и приложений, платформ и даже систем Интернета вещей (IoT).

Учитывая нехватку талантов в области кибербезопасности, профессионалам необходим доступ к мощным инструментам, которые помогут им реагировать быстрее и эффективнее. Платформы управления данными в режиме реального времени делают это, используя различные решения для непрерывной диагностики и смягчения последствий, такие как аналитика угроз, безопасность конечных точек, управление доступом, облачная безопасность, Zero Trust, безопасность учетных записей, мониторинг активности пользователей и новые технологии.

Эти платформы предоставляют множество функций, которые защищают каждый аспект инфраструктуры государственного ведомства, высвобождая время и таланты руководителей службы безопасности и их команд. Кроме того, они служат мощным конкурентным преимуществом для защиты секретных данных и частной интеллектуальной собственности. Ни одно государственное ведомство не может позволить себе ждать разрешения кризиса кадров, оставляя под угрозой критически важную государственную инфраструктуру, и платформы управления базами данных в режиме реального времени могут восполнить этот пробел и устранить растущие угрозы кибербезопасности». ***(Martin James. Using real-time data platforms to plug cybersecurity skills gap // Adjacent Digital Politics Ltd (https://www.openaccessgovernment.org/using-real-time-data-platforms-plug-cybersecurity-skills-gap/152529/). 02.02.2023).***

***

«…Исследование нарушений кибербезопасности, проведенное правительством Великобритании в 2022 году, показало, что 82% британских советов директоров и высшего руководства считают кибербезопасность высокоприоритетной задачей, в то время как документ «Исследование приоритетов безопасности» показывает, что 90% респондентов считают, что их организация не справляется с киберрисками должным образом.

Повышение квалификации, автоматизация и аутсорсинг — все это варианты, которые организации могут и должны использовать для создания устойчивой системы кибербезопасности при ограниченном бюджете.

Необходимость повышения квалификации и обучения

Нехватка цифровых навыков — это постоянная проблема, которая сильно ощущается во всей технологической отрасли. Эта проблема распространяется на кибербезопасность, однако ее последствия можно было бы уменьшить, если бы ИТ-команды прошли обучение кибербезопасности.

Отчет Fortinet о пробелах в навыках кибербезопасности за 2022 год показал, что 64% организаций по всему миру столкнулись с той или иной формой нарушения безопасности, что связывает 80% этих атак с пробелами в навыках кибербезопасности. Кроме того, непредумышленные ошибки пользователя были названы основной причиной инцидентов, связанных с безопасностью. Это подчеркивает пробел в осведомленности и понимании кибератак нынешними сотрудниками, а также необходимость улучшения образования в отношении угроз как для сотрудников, занимающихся кибербезопасностью, так и для сотрудников, не занимающихся кибербезопасностью.

Благодаря регулярному обучению и повышению квалификации организации смогут вооружить своих сотрудников знаниями, которые позволят им эффективно действовать для защиты от атак, а также понять, что делать для восстановления после успешной атаки.

Кроме того, существует множество неиспользованных пулов людей, которых можно привлечь, чтобы восполнить пробел. Например, женщины практически не представлены в мире технологий, и только 19 процентов технологической отрасли составляют женщины. Нестандартное мышление при поиске талантов позволяет организациям в одностороннем порядке расширять доступные им кадровые резервы без дополнительных затрат.

Хотя обучение персонала, поиск талантов и устранение человеческих ошибок — непростая задача, это относительно небольшие расходы по сравнению с финансовыми, временными и репутационными затратами на украденные данные.

Почему автоматизированные технологии — это путь вперед

Обучение и повышение квалификации нынешних сотрудников — это один из способов минимизировать киберриски, но искоренение человеческих ошибок на неопределенный срок практически невозможно без правильной технологии. Технологии автоматизации могут укрепить и дополнить усилия сотрудников, и только 45% компаний в настоящее время используют автоматизированные решения в области кибербезопасности для предотвращения атак и восстановления после них, и их ценность не реализуется в полной мере.

Resilient Zero Trust — одно из эффективных решений для мониторинга конечных устройств и приложений организации на предмет подозрительной активности. Если устройство входит в систему из незнакомого места или получает доступ к приложению с ограниченным доступом, предупреждение может быть отправлено в централизованную ИТ-команду, которая имеет право заморозить или отключить устройство, чтобы предотвратить потенциальное нарушение. Цель этой технологии состоит в том, чтобы сотрудники продолжали работать, а не просто отключались от них при первой же возможности, а также помогали автоматизировать обнаружение угроз.

Количество архитектур с нулевым доверием, развернутых предприятиями, выросло на 8% в период с 2021 по 2022 год, поскольку эта технология предлагает экономически эффективный способ укрепления киберзащиты.

Технологии самовосстановления также могут усилить портфель средств безопасности организации, автоматически восстанавливая и восстанавливая скомпрометированные устройства, снижая риск повторного заражения и позволяя компаниям продолжать использовать свои существующие корпоративные устройства.

Надлежащая подготовка к реагированию на инциденты безопасности занимает первое место при рассмотрении ключевых приоритетов безопасности, а наличие автоматизированных технологий, которые помогают с реагированием и восстановлением, позволит организациям комфортно работать, не беспокоясь о надвигающейся кибератаке.

Аутсорсинг поставщикам услуг

Аутсорсинг — еще одно недорогое решение, которое предприятия могут использовать для улучшения своей кибербезопасности. Поскольку время и деньги являются важным фактором, 83% ИТ-руководителей, которые в настоящее время используют собственную команду безопасности, теперь рассматривают возможность аутсорсинга.

Делегирование задач по обеспечению безопасности квалифицированным специалистам за пределами вашей организации может компенсировать нехватку доступных цифровых талантов, в то же время укрепляя киберзащиту.

Аутсорсинг — это экономически эффективное решение, которое в условиях ограниченного бюджета является огромным стимулом. Организациям не нужно будет беспокоиться об обучении и заработной плате штатных сотрудников, а вместо этого отдать на аутсорсинг услуги, которые просто дешевле.

Кибербезопасность должна оставаться приоритетом, и сложные экономические условия не могут быть оправданием. Имея несколько недорогих подходов к повышению киберустойчивости, организациям следует переосмыслить свои процессы, чтобы извлечь выгоду из доступных им ресурсов.

Развернув сочетание повышения квалификации, автоматизации и аутсорсинга, организации смогут создать надежный портфель кибербезопасности для защиты от входящих угроз и помощи им в восстановлении и эффективном реагировании на атаки». ***(Achi Lewis. Upskilling And Automation The Keys To Cyber Resilience For Businesses // Cyber Defense Media Group.***

(https://www.cyberdefensemagazine.com/upskilling-and-automation-the-keys-to-cyber-resilience-for-businesses/). 13.02.2023).

***

«В Lufthansa произошел «сбой ИТ», из-за чего немецкая группа авиакомпаний задержала и отменила все свои рейсы.

«В настоящее время авиакомпании Lufthansa Group страдают от сбоя ИТ», — говорится в сообщении компании в социальной сети в среду утром. «Это приводит к задержкам и отменам рейсов. Мы сожалеем о неудобствах, которые это доставляет нашим пассажирам».

Программная ошибка влияет на его глобальную сеть. Lufthansa также управляет Austrian Airlines, Brussels Airlines, Swiss и Eurowings.

В настоящее время авиакомпания расследует, связан ли этот инцидент с кибератакой на европейскую авиакомпанию SAS, сообщает Bloomberg.

Различные шведские компании недавно пострадали от предполагаемых кибератак, в том числе телекомпания SVT, которая заявила, что группа под названием «Анонимный Судан» взяла на себя ответственность за атаку, разместив в Telegram сообщение о том, что шведские СМИ будут атакованы в результате сожжения Корана в Швеции». ***(Matthew Parson. Lufthansa Grounds Flights Due to Software Problem // Skift (https://skift.com/blog/lufthansa-grounds-flights-due-to-software-problem-cyber-attack-being-investigated/). 15.02.2023).***

***

«Финляндия запускает проект Cyber Citizen…

Целью проекта Cyber Citizen является создание обучающего портала, содержащего контент, предназначенный для граждан, с учетом различных целевых групп. Портал предлагает образовательные и коммуникационные элементы, которые повышают способность граждан безопасно работать в цифровом мире. В рамках проекта также разрабатывается игра, обучающая гражданским навыкам, связанным с кибербезопасностью. Проект получил 5 миллионов евро финансирования от Фонда восстановления и устойчивости ЕС на три года.

На первом этапе проекта было изучено текущее состояние обучения граждан навыкам кибербезопасности во всех странах-членах Европейского Союза. В отчете об исследовании подчеркиваются знания и навыки, необходимые кибергражданам ЕС в их повседневной жизни, которая становится все более цифровой. Одним из ключевых наблюдений было то, что кибербезопасность граждан по-разному воспринимается в разных странах ЕС. Хотя цифровая повседневная жизнь становится все более значительной частью повседневной жизни, восприятие информации и навыков, связанных с кибербезопасностью, значительно различается в разных странах ЕС.

Исследование показало, что страны ЕС имеют явное желание развивать навыки граждан в области кибербезопасности и поддерживать обучение на протяжении всей жизни. Однако различия между различными целевыми группами еще недостаточно учтены, и требуется больше экспертов и инструкторов по кибербезопасности. В исследовании также подчеркивается, что руководящие

принципы обучения стратегической кибербезопасности в странах ЕС появились относительно недавно.

На следующем этапе проекта Cyber Citizen будет разработана модель обучения граждан навыкам кибербезопасности, а на третьем этапе будет реализован учебный портал, разработка игр и производство другого контента. Геймификация обучения станет неотъемлемой частью учебного портала, поскольку в исследовании подчеркивается, что игры стали формой социального поведения и все более важной формой обучения.

Дальнейшая работа проекта также включает создание общеевропейской сети сотрудничества, которая приветствует всех, кто заинтересован в развитии навыков кибербезопасности граждан. Проект «Кибергражданин» — это важный шаг на пути к наделению граждан необходимыми навыками и знаниями для защиты себя и своей личной информации в цифровом мире». ***(Finland is launching the cyber citizen project, the aim of which is to teach EU citizens important cyber security skills // Nord News (https://nord.news/2023/02/19/finland-is-launching-the-cyber-citizen-project-the-aim-of-which-is-to-teach-eu-citizens-important-cyber-security-skills/). 19.02.2023).***

***

Австралія та Нова Зеландія

«Австралия приняла новую программу управления рисками, ориентированную на кибербезопасность, чтобы повысить устойчивость и безопасность своей критически важной инфраструктуры и основных услуг.

Министр внутренних дел и кибербезопасности Австралии Клэр О'Нил заявила, что новые правила помогут предприятиям подготовиться к угрозам для критически важных активов страны, предотвратить и смягчить их.

«Активы критической инфраструктуры уязвимы для стихийных бедствий и являются привлекательными целями для иностранного вмешательства, киберпреступников и других злоумышленников, которые стремятся причинить вред Австралии», — сказала О'Нил.

Правила управления рисками являются третьей и последней мерой безопасности в недавних поправках к Закону о безопасности критически важной инфраструктуры 2018 года.

Программа управления рисками критической инфраструктуры требует, среди прочего, требования ежегодной отчетности, соответствия и нормативных правил, обязательной отчетности о кибер-инцидентах и нескольких мер государственной помощи.

Правила вступили в силу 17 февраля 2023 года и позволяют критическим активам, которые в настоящее время являются необязательными, в течение шести месяцев принять письменный план управления рисками и дополнительно в течение 12 месяцев для обеспечения соответствия.

Австралия провела несколько реформ в области кибербезопасности в ответ на волну кибератак, с которыми страна столкнулась за последний год. Он также возглавляет глобальную целевую группу по программам-вымогателям, состоящую

из 37 правительств-единомышленников, которые стремятся обмениваться разведывательными данными, чтобы предотвратить будущие атаки с цифровым вымогательством…

В соответствии с последними изменениями в политике Австралия также запустила обновленную Стратегию обеспечения устойчивости критически важной инфраструктуры, которая представляет собой дорожную карту для защиты основных услуг и активов, включая электричество, воду, здравоохранение и продукты.

Цели стратегии заключаются в том, чтобы поддержать владельцев и операторов критической инфраструктуры в эффективном управлении рисками с помощью зрелых, основанных на рисках и устойчивых подходов, а также в укреплении их безопасности и устойчивости с помощью нормативно-правовой базы и улучшения сотрудничества. Она также стремится реализовывать инициативы посредством прочных партнерских отношений между промышленностью и правительством…» ***(Mihir Bagwe. Australia Unveils Game Plan to Guard Critical Infrastructure // Information Security Media Group, Corp. (https://www.govinfosecurity.com/australia-unveils-game-plan-to-guard-critical-infrastructure-a-21276). 21.02.2023).***

***

«Министерство обороны Австралии изымает камеры, сделанные китайскими производителями Hikvision и Dahua, в то время как правительство рассматривает возможность запрета их использования во всех федеральных агентствах.

Использование правительством средств безопасности, произведенных китайскими производителями, превратилось в политический спор в четверг после того, как министр теневой кибербезопасности Джеймс Патерсон оказал давление на правительство премьер-министра Австралии Энтони Альбанезе из Лейбористской партии. Патерсон сказал, что его офіс обнаружил более 900 таких камер, работающих в правительственных учреждениях Австралии.

«Это проблема… и там, где будут найдены эти камеры, они будут удалены», — заявил министр обороны Ричард Марлес в интервью Австралийской радиовещательной корпорации.

Во время парламентского часа вопросов в четверг сенатор Мюррей Уотт, выступая от имени правительства, сказал, что генеральный прокурор «запросил совет о том, требуется ли общегосударственный запрет для устранения угроз безопасности».

Технологии китайского производства вызвали подозрения на международном уровне из-за предполагаемого влияния китайской разведки, опасения, которые особенно усилились после принятия в 2017 году Закона о национальной разведке Китая, который требует от организаций поддержки разведывательной работы. Роль государственных компаний Hikvision и Dahua в увековечивании серьезных нарушений прав человека в отношении уйгурского населения на севере Китая также поставила их под усиливающееся регулирующее давление на Западе.

В Соединенных Штатах Федеральная комиссия по связи в ноябре запретила импорт Hikvision и Dahua по соображениям национальной безопасности. Он также запретил товары и услуги от ZTE и Huawei, крупнейшего в мире производителя телекоммуникационного оборудования.

В ноябре правительство Великобритании приказало правительственным учреждениям удалить китайское оборудование для наблюдения с секретных объектов и рассмотреть вопрос о полном удалении.

Китайские компании и коммунистическое правительство Пекина преуменьшают обвинения в том, что технологические компании действуют как расширения аппарата по сбору разведданных. Во время ежедневной пресс-конференции в четверг официальный представитель министерства иностранных дел заявила, что Китай выступает против «ошибочной практики чрезмерного натяжения концепции национальной безопасности и злоупотребления государственной властью». ***(Jayant Chakravarti. Australia Bans Hikvision & Dahua Cameras From Defense Sites // Information Security Media Group, Corp. (https://www.govinfosecurity.com/australia-bans-hikvision-dahua-cameras-from-defense-sites-a-21179). 10.02.2023).***

***

Російська Федерація та країни ЄАЕС

«Голова думського комітету з інформполітики Олександр Хінштейн заявив, що хакерів, які діють в інтересах російської сторони, мають звільнити від відповідальності після наради з питань кібербезпеки країни-терориста.

«Йдеться про те, щоб загалом опрацювати звільнення від відповідальності для тих осіб, хто діє в інтересах країни у сфері комп'ютерної інформації як на території нашої країни, так і за її межами», — сказав він.

За словами Хінштейна, слід розглянути можливість встановлення законодавчих гарантій для хакерів, які працюють в інтересах уряду: «Я, наприклад, твердо переконаний, що необхідно використовувати будь-які ресурси для ефективної боротьби з противником. Якщо сьогодні нас атакують такі центри, то в нас має бути можливість для адекватної відповіді».

Наразі на росії діяльність щодо виготовлення, використання та розповсюдження шкідливих комп'ютерних програм кримінально карається позбавленням волі на строк до 7 років». ***(Російських хакерів планують законодавчо звільнити від відповідальності у разі співпраці з спецслужбами // No worries! (https://noworries.news/rosijskyh-hakeriv-planuyut-zakonodavcho-zvilnyty-vid-vidpovidalnosti-u-razi-spivpraczi-z-speczsluzhbamy/). 12.02.2023).***

***

«…Роскомнагляд планує запустити в Росії нову систему виявлення загроз в інтернеті під назвою «Вепрь». Ця розробка має стати інструментом для боротьби з кіберзлочинами та прогнозуванням ризиків їх виникнення, які стають все більш поширеними на території Російської Федерації.

Система «Вепрь» тестується у парі з технологією «Окулус», – пише ТАСС. Вони здійснюватимуть моніторинг інтернет-трафіку, щоб виявляти можливі загрози для національної безпеки, та забезпечуватимуть оперативний зв'язок між фахівцями Роскомнагляду та компаніями-операторами.

Відомство має намір запровадити цю систему з метою захисту національних інтересів та державної безпеки. «Вепрь» збиратиме інформацію про підозрілі дії в інтернеті, такі як поширення екстремістських матеріалів, публікація нелегальних контенту та інших можливих загроз для безпеки Росії.

За даними «Ведомостей», вартість розробки системи «Вепрь» в Росії оцінювалася в 60 млн рублів, проте пізніше була знижена до 30 млн рублів. Нині немає інформації про додаткові витрати на розробку системи «Вепрь».

Система «Вепрь» буде інтегрована в єдину базу даних з інтернет-трафіку. Вона дозволить Роскомнагляду оперативно виявляти та припиняти загрози в інтернеті. Відомство заявляє, що система поважатиме права користувачів і не використовуватиметься для масового спостереження чи обмеження свободи інтернету.

Очікується, що система «Вепрь» буде запущена у другій половині 2023 року». ***(У Росії створюють систему «Вепрь» для виявлення в інтернеті інформзагроз // mediasat (https://mediasat.info/uk/2023/02/20/u-rosiyi-stvoryuyut-systemu-vepr-dlya-vyyavlennya-v-interneti-informzagroz/). 20.02.2023).***

***

«Согласно сообщениям, онлайн-трансляции ежегодного выступления президента Владимира Путина были прерваны во вторник после явной кибератаки.

Агентство Reuters сообщило, что журналисты в нескольких местах не смогли получить доступ к веб-сайтам, связанным с Всероссийской государственной телевизионной и радиовещательной компанией (ВГТРК), государственной вещательной компанией, во время выступления Путина перед федеральным собранием.

По данным Reuters, платформа для прямых трансляций Smotrim.ru, которая транслирует государственный телеканал «Россия-24», также периодически отключалась. (Похоже, что оба веб-сайта теперь снова в сети.)

ТАСС, российское государственное информационное агентство, подтвердило в своем сообщении, что трансляция выступления на этих сайтах была прервана, отметив, что вместо этого появилось сообщение об ошибке, в котором говорилось, что «ведутся технические работы».

Тем временем российское государственное информационное агентство РИА Новости заявило, что сбои в трансляции были результатом атаки распределенного отказа в обслуживании (DDoS). Это когда серия ботов наводняет веб-сайт или службу HTTP-запросами и трафиком, пытаясь отключить сеть и сделать ее недоступной для предполагаемых пользователей.

Инсайдер не смог самостоятельно проверить причину сбоев.

Хотя неясно, кто или что стояло за отключениями, по крайней мере одна проукраинская хакерская группа взяла на себя ответственность.

IT-армия Украины, добровольческая организация кибервойны, созданная вскоре после вторжения России в Украину, сообщила в Твиттере: «Мы запустили DDoS-атаку на каналы, транслирующие обращение Путина к Федеральному собранию: 1ТВ, ВГТРК и СМОТРИМ», — говорится в сообщении группы в Твиттере. «Слава Украины».

Newsweek сообщил, что другая хакерская группа, утверждающая, что работает от имени российского оппозиционера Алексея Навального, также взяла на себя ответственность, заявив, что она вызвала сбои вместе с «другими хакерами».

Во время двухчасового обращения, прозвучавшего незадолго до годовщины вторжения России в Украину, Путин выступил против Запада и заявил, что Россия готова возобновить испытания ядерного оружия». ***(Joshua Zitser. Hackers claim to have caused Russian websites broadcasting Vladimir Putin's annual address to go offline // Insider Inc. (https://www.businessinsider.com/cyberattack-temporarily-stops-broadcasts-putin-speech-russia-hack-ddos-ukraine-2023-2). 21.02.2023).***

***

Індія

«Председатель Национальной комиссии по правам человека (NHRC) судья (в отставке) Арун Кумар Мишра в четверг призвал принять строгий закон для борьбы с «незаконным поведением в Интернете и киберпреступлениями». Он выступил после открытия 25-й Всеиндийской конференции судебно-медицинских экспертов в Национальном университете криминалистики в Гандинагаре.

«Необходимо продвигать киберэтику. И правительство должно принять строгое законодательство для наказания за незаконное поведение в Интернете и киберпреступления», — сказал бывший судья Верховного суда.

По его словам, многие страны внесли поправки в свои законы «специально для борьбы с киберпреступлениями наряду с появлением новых видов преступлений».

По словам Мишры, свобода слова, применимая к «социальным сетям и киберпространству», не «больше», чем свобода, предоставляемая отдельным лицам или СМИ.

«Свобода слова в соответствии со статьей 19 Конституции, предоставленная средствам массовой информации или отдельным лицам, такая же, как и свобода, предоставленная социальным сетям или киберпространству, она не шире... Таким образом, должно быть строгое законодательство для борьбы с киберпреступностью. «Мы должны очень строго бороться с неправомерным использованием», — сказал он.

Бывший судья добавил, что киберпространство используется для нарушения гражданских прав и прав человека, а также для нарушения частной жизни.

«Киберпространство вызывает нарушение неприкосновенности частной жизни онлайн-личностей и нарушает право на достойную жизнь. Кибербезопасность является ключом к борьбе с киберпреступностью и защите прав

человека. Глобальные исследования показывают, что Индия занимает третье место по киберугрозам и второе по целенаправленным атакам». ***(NHRC Chief Calls for Strict Laws for Unlawful Internet Behaviour, Cyber Crimes // Red Pixels Ventures Limited (https://www.gadgets360.com/internet/news/nhrc-head-calls-strict-laws-unlawful-internet-behaviour-cyber-crimes-3748306). 02.02.2023).***

***

«В 2022 году в Индии произошло 13,91 миллиона инцидентов кибербезопасности, сообщил в пятницу (10 февраля) парламенту государственный министр по электронике, информации и технологиям Раджив Чандрасекар.

Цифры по-прежнему не дают полной картины кибератак в стране, поскольку эта статистика включает только информацию, сообщаемую и отслеживаемую Индийской группой реагирования на компьютерные чрезвычайные ситуации (CERT-In)

Однако количество зарегистрированных кибератак сократилось в 2022 году по сравнению с 14,02 лакха в 2021 году. По данным правительства, в 2018 году было зарегистрировано 2,08 лакха инцидентов, в 2018 году было зарегистрировано 3,94 лакха атак и 11,58 лакха инцидентов кибербезопасности было сообщено CERT-In. в 2020 году.

Министр также раскрыл результаты технического анализа кибератаки AIIMS Delhi. Чандрасекар сказал, что атаки были делом рук неизвестных злоумышленников и были вызваны неправильной сегментацией сети.

«Согласно анализу, серверы в сети информационных технологий AIIMS были скомпрометированы неизвестными злоумышленниками из-за неправильной сегментации сети, что привело к нарушению работы из-за нефункциональности критически важных приложений. CERT-In и другие заинтересованные стороны рекомендовали необходимые меры по исправлению положения в отношении того же самого», — отмечается в ответе.

В результате инцидента пострадало целых пять серверов AIIMS Delhi, и хакеры зашифровали 1,3 терабайта (ТБ) данных.

Главный медицинский институт страны стал объектом крупной кибератаки в ноябре прошлого года, которая парализовала работу важнейших объектов национальной инфраструктуры. В конце концов, дело о вымогательстве и кибертерроризме было зарегистрировано подразделением разведки и стратегических операций (IFSO) полиции Дели. Дело расследуют CERT-In, CBI, NIA и множество других агентств.

Отвечая на вопрос депутата Сушила Моди, Минпромторг также сообщил, что Секретариат Совета национальной безопасности (СНБ) уже сформулировал проект Национальной стратегии кибербезопасности, в котором будут решаться вопросы, связанные с безопасностью национального киберпространства.

Отметив, что оно «полностью осведомлено» о различных инцидентах в области кибербезопасности, правительство заявило, что оно приняло различные меры для «укрепления состояния кибербезопасности и пресечения инцидентов в области кибербезопасности».

Проблема цифровой безопасности

В то время как правительство заявило, что CERT-In отследил всего 13,91 миллиона инцидентов кибербезопасности в 2022 году, высокопоставленный руководитель Google в августе прошлого года оценил это число в 18 миллионов кибератак в день

В прошлом году хакеры из Индонезии и Малайзии также начали полномасштабную кибервойну против Индии после комментариев бывшего лидера БДП Нупура Шармы о пророке Мухаммеде во время телевизионных дебатов.

Согласно отчету, кибератаки на правительственные учреждения Индии увеличились более чем вдвое в 2022 году, поскольку страна стала наиболее часто подвергаемой атакам страной в мире в этом аспекте. Кроме того, несколько индийских агентств из Oil India Limited, Ladakh Power Grid, UIDAI и других агентств, как утверждается, неоднократно подвергались атакам за последние несколько лет.

Индийские агентства были легкой мишенью из-за слабых норм кибербезопасности и доступа к огромному массиву данных. Поскольку во многих случаях для защиты важных пользовательских данных развертывались нестандартные брандмауэры, в недавнем прошлом как государственные, так и негосударственные субъекты стремились использовать уязвимости в системе.

Хотя правительство утверждает, что добавило больше мер безопасности и усилило меры, еще неизвестно, насколько эффективны эти новые брандмауэры. Поскольку большинство отчетов указывают на более сложный год в сфере кибербезопасности для Индии, все внимание сейчас приковано к тому, насколько эффективно власти сдерживают такие атаки». ***(Chetan Thathoo. India Witnessed 13.9 Lakh Cybersecurity Incidents In 2022: Govt // Inc42 (https://inc42.com/buzz/india-witnessed-13-9-lakh-cybersecurity-incidents-in-2022-govt/). 11.02.2023).***

***

«ВМС Индии ищут автономный механизм обнаружения и устранения угроз на основе искусственного интеллекта для блокировки программ-вымогателей и атак нулевого дня. Об этом сообщило морское подразделение вооруженных сил Индии в заявлении о проблеме, опубликованном в рамках конкурса Defense India Startup Challenge (DISC).

Министерство обороны запустило челлендж, целью которого является поощрение стартапов, малого бизнеса и новаторов к созданию прототипов или коммерциализации решений в области национальной обороны и безопасности.

«Атаки программ-вымогателей представляют серьезную угрозу для облачных сервисов и способны заблокировать сервис с повреждением системных файлов или без такового. Кроме того, атаки нулевого дня могут использовать уязвимость в облачной службе до тех пор, пока уязвимость не будет обнаружена разработчиком и устранена», — говорится в заявлении военно-морского флота. «Решение должно предоставлять систему управления оповещениями на основе ИИ, которая может автоматически обнаруживать проблемные программы-вымогатели и атаки нулевого дня и помогать снижать нагрузку на аналитиков безопасности».

Данные Индийской группы реагирования на компьютерные чрезвычайные ситуации показали, что в 2022 году от атак программ-вымогателей пострадали 19 правительственных организаций. Всего CERT-In зафиксировал 198 атак программ-вымогателей, затронувших индийские компании, работающие в стране, в 2022 году. В 2021 году этот показатель составлял 111.

Помимо военно-морского флота, индийская армия и индийские ВВС опубликовали несколько заявлений о проблемах, связанных с наблюдением и кибербезопасностью, в рамках DSIC.

Индийская армия

Армия ищет платформу, которая может проводить оценку уязвимости и обнаружение порчи своих веб-сайтов, выходящих в Интернет. Веб-порча — это атака, при которой злоумышленники удаляют или изменяют контент на сайте, заменяя его своими сообщениями.

«Платформа должна сканировать веб-сайт на наличие нижеперечисленных проблем и генерировать отчет о выявленных уязвимостях, а также предлагать необходимые меры по их устранению. Кроме того, платформа должна иметь возможность сканировать мобильное приложение Android для обнаружения любой уязвимости или вредоносного контента», — говорится в заявлении армии.

Армия также ищет местный инструмент мониторинга социальных сетей для разведки и операций.

«Разработайте и внедрите платформу мониторинга социальных сетей на основе графического интерфейса пользователя (GUI) для определенного сканирования различных платформ социальных сетей, таких как Twitter, Facebook, Instagram, Discord и т. д.», — говорится в сообщении.

Воздушные силы

Индийские ВВС (IAF) ищут антивирусное решение, способное обрабатывать и идентифицировать сложные вредоносные программы. Ему также нужен подключаемый модуль для браузера, который может обнаруживать фишинговые письма и предпринимать соответствующие действия.

В настоящее время сеть защиты имеет воздушный разрыв или отключена от незащищенных сетей. Однако сотрудники всех трех служб используют Национальный центр информатики и другие службы электронной почты в личных и служебных целях, говорится в сообщении.

Это делает их уязвимыми для фишинговых атак, которые не нейтрализуются стандартными средствами безопасности (антивирусами/брандмауэрами).

«Предлагается создать браузерный плагин для Chrome и Firefox, способный обнаруживать фишинговые письма и предпринимать соответствующие действия», — говорится в описании задачи.

В другом заявлении о проблеме ВВС выдвинули требование к собственному программному обеспечению, чтобы избежать несанкционированного доступа к данным с интеллектуальных устройств. Он указал, что в таких странах, как Израиль, использование смартфонов в особо важных местах не запрещено.

«Для обеспечения аналогичной среды в МАФ предлагается спроектировать/разработать приложение, которое в обязательном порядке должно быть установлено на смартфоны отдельных лиц (всех, кто желает носить их в

учреждениях МАФ), и должно удовлетворять все потребности безопасности организации», — добавил он». ***(Aihik Sur. Indian defence services seek cyber-security, surveillance products // e-Eighteen.com Ltd. (https://www.moneycontrol.com/news/business/startup/indian-defence-services-seek-cyber-security-surveillance-products-10133471.html?utm_source=flipboard&utm_medium=referral&utm_campaign=flipboard-magazine). 21.02.2023).***

***

«Чтобы способствовать прозрачности и подотчетности в целях улучшения усилий по решению проблемы кибербезопасности, д-р Джимсон Олуфуйе призвал правительства африканских стран принять законы, требующие раскрытия информации о кибератаках и потерях юридических и физических лиц.

Олуфуйе, который был ведущим научным сотрудником Экономической комиссии Организации Объединенных Наций для Африки (ЭКА ООН) исследования кибербезопасности в целях развития в 4-й промышленной революции (4IR), рекомендовал это как часть своих выводов во время презентации результатов исследования на 17-й конференции. Форум по управлению Интернетом (IGF) прошел в Аддис-Абебе.

В рамках своей стратегии участия в кибербезопасности Экономическая комиссия для Африки (ЭКА) заказала исследование, чтобы подчеркнуть кибербезопасность как императивную движущую силу развития в 4IR.

Согласно Олуфуйе в заключении исследования, было также рекомендовано создать механизмы, облегчающие потерпевшим сообщение о таких случаях.

Приводя пример, он сказал, что веб-приложения могут упростить составление отчетов с помощью бесплатных советов по предотвращению будущих атак и восстановлению после потерь.

В своей презентации Олуфуйе подчеркнул положительную связь между кибербезопасностью и развитием в условиях четвертой промышленной революции. В отчет включены данные национальных регуляторов электросвязи, Платформы открытых данных Всемирного банка и Глобального индекса кибербезопасности МСЭ, среди прочего, за десятилетний период.

Результаты исследования, по словам Олуфуйе, выявили три ключевые рекомендации, в том числе необходимость стабильной и подотчетной национальной и организационной системы управления в течение длительного периода, чтобы кибербезопасность имела более тесную связь с развитием.

По его словам, было также рекомендовано принять законы, требующие раскрытия информации о кибератаках и потерях юридических и физических лиц, чтобы способствовать прозрачности и подотчетности в целях улучшения усилий по решению проблемы кибербезопасности.

По его словам, производители и поставщики оригинального оборудования по замыслу должны соблюдать принцип безопасности, чтобы гарантировать, что перед добавлением оборудования в производство оно должно как минимум запрашивать изменение кодов доступа по умолчанию.

Исследование, проведенное Цифровым центром ЕСА, показало положительную связь между кибербезопасностью и развитием. Соответственно, исследование показало, что повышение зрелости кибербезопасности на 10% приводит к увеличению ВВП на душу населения в Африке от 0,66% до 5,4%.

Было отмечено, что чем выше зрелость страны в области кибербезопасности, тем ниже финансовые потери в киберпространстве на душу населения. Данные по выборке из 40 африканских стран показали, что увеличение проникновения Интернета на 10% обеспечивает увеличение ВВП на душу населения в Африке на 1–8,2%.

В отчете также указано, что зрелость кибербезопасности в Африке составляет 29,1% по сравнению с Латинской Америкой и Азией/Ближним Востоком (35,6% и 61% соответственно).

Заместитель министра в Министерстве информационных и коммуникационных технологий Республики Намибия приветствовал отчет и дальнейшие усилия по сотрудничеству для получения большего количества данных по Африке для обеспечения принятия правильных решений.

Она добавила важность дальнейшего изучения гендерного аспекта исследования.

Жан-Поль Адам, директор по технологиям, управлению изменением климата и природными ресурсами в ЕСА, отметил важность этого исследования в том, чтобы «пролить больше света на кибербезопасность как на важнейшую основу программы развития потенциала кибербезопасности в Африке».

Мактар Сек, начальник отдела технологий и инноваций ЕСА, также указал на важность исследования, отметив, что «низкий уровень готовности Африки в области кибербезопасности обходится государствам-членам в среднем в 10% их ВВП».

Крист Пейнтер, президент Глобального форума киберэкспертизы (GFCE), высоко оценил усилия ЕСА и подчеркнул необходимость проведения дополнительных исследований, имеющих отношение к региону, и повышения осведомленности о кибербезопасности, чтобы помочь уменьшить киберпреступность». ***(Enact laws requiring disclosure of cyber-attacks, losses in corporate entities, Olufuye tells African govt // Vanguard Media Limited, Nigeria (https://www.vanguardngr.com/2023/02/enact-laws-requiring-disclosure-of-cyber-attacks-losses-in-corporate-entities-olufuye-tells-african-govt/). 04.02.2023).***

***

«Денежно-кредитное управление Бермудских островов опубликовало пересмотренный Кодекс поведения по управлению операционными киберрисками («Кодекс киберрисков») для поставщиков корпоративных услуг, трастовых компаний, компаний, предоставляющих денежные услуги, инвестиционных компаний, поставщиков услуг по управлению фондами,

банков и депозитных компаний от 26 сентября 2022 г. Все соответствующие юридические учреждения должны соблюдать Кодекс киберрисков к 15 февраля 2023 г.

Кодекс кибер-рисков требует, чтобы совет директоров и высшее руководство осуществляли надзор за кибер-рисками, а совет директоров не реже одного раза в год утверждал политику кибер-рисков. Каждое соответствующее юридическое учреждение также обязано назначить главного сотрудника по информационной безопасности для надзора и реализации его программы киберрисков и обеспечения соблюдения политик киберрисков». ***(Julie E. McLean, Jacari Brimmer-Landy. Bermuda Cyber Risk Code Compliance Deadline // Conyers Dill & Pearman (https://www.conyers.com/publications/view/bermuda-cyber-risk-code-compliance-deadline/). 02.2023).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«У неділю, 12 лютого, хакери держави-терориста атакували сайт Штабу спеціальних операцій НАТО (NSHQ). Речниця альянсу підтвердила інцидент і наголосила, що питання кібербезпеки зараз є основним пріоритетом відомства. Цікаво, що жодних офіційних заяв щодо злому на сторінках НАТО у соцмережах так і не опублікували.

Видання The Telegraph інформує, що хакери країни-окупанта також порушили комунікацію між НАТО і військовими літаками, які надають допомогу жертвам турецько-сирійського землетрусу, що забрав щонайменше 28 000 життів. У Killnet визнали свою причетність до DDoS-атак. «Ми завдаємо удари по НАТО», — це все, що написали у своєму Telegram-каналі кіберзлочинці у відповідь на чисельні реакції користувачів соцмереж.

Killnet — група прокремлівських злочинців, які прагнуть вивести з ладу військові та урядові сайти країн за допомогою кібератак. Хакери націлені на держави, які надають військову допомогу Україні у повномасштабній війні з росією. Зломи від російських програмістів зазвичай не завдають значної довготривалої шкоди. Щоправда, західні спецслужби припускають, що держава-терорист може нарощувати свій кіберпотенціал для масованої цифрової атаки у майбутньому.

Примітно, що торік у травні британська поліція заарештувала члена Killnet у Лондоні. У відповідь кіберзлочинці погрожували відключити апарати штучної вентиляції легень у британських лікарнях. У березні 2022 року, невдовзі після початку повномасштабної російської агресії на території нашої держави, Killnet опублікувала відео, на якому фігура в капюшоні зі спотвореним голосом закликала росіян «не тікати з країни, а підтримувати батьківщину».

Також Killnet намагалася завадити викривальницькій кібердіяльності хакерів з Anonymous, який атакував російські сайти й розповідав правду про звірства окупантів на території України. Killnet навіть вихвалялися, що вивели з ладу сервер Anonymous, щоправда, так цього й не довели…» ***(Російські хакери зламали сайт***

НАТО // No worries! (https://noworries.news/rosijski-hakery-zlamaly-sajt-nato/). 13.02.2023).

***

«Хакери Killnet порушили комунікацію між НАТО і літаком, який надавав допомогу жертвам турецько-сирійського землетрусу, що забрав понад 30 000 життів. Пілота попередили про збої в системі адресації та звітності авіаційних комунікацій (ACARS), яку використовують, зокрема, для передачі конфіденційної інформації. Як припускають в альянсі, збій був викликаний, вчорашньою DDoS-атакою на сайти НАТО.

Хоча контакт із літаком не втрачався, атака хакерів, за словами представників відомства, таки вплинула на доставляння гуманітарної допомоги…» ***(Хакери, які атакували сайт НАТО, змогли короткостроково пошкодити систему зв'язку для авіації // No worries! (https://noworries.news/hakery-yaki-atakuvaly-sajt-nato-zmogly-korotkostrokovo-poshkodyty-systemu-zvyazku-dlya-aviacziyi/). 14.02.2023).***

***

«Центр киберзащиты НАТО привлекает DISA в качестве руководителя американской группы для борьбы с интенсивными кибератаками

…Чтобы быстро определить потенциальную кибератаку, Соединенные Штаты совместно с нашими союзниками по НАТО проводят ежегодные учения, которые позволяют экспертам по кибербезопасности и ИТ повысить свои навыки защиты ИТ-систем и критической инфраструктуры от атак в реальном времени.

Locked Shields — это ежегодные учения, организуемые Центром передового опыта совместной киберзащиты НАТО (CCDCOE), которые считаются наиболее интенсивной проверкой навыков киберзащиты, интегрированных в оперативную и стратегическую среду, в ходе которых надежная, высококвалифицированная Красная команда CCDCOE противостоит 24 кибератакам. совместные синие команды по киберзащите…

CCDCOE выбрала Агентство оборонных информационных систем, чтобы возглавить команду США третий год подряд. В этой роли DISA будет помогать синей команде США, обеспечивать обучение, руководство и руководство на протяжении всего процесса планирования и проведения учений. Участие DISA в учениях согласуется с поддержкой агентством Стратегии национальной обороны, направленной на защиту родины и сдерживание стратегических атак против Соединенных Штатов, наших союзников и партнеров.

В этом году учения пройдут с 17 по 21 апреля. Американская группа будет работать в Оружейной палате Моргантауна в Моргантауне, Западная Вирджиния…» ***(NATO Cyber Defence Center Taps DISA as U.S. Team Lead for Intense Cyberattack Challenge // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/nato-cyber-defence-center-taps-disa-as-u-s-team-lead-for-intense-cyberattack-challenge/). 10.02.2023).***

***

«Останній рік бойових дій на території України став «засвоєним уроком» для демократичних держав усього світу, які намагаються зрозуміти, як надалі зможуть розвиватися не лише стратегії, а й технології. Фокус розповість, чого очікують військові аналітики, коли йдеться про збройні конфлікти в майбутньому.

Штучний інтелект і кібератаки — новий військовий тренд

ЗСУ широко використовували нові технології, які хоч і не впливали радикально на перебіг бойових дій, проте стали опорною точкою для відстеження тренду технологічного розвитку ВПК, пише у своїй колонці військовий аналітики Пітер Сінгер.

Перше, про що варто поговорити, — широке застосування штучного інтелекту (ШІ), а саме: програмне забезпечення для розпізнавання облич для ідентифікації російських солдатів, алгоритми машинного навчання (МН) для підвищення ефективності логістики військових і волонтерів, ведення розвідки, ведення інформаційної війни.

«Використання нейромереж різного функціоналу набиратиме обертів, оскільки ШІ вже сьогодні має велике значення для соціуму. Жодна інша область технологій сьогодні не фінансується так активно, як ШІ та МН. У розвитку нейромереж зацікавлені національні уряди і, як наслідок, їхні збройні сили, а також великий бізнес», — стверджує автор.

Другий важливий момент — кібербезпека також стала новим фронтом цієї війни. На початку конфлікту російські хакери намагалися атакувати різні українські мережеві системи — від електромереж до космічного зв'язку. Але, як і ЗС Росії, вони не досягли успіху. І тут автор бачить дві основні причини:

Путін не підготував ані військових, ані хакерів до війни, яку він планував.

Кіберзахисники України змогли впоратися з більшістю атак.

Кібербитва теж радикально не вплинула на хід війни, але уявімо, що могла б зробити в майбутньому група або військовий підрозділ, які були б більш організованими, підготовленими, мали б актуальні розвіддані й інструменти планування, що мають можливість атакувати таку велику ціль як інфраструктура всієї країни.

«Кібератаки — майбутнє війни. Ми все більше й більше залежимо від інтернету, від нього ж залежать і пристрої, які тепер управляють операціями майже в усіх галузях критичної інфраструктури. Отже, цілей для злому теж стає більше. Однак кібербезпеку надто часто відсувають на другий план. У результаті інтернет речей, на який ми все більше й більше покладаємося, стає дуже вразливим. І зловмисники користаються цим», — пише Сінгер.

Безпілотники: нове — добре забуте старе

БПЛА використовувалися під час Другої світової війни, в конфліктах в Афганістані й Іраку, Пакистані та Лівії. Але деякі військові експерти вважали, що безпілотники не такі вже й важливі у "звичайній" війні, маючи на увазі, що дрони гарні в точкових конфліктах із терористами та повстанцями.

«Ця академічна та військова суперечка закінчена. Безпілотні системи виявилися неймовірно важливими у бойових діях в Україні, у різних ролях і навіть областях. Вони відіграли вирішальну роль у зупинці колон російських танків, у забезпеченні високої точності українських артилерійських і ракетних ударів, на

морі, потопивши російський флагман «Москва», у завданні ударів по російських військово-морських базах у Криму», — наголошує експерт.

Безліч різних систем заповнили поле бою: і великі дорогі БПЛА військового рівня, і тисячі маленьких комерційних квадрокоптерів. І українські сили, і російські використовують дрони не лише для розвідки, а й для завдання ударів, коригування вогню. Завдяки інтеграції ШІ з безпілотниками ЗСУ все частіше розгортають автономні системи, використовуючи дрони і як баражуючі боєприпаси, що діють як поодинці, так і роєм.

«Бої дронів говорять про те, якими будуть конфлікти надалі та наскільки величезною буде роль безпілотних літальних апаратів у них», — резюмує фахівець.

Розвідка за відкритими даними та соцмережі, як зброя

Ще одна область, в якій технологія, що давно використовується, досягла нових висот у 2022 році, — використання соціальних мереж як зброя.

«Кібервійна має на увазі злом мереж, а от дипфейки — «злом» людей шляхом поширення інформації через лайки та репости", — йдеться в колонці. «У російсько-українському конфлікті інформаційна війна вийшла на новий рівень стратегічного значення».

Однією з важливих сторін інфойни стала розвідка на основі аналізу відкритих джерел (OSINT). Українці перетворили свої стільникові телефони та облікові записи в соціальних мережах на новий «інструмент шпигунства», збираючи інформацію по крихтах і передаючи її військовим, ЗМІ.

Завдяки OSINT світ дізнався, що Путін брехав, коли говорив про те, що Росія просто реагувала на надзвичайну ситуацію, а не планувала вторгнення, що в результаті підірвало його політичну стратегію. Зі свого боку, ЗСУ брали дані OSINT буквально в тисяч місцевих жителів і російських солдатів-невдах, які знімають тік-токи та видають своє місце розташування, щоб відстежувати дії російських військових.

Поширення інформації про те, що відбувається в Україні, буквально в режимі реального часу, мало величезний уплив на іноземну аудиторію. Симпатія до українського народу змінила політичний контекст і пріоритети від США до Японії та Австралії. Полеміка останніх місяців щодо відправлення Німеччиною танків Україні (що врешті-решт і сталося знову ж таки через зміну ставлення до українців) показує, що знадобився рік, щоб «перекроїти» зовнішню політику Німеччини, яку вона мала 75 років.

Економічна війна та роль у ній IT-компаній

Розв'язана Росією вона проти України мала й потужний економічний ефект. Близько 400 із 500 провідних компаній світу пішли з російського ринку (серед яких — велика кількість IT-корпорацій), і не тому, що того вимагали закон чи санкції, а тому, що мати бізнес у Росії означає мати погану репутацію. Такого роду новий вид "геополітичної скасування" в довгостроковій перспективі вплине як на російську економіку, так і на те, що інші країни думають про свою економіку під час війни. І це може бути одним із найзначніших наслідків воєн майбутнього, упевнений автор.

За даними МВФ, перший великий конвенційний конфлікт XXI століття в Європі стався між 9-ю та 56-ю за величиною економіками світу. Руйнування були колосальними: від енергетичних ринків до ланцюжків постачань, не тільки для

самих комбатантів, але й для всього світу. Росія відчула ефект на собі, коли була змушена вилучати мікрочипи зі старих холодильників і пральних машин, призупинити розгортання не тільки 5G-, а й 4G-мереж, уповільнити мобільний трафік, залишитися без оновлення різного ПЗ, без якісних гаджетів і побутової електроніки.

«І у Вашингтоні, і в Пекіні тепер мають переосмислити зв'язки між національною та економічною безпекою і те, як на них впливають війни», — наголошує Сінгер.

Українська держава та суспільство не впали в перші дні боїв, як сподівався Кремль. Згідно зі соцопитуваннями, 70% українців вважають, що ЗСУ виграють війну, попри меншу чисельність техніки та живої сили, порівнюючи зі ЗС РФ.

«На війні людська воля має значення, і цифрова сфера виявилася цінним новим засобом досягнення та мобілізації цієї волі», — резюмував автор». ***(Ірина Рефагі. Дрони, ШІ, кібератаки: які уроки засвоїв світ через рік війни в Україні // Фокус (https://focus.ua/uk/digital/551836-drony-ii-kiberataki-kakie-uroki-izvlek-mir-spustya-god-voyny-v-ukraine). 25.02.2023).***

***

«Американский компьютерный гигант Microsoft заявил в пятницу, что идентифицировал иранских государственных деятелей как стоящих за недавней кибератакой на французскую сатирическую газету Charlie Hebdo.

Клинт Уоттс, генеральный менеджер Центра анализа цифровых угроз Microsoft, заявил, что хакеры, называющие себя «Святые души», были иранской фирмой по кибербезопасности Emennet Pasargad, сообщает AFP.

В начале января Holy Souls объявили, что получили личную информацию более чем 200 000 клиентов Charlie Hebdo, и опубликовали образец данных в качестве доказательства.

Кибератака произошла после того, как Charlie Hebdo опубликовала карикатуры на верховного лидера Ирана Али Хаменеи в специальном выпуске, приуроченном к годовщине нападения на его парижские офисы в 2015 году, в результате которого погибли 12 человек.

Иран сделал официальное предупреждение Франции за «оскорбительные и непристойные» карикатуры.

Эменнет Пасаргад был работодателем двух иранцев, Мохаммада Хосейна Мусы Каземи и Саджада Кашиана, которым министерство юстиции США предъявило обвинения в ноябре 2021 года.

Они якобы провели киберкампанию, «чтобы запугать и повлиять на американских избирателей, а также иным образом подорвать доверие избирателей и посеять раздор» во время президентских выборов в США в 2020 году.

Каземи и Кашиан якобы получили конфиденциальную информацию об избирателях и рассылали электронные письма с угрозами, распространяя ложную информацию, чтобы повлиять на избирателей как демократов, так и республиканцев, а также пытались взломать веб-сайты, связанные с голосованием в штатах, заявило ведомство.

Хакеры Charlie Hebdo, чью операцию Microsoft назвала «Neptunium», предложили украденную базу данных подписчиков для продажи в Интернете за 20 биткойнов, что в настоящее время составляет около 460 000 долларов, сообщила Microsoft.

«Что бы вы ни думали о выборе редакции Charlie Hebdo, раскрытие личной информации о десятках тысяч ее клиентов представляет собой серьезную угрозу», — заявили в Microsoft». ***(Microsoft Says Iranians Hacked France's Charlie Hebdo // H H Saudi Research and Marketing LTD (https://english.aawsat.com/home/article/4136981/microsoft-says-iranians-hacked-frances-charlie-hebdo). 04.02.2023).***

***

«Израиль создает «Железный купол» в киберпространстве для борьбы с ростом числа кибератак со стороны враждебных иностранных правительств, заявил на этой неделе премьер-министр Биньямин Нетаньяху.

«Кибервойна находится в зачаточном состоянии», — сказал он, выступая по видеосвязи на конференции Cybertech Global 2023 в Тель-Авиве.

Он сказал, что ЦАХАЛ строит в Беэр-Шеве школу компьютерных наук, а специальное подразделение будет обучать около 20 000 молодых людей в области кибербезопасности.

Мероприятие собрало мировых киберлидеров, в нем приняли участие почти 20 000 человек из 86 стран.

Среди них был бывший директор ЦРУ Дэвид Петреус, который сказал JC, что мир должен быть очень обеспокоен киберугрозами, хотя в этой области были достигнуты «большие успехи», сославшись на войну в Украине.

Он сказал: «Россия бросила все на Украину, а также на Соединенные Штаты и некоторые другие западные страны в начале вторжения, но Украина оказалась гораздо более стойкой и способной, то же самое можно сказать и о США.

«Но это был успех не только государственных органов и возможностей, но и тех, кто работает в отрасли. Microsoft, например, сыграла очень важную роль, что неудивительно, учитывая их вездесущий характер с точки зрения продуктов, которые у них есть.

— Это не значит, что мы можем ослабить бдительность. Угроза продолжает развиваться и становится все более дьявольски умной. Атаки продолжаются ежедневно. Вы видите впечатляющую реакцию правительств. Великобритания с ее национальным центром кибербезопасности действительно была впереди планеты всей».

Он описал Израиль как один из величайших технологических центров во всем мире, который находится в процессе «превращения из страны стартапов в страну масштабирования».
Петреус, который был директором ЦРУ с 2011 по 2012 год, назвал технологическую отрасль в Израиле «выдающейся».

Он продолжил: «Многие из нас приходят сюда, чтобы посмотреть, что представляют собой новые стартапы, и определить те, с которыми мы можем сотрудничать».

Трехдневная конференция стала первым случаем, когда на одной сцене собрались правительственные киберруководители из Израиля, США, ОАЭ, Марокко и Бахрейна. Они сказали, что новое сотрудничество между странами стало началом вновь обретенного доверия.

На конференции также были представлены доклады о предпринимательстве и инвестициях в киберпространство в свете глобальной рецессии; войны будущего на фоне постоянного роста кибервойн; фейковые новости и искусственный интеллект в киберпространстве; и кибер-разработки в области интеллектуального транспорта, здравоохранения, авиации и финансовых технологий.

Министр экономики Нир Баркат, который сам был успешным предпринимателем в сфере высоких технологий до того, как занялся политикой, обратился к вопросу о недавнем протесте работников сферы высоких технологий против предложенной правительством реформы Верховного суда.

«Мы должны отделить экономику от политики», — сказал он. «Здесь идет оживленная дискуссия и выводы о том, что еще не произошло и все еще происходит. Я не вижу эффекта от предлагаемых изменений, потому что инвесторам интересны лучшие предприниматели, лучшие идеи и лучшие решения. Это то, что ими движет».

Говоря о следующих проблемах израильских высоких технологий, г-н Баркат добавил: «Мы должны инвестировать в предпринимателей и прислушиваться к тому, что они говорят.

«Наша главная задача — помочь им выйти на дополнительные рынки. Сегодня киберпространство есть во всех сферах, и наша цель — помочь сделать израильское предпринимательство доступным для всех сфер мира на глобальном уровне.

«Еще одним аспектом является участие в образовании. Нам необходимо сделать знания и технологическое предпринимательство доступными для молодежи».

Основатель Cybertech Амир Рапапорт сказал:

«Беспрецедентное количество участников отражает массовый рост киберпространства с января 2020 года». ***(Natalie Lisbona. Netanyahu: Israel is creating an Iron Dome in cyberspace // The Jewish Chronicle (https://www.thejc.com/news/world/netanyahu-israel-is-creating-an-iron-dome-in-cyberspace-4vL16QvZPa3VLxdhwI0dFP). 02.02.2023).***

***

«Дания во вторник повысила уровень предупреждения о кибербезопасности со «среднего» до «высокого» после нескольких атак пророссийских хакерских групп в последние недели, сообщил Центр кибербезопасности страны.

«Уровень риска повышается на фоне высокой активности пророссийских кибератывистов, которые проводят множество атак на цели в широком диапазоне стран НАТО», — говорится в сообщении центра.

Веб-сайты нескольких учреждений и компаний в Дании, включая центральный банк, коммерческие банки, министерства и военные, в прошлом

месяце все чаще становились мишенью так называемых распределенных отказов в обслуживании (DDoS), которые направляют трафик на целевые серверы в заявка на то, чтобы выбить их из сети.

Пророссийские хакерские группы в Telegram взяли на себя ответственность за некоторые недавние атаки на датские учреждения. Москва последовательно отрицает, что проводит хакерские операции.

Хакеры стали лучше планировать и проводить свои атаки, что придало им больше «поражающей силы», заявили в центре, добавив, что ожидают увидеть больше таких атак в будущем.

Хакеры «движимы идеологическими или политическими мотивами», что увеличивает вероятность атак в ответ на отдельные инциденты, такие как сожжение Корана перед посольствами Турции в Стокгольме и Копенгагене, говорится в сообщении центра». ***(Denmark Raises Cyber Security Alert Level After Attacks From Russian Hacker Groups // Wells Media Group, Inc. (https://www.insurancejournal.com/news/international/2023/02/01/705555.htm). 01.02.2023).***

***

«Серия инцидентов за последние три месяца вызвала обеспокоенность Тайваня по поводу безопасности данных. Особую тревогу вызывает возможность того, что конфиденциальная информация о тайваньской общественности, в том числе о высокопоставленных членах тайваньского правительства, попадет в руки китайского правительства.

В конце декабря появились новости о предполагаемой утечке информации о регистрации домохозяйств почти всех тайваньских граждан. Данные продавались на веб-сайте BreachedForum и включали 23,57 миллиона единиц информации, которые, по-видимому, были украдены из Департамента регистрации домашних хозяйств Министерства внутренних дел.

Чтобы доказать ее подлинность, в качестве образца были просмотрены 200 000 фрагментов информации. Это включало информацию о резиденциях вице-президента Уильяма Лая, генерального секретаря Совета национальной безопасности Веллингтона Ку и министра экономики Ван Мэй-хуа. Особое беспокойство вызывает то, что считается, что эта информация, вероятно, окажется в руках китайского правительства.

Информатор, который передал информацию Taiwan People News (民報), заявил, что информация была просочилась в даркнет в мае 2020 года хакером TooGod. Предположительно, информация относится к 2019 году. С 2020 года поступали сообщения об утечке более 20 миллионов регистраций домохозяйств, хотя неясно, действительно ли имела место утечка данных. В ответ на утечку в МВД заявили, что информация устарела, так как в ней используется система форматирования, которой больше нет.

Учетная запись, которая продавала данные на BreachedForum, также продавала 1,68 миллиона единиц информации с Тайваньской фондовой биржи и 28,11 миллиона единиц информации из Бюро страхования труда.

В то же время, в январе, общественность возмутилась после того, как стало известно, что прокуратура ведет расследование в отношении трех бывших сотрудников Национальной администрации медицинского страхования (NHIA) по обвинению в утечке данных из системы национального медицинского страхования Тайваня (NHI) в Китай. Было обнаружено, что два сотрудника NHIA по фамилии Се и Ли провели поиск в 133 000 и 35 000 записей соответственно, при этом Се провел поиск более 100 000 записей в 2018 году. Предположительно просочились данные за период с 2009 по 2022 год.

NHIA заявило, что не нашло никаких доказательств того, что обвиняемые сотрудники хранили данные и что они получали доступ к данным в рамках статистического исследования.

После сообщений Mirror Media (鏡週刊) о том, что у бывшего главного секретаря NHIA Е Фэн-мина, возможно, был 1 миллиард тайваньских долларов на зарубежных счетах, в СМИ появились слухи о том, что Йе работал в сговоре с Се и Ли, чтобы продать эти данные Китаю в течение 13 лет., что может привести к краже данных сотрудников национальной безопасности.

Депутаты Демократической прогрессивной партии (ДПП), такие как Мишель Линь и Лю Ши-фан, предположили, что Китай стремится развивать связи между персоналом NHIA посредством обменов по обе стороны пролива. Оба законодателя раскритиковали NHIA за неспособность успокоить общественность.

Опасения по поводу возможной утечки данных NHIA, вероятно, повлияют на будущие научные исследования с использованием государственных данных о здравоохранении. Исследовательский проект Института биомедицинских наук Academia Sinica по сопоставлению пациентов с лекарствами на основе генетической информации, в котором используется генетическая информация 600 000 пациентов, был раскритикован законодателем DPP Хуан Го-шу в начале этого месяца за потенциальное нарушение Закона об управлении биобанками человека. Помимо опасений по поводу наличия у пациентов достаточных механизмов отказа, чтобы избежать нарушения их прав на неприкосновенность частной жизни, вероятно, есть опасения, что эта информация может оказаться в руках Пекина. Сообщается, что китайское правительство собирает генетическую информацию об уйгурах, тибетцах и других этнических меньшинствах.

Утечки данных затронули и частный сектор. База данных службы проката автомобилей iRent, содержащая личную информацию 140 000 человек, оказалась доступной в Интернете. Информация включала имя, домашний адрес, адрес электронной почты, номер мобильного телефона, фотографию водительских прав и частично отредактированную информацию о кредитных картах пользователей iRent.

Информация хранилась на облачном сервере, принадлежащем оператору iRent Hotai Motor Company, без защиты паролем и была доступна только по IP-адресу. У iRent около 1,4 миллиона пользователей.

О небезопасном сервере впервые сообщило американское издание TechCrunch. TechCrunch сначала попытался сообщить Hotai о незащищенной базе данных, но не получил ответа. Однако после того, как TechCrunch связался с

Министерством цифровых дел, министерство приняло меры, чтобы запретить доступ к базе данных.

iRent заявила, что компенсирует 400 000 пользователей, которые зарегистрировались в службе с момента начала использования незащищенной базы данных, бесплатными часами. Тем не менее, городские власти Тайбэя оштрафовали компанию на 90 000 тайваньских долларов, а Министерство транспорта и коммуникаций оштрафовало iRent еще на 200 000 тайваньских долларов.

Позже другой сервис по аренде автомобилей, Car-Plus, был обвинен депутатом New Power Party Чиу Сянь-чжи в том, что в его приложении есть незащищенные данные, позволяющие получить доступ к данным транзакций. Car-Plus заявила, что с тех пор уведомила 16 000 пользователей своего приложения об утечке данных.

После инцидента законодатели DPP призвали правительство создать государственный орган по безопасности данных. Большинство призывов к созданию этой организации были вызваны скандалом с iRent, а не утечкой информации о регистрации домохозяйства или информации о медицинском страховании. О скандале с iRent сообщалось сравнительно больше, чем о двух других скандалах.

В то же время за последние два месяца было несколько случаев, связанных с опасениями по поводу потенциальных утечек данных с участием компаний, обвиняемых в связях с Китаем, в частности компаний, базирующихся в Сингапуре.

Один случай связан с Bondee, приложением для социальных сетей, которое позволяет пользователям создавать виртуальные аватары и чаты, где они могут общаться с 50 своими друзьями. Бонди быстро завоевал популярность среди дизайнеров, музыкантов и других творческих кругов.

Однако были высказаны опасения по поводу сходства Bondee с китайским приложением для социальных сетей Jelly (啫喱). Похоже, это было то же самое приложение, но с другим названием, хотя Bondee была зарегистрирована как сингапурская компания. Кроме того, пользователи отметили, что в пользовательском соглашении Bondee Тайвань упоминается как часть Китая, что было необычно.

Jelly превзошел WeChat как самое загружаемое приложение в китайской экосистеме приложений в январе 2022 года. Но к февралю 2022 года Jelly был удален из китайской экосистемы приложений после того, как пользователи сообщили о спам-звонках и случаях мошенничества после регистрации. Опасения заключались в том, что Bondee было тем же самым китайским приложением, стремящимся выйти на тайваньский рынок после того, как его вытеснили из Китая из-за утечки личной информации пользователей.

Аналогичные опасения были высказаны в отношении платформы электронной коммерции Shopee, которая в настоящее время управляет несколькими обычными магазинами на Тайване. Как и Bondee, Shopee — сингапурская компания, но ее обвиняют в тесных связях с Китаем, учитывая китайские инвестиции в компанию. Tencent Holdings владела 39,7% Shopee, когда ее тайваньское предприятие было зарегистрировано в 2015 году, хотя ее текущая доля сейчас составляет 18,7%.

Тайваньские регулирующие органы подверглись критике со стороны групп гражданского общества, таких как Союз экономической демократии (EDU), за то, что они проявили слабость к Shopee после трех отключений сети, обвиненных в компрометации информации тайваньских пользователей — не говоря уже о том, что Shopee уже является одним из электронных торговых площадок на Тайване с наибольшим количеством случаев мошенничества. По данным EDU, это произошло, несмотря на штрафы, наложенные на тайваньские компании за аналогичные отключения сети. В противном случае Shopee обвиняют в недобросовестной деловой практике, направленной на то, чтобы закрепиться на тайваньском рынке, например, изначально не взимать плату за доставку, но затем существенно повысить ее, а также в том, что ей разрешено работать на тайваньском рынке без поддержки лицензированного учреждения. Комиссией финансового надзора.

Недавние инциденты вызывают вопросы о безопасности данных как в государственном, так и в частном секторах Тайваня. В контексте Тайваня уровень опасений по поводу утечек или утечек данных связан с возможностью того, что конфиденциальная информация окажется в руках китайского правительства. Еще неизвестно, предпримут ли администрация Цая согласованные действия по таким вопросам». ***(Brian Hioe. Mass Data Leaks Sound Alarm About Taiwan's Cybersecurity // Diplomat Media Inc. (https://thediplomat.com/2023/02/mass-data-leaks-sound-alarm-about-taiwans-cybersecurity/). 15.02.2023).***

***

«В четверг высокопоставленный чиновник ФБР предупредил государственных чиновников об угрозе, которую китайские хакеры представляют для безопасности американских штатов, и о потенциальном росте киберактивности Китая в 2023 году.

Заместитель помощника директора киберподразделения Синтия Кайзер заявила на конференции Национальной ассоциации государственных секретарей в Вашингтоне, округ Колумбия, что «мы можем увидеть более значительную киберактивность Китая против ваших штатов в следующем году», — сообщает CNN.

Кайзер также признал, что российские киберсубъекты представляют сравнимую угрозу безопасности, но указал, что разведданных, предполагающих, что Москва намерена активизировать свои собственные усилия против США на государственном уровне, немного.

«У нас нет никаких разведывательных данных о том, что Россия пытается атаковать государственные и местные или избирательные системы более непосредственно, чем раньше. Но мы, безусловно, знаем о … возможности и у нас очень низкий порог для обмена этой информацией», — сказала она.

Пристальное внимание к китайскому шпионажу и киберусилиям приковано к недавним последствиям, связанным с полетом предполагаемого китайского воздушного шара-шпиона над Соединенными Штатами, прежде чем военные сбили его у побережья Каролины.

Китай отрицает наличие обширной хакерской программы, которая, по утверждению Вашингтона, затмевает программы других стран». ***(Ben Whedon. FBI warns states of threat posed by Chinese hackers // Bentley Media Group, LLC (https://justthenews.com/government/federal-agencies/fbi-warns-states-threat-posed-chinese-hackers?utm_source=flipboard.com&utm_medium=news-app&utm_campaign=external-news-aggregators). 16.02.2023).***

***

«Кибератака, похоже, взломала сеть, принадлежащую Федеральному бюро расследований (ФБР).

Как сообщает CNN (opens in new tab) со ссылкой на два источника, проинформированных по этому поводу, пока еще неизвестный злоумышленник взломал компьютерную систему полевого офиса в Нью-Йорке, используемую ФБР для расследования случаев сексуальной эксплуатации детей.

«ФБР известно об инциденте и работает над получением дополнительной информации», — говорится в заявлении правоохранительных органов США для СМИ. «Это единичный инцидент, который удалось локализовать. Поскольку это продолжающееся расследование, у ФБР пока нет комментариев».

Это не первый раз, когда ФБР приходится бороться с кибератакой в собственной сети. В конце 2021 года злоумышленнику удалось взломать почтовый ящик агентства (откроется в новой вкладке) и рассылать спам-сообщения.

В то время BleepingComputer (открывается в новой вкладке) отметил, что «десятки тысяч» спам-сообщений были отправлены волнами с адреса eims@ic.fbi.gov и что сообщения достигли не менее 100 000 почтовых ящиков.

Тем не менее, он отметил предположение некоммерческой организации SpamHaus, занимающейся отслеживанием спама, о том, что эти цифры были довольно консервативными и что охват был «потенциально намного, намного больше».

Будучи правительственным учреждением, ФБР сталкивается с постоянным шквалом кибератак. Государственные организации сегодня являются одними из самых целевых фирм в мире, наряду с телекоммуникационными фирмами, организациями здравоохранения и индустрией образования и обучения.

Злоумышленники могут атаковать эти организации с помощью спам-сообщений электронной почты, содержащих вредоносное ПО во вложениях или предлагающих фишинговые ссылки, по которым жертвы выдают свои учетные данные для входа и другую конфиденциальную информацию, которая может быть использована на втором этапе атаки». ***(Sead Fadilpašić. The FBI might have suffered a cyberattack // Future US, Inc. (https://www.techradar.com/news/the-fbi-might-have-suffered-a-cyberattack). 20.02.2023).***

***

«В четверг высокопоставленные чиновники штатов по вопросам выборов и кибербезопасности предупредили об угрозах, исходящих от России и других иностранных противников в преддверии выборов 2024 года, отметив,

что децентрализованная система Америки, состоящая из тысяч местных избирательных участков, создает особую уязвимость.

Россия и Иран вмешивались в предыдущие выборы, в том числе пытались подключиться к подключенным к Интернету электронным базам данных избирателей. Отвлеченные войной и протестами, ни одна из стран, похоже, не сорвала прошлогодние промежуточные выборы, но представители службы безопасности заявили, что ожидают, что противники США будут более активны по мере приближения сезона следующих президентских выборов. До первых праймериз осталось меньше года.

Джен Истерли, директор Федерального агентства по кибербезопасности и безопасности инфраструктуры, сослалась на нападение России на Украину и усилия США по поставке оружия и другой помощи осажденной стране в качестве возможного мотива. Она сказала, что агентство «очень обеспокоено возможным ответным ударом со стороны России в отношении нашей критически важной инфраструктуры».

Она также упомянула Китай как возможный источник вмешательства в выборы, тем более что отношения между двумя странами ухудшились, в основном в последнее время из-за предполагаемого воздушного шара-шпиона, который пролетел над страной, прежде чем был сбит американским истребителем…

Особую озабоченность вызывает децентрализованный характер избирательной системы Америки. По данным Национальной конференции законодательных собраний штатов, в США насчитывается около 10 000 местных избирательных участков, включая округа и поселки.

Не у всех из них есть финансирование для нового оборудования, надлежащего укомплектования штатов или обновленного обучения избирательных работников. Истерли сказала, что приоритетом ее агентства было получение денег и опыта для тех, кого она назвала «целевыми богатыми, кибер-бедными» организациями.

Меган Вульф, администратор Избирательной комиссии Висконсина, сказала, что в ее штате около 1850 местных чиновников проводят выборы, что затрудняет эффективное распределение федеральных денег в долгосрочной перспективе. Висконсин — это вечный колеблющийся штат, где четыре из шести последних президентских гонок были решены менее чем на процентный пункт, а предвыборные заговоры нашли благодатную почву после выборов 2020 года.

«Часто, если вы не видите ничего плохого в сфере кибербезопасности, об этом как бы забывают», — сказал Вулф, который также является президентом Национальной ассоциации государственных избирательных комиссий. «Люди не помнят, что это реальная и неминуемая угроза, и поэтому заставить эти местные юрисдикции, их руководящие органы действительно поверить в эту концепцию и поддержать устойчивые решения для местных избирательных юрисдикций, также по-прежнему остается реальной проблемой».

Несколько государственных секретарей призвали к дополнительному федеральному финансированию местных избирательных комиссий, которые не только должны быть готовы к угрозам кибербезопасности, но и сталкиваться с преследованием и угрозами с 2020 года.

Государственный секретарь штата Аризона Адриан Фонтес отметил, что сотрудники избирательных комиссий и даже избиратели в самом густонаселенном округе его штата, Марикопе, подвергались преследованиям и запугиванию.

Стивен Сполдинг, политический директор комитета Сената США по правилам и администрации, сказал, что председатель комитета, сенатор-демократ Эми Клобушар, пытается получить больше финансирования для выборов после неудачной попытки в конце прошлого года. Конгресс выделил штатам 75 миллионов долларов в виде грантов на обеспечение безопасности выборов, но этого было намного меньше, чем просили многие государственные и местные чиновники.

«На наш взгляд, явно необходимо более 75 миллионов долларов из прошлогоднего омнибуса», — сказал Сполдинг. «Мы неоднократно слышали о том, что устойчивое финансирование обеспечивает бесперебойное проведение наших выборов, способствует предсказуемости и планированию, и мы стремимся работать на двухпартийной основе, чтобы добиться этого». ***(Ayanna Alexander. Security experts warn of foreign cyber threat to 2024 elections // The Columbian (https://www.columbian.com/news/2023/feb/16/security-experts-warn-of-foreign-cyber-threat-to-2024-elections/). 16.02.2023).***

***

Кіберзахист критичної інфраструктури

«По словам Андреа Пениш, аналитика Dryad Global, для регионов, не затронутых конфликтами или горячими точками пиратства, кибербезопасность является основным риском для безопасности.

«Важно, однако, что это в основном связано с отсутствием физической угрозы со стороны воюющих или преступных субъектов, а не с большей известностью киберугроз», — сказал Пениш Rigzone.

По словам аналитика, больший риск для многих морских нефтяных вышек представляет физическая угроза. Пениш, однако, отметил, что «хотя эти физические угрозы представляют собой основную угрозу, с которой приходится бороться оффшорной нефти, кибербезопасность занимает второстепенное место в соображениях безопасности».

Аналитик Dryad Global подчеркнул, что морские нефтегазовые буровые установки в основном используют тот же Интернет, что и все остальные, для обеспечения связи. Безопасность этого соединения «чрезвычайно важна, но не обязательно больше, чем у кого-либо еще», — подчеркнул Пениш.

«Важно то, как у них настроены бортовые системы. Есть ли у кого-то доступ за пределами буровой установки к механическим операциям буровой установки, которые могут вызвать экологическую катастрофу (т.е. доступ к буровому механизму)?», - сказал Пениш.

«Эта доступность зависит от того, как связаны их различные кибераспекты; механические функции, связь, информационные системы», — добавил Пениш.

«Однако кибератака, получающая контроль над буровыми механизмами с целью манипулирования бурением, является скорее террористической или государственной угрозой, чем угрозой, исходящей от обычных хакеров», — продолжил аналитик.

Пениш отметил, что регулярные кибератаки с большей вероятностью будут либо искать информацию, либо удерживать системы с целью получения выкупа, поскольку их намерения обычно ограничиваются получением денег, а их возможности также ограничены более простыми системами для получения выкупа.

«Если эти механические системы будут взломаны, существует вероятность получения выкупа, но их очень сложно вернуть в сеть», — сказал Пениш.

По словам Пенише, количество атак на буровые установки «с террористическими намерениями» остается низким.

«Атака кибербезопасности на буровые механизмы… вероятно, вызовет серьезную экологическую катастрофу, которая поразит не только буровую компанию, но, вероятно, также повлечет за собой серьезные последствия для государств», — сказал Пениш.

«По этой причине в краткосрочной и среднесрочной перспективе этот тип кибератаки менее вероятен, чем атаки на обычные компьютерные системы и средства связи», — добавил Пениш». ***(Andreas Exarheas. How Critical Is Cyber Security for Offshore Oil and Gas Installations? // Rigzone.com, Inc. (https://www.rigzone.com/news/how_critical_is_cyber_security_for_offshore_oil_and_gas_installations-08-feb-2023-172008-article/). 08.02.2023).***

***

Кіберзахист закладів охорони здоров'я

«Десятилетия консолидации больниц превратили местные общественные больницы в аномалии. Здание и название могут быть такими же, но больница, скорее всего, теперь принадлежит системе здравоохранения, заботящейся о затратах, которая обслуживает обширную географию.

В разгар новой пандемии коронавируса количество слияний и поглощений в секторе здравоохранения резко сократилось, но теперь, похоже, они медленно восстанавливаются.

Эта продолжающаяся волна концентрации рынка имеет хорошо известные последствия: рост цен, снижение качества медицинской помощи и возможное несоответствие между медицинскими потребностями местного населения и доступной медицинской помощью.

Одним из наиболее часто упускаемых из виду последствий слияний является вероятность новых утечек данных пациентов. Слияние больниц не просто объединяет клиники. Они также объединяют свои базовые ИТ-системы. Насколько хорошо обслуживаются и защищены многие из этих систем, в первую очередь, варьируется. Объединение их вместе создает сеть, самое слабое звено которой может вызвать инцидент с утечкой данных, последствия которого ощущаются далеко за пределами местного населения больницы. Данные пациентов в одном

штате могут быть раскрыты из-за инцидента со взломом, произошедшего в больнице в трех штатах.

Это может иметь место в случае инцидента с программами-вымогателями прошлой осенью, связанного с сетью католических больниц CommonSpirit в Чикаго, которая является продуктом слияния в 2019 году компаний «Католические инициативы в области здравоохранения» и Dignity Health. CommonSpirit снова расширился в 2021 году за счет приобретения Virginia Mason Franciscan Health в штате Вашингтон.

CommonSpirit сообщил властям, что инцидент вызвал утечку данных, затронувшую более полумиллиона пациентов в Вашингтоне, но последствия атаки программы-вымогателя, по-видимому, ощущались в мегасистеме из 140 больниц, работающих в 21 штате.

Истцы в предлагаемых коллективных исках, поданных против CommonSpirit, утверждают, что число пострадавших может исчисляться десятками миллионов.

Пострадавшие больницы включают MercyOne в Де-Мойне, штат Айова, которая ранее принадлежала CommonSpirit и Trinity Health в Мичигане, прежде чем была приобретена Trinity Health в прошлом году. Во время инцидента с программой-вымогателем MercyOne все еще использовала ИТ-системы CommonSpirit, а доступ к электронным медицинским картам медицинского центра Айовы и другие функции приложений были недоступны в течение нескольких недель после инцидента с программой-вымогателем.

По словам экспертов, такие инциденты, как атака программы-вымогателя CommonSpirit, подчеркивают исключительную важность для организаций тщательной оценки и устранения потенциальных рисков ИТ-безопасности, связанных с возможным слиянием или поглощением.

«Мы видим, что хорошо зарекомендовавшие себя системы здравоохранения или организации, имеющие очень зрелые программы кибербезопасности, берут на себя менее защищенную организацию», — говорит Джон Ригги, национальный советник по кибербезопасности и рискам Американской ассоциации больниц.

Ассоциация рекомендует при слиянии больниц относиться к киберрискам с таким же приоритетом, как к финансовому анализу при слиянии.

Но определение и идентификация массива систем и множества устройств, используемых другой приобретаемой организацией здравоохранения, непроста.

«Когда вы покупаете организацию, вы, как правило, не знаете всего, что покупаете», — говорит Кэти Хьюз, директор по информационным технологиям компании Northwell Health, расположенной в Нью-Йорке, которая имеет 21 больницу и более 550 амбулаторных учреждений, многие из которых были приобретены организация, которая является результатом слияния в 1997 году между North Shore Health System и Еврейским медицинским центром Лонг-Айленда.

Процесс слияния не позволяет обеим сторонам задавать слишком много вопросов о состоянии кибербезопасности другой стороны, особенно о рисках, связанных с третьими сторонами.

В наши дни любой крупный поставщик медицинских услуг полагается на деловых партнеров и других поставщиков, и эти отношения держатся в

строжайшем секрете, говорит Ван Стил, руководитель отдела информационной безопасности в сфере здравоохранения в консалтинговой фирме LBMC Information Security.

По его словам, немногие из продавцов, как правило, даже знают, что рассматривается сделка по слиянию и поглощению. «Поэтому мы не можем просто позвонить их ИТ-менеджеру или директору по информационной безопасности и сказать: «Расскажите мне все о вашей структуре безопасности и списке поставщиков, обо всех ваших связях, методах и тому подобном», потому что мы с ними пока нельзя даже разговаривать, потому что сделка еще не заключена».

Покупающая организация здравоохранения может запросить доказательства того, что продавец провел внутреннюю оценку рисков в соответствии с требованиями HIPAA. «Много раз они этого не делали, но, надеюсь, сделали», — говорит Стил.

Покупатель должен «задавать те же вопросы, которые вы задаете стороннему поставщику, об их мерах безопасности, практиках, понимании инвентаризации используемых систем, любых предыдущих взломах, сборе этой информации», — говорит Хьюз.

Она советует, что после слияния организациям следует медленно приступать к интеграции систем. «Возможно, вы захотите только открыть для вновь приобретенной организации возможность доступа к электронной почте или системе учета рабочего времени», — говорит она.

«Со временем, когда вы сможете привести системы в соответствие со своими стандартами или перенести их на существующие корпоративные платформы, вы откроете больше и интегрируете больше».

Кажется очевидным, что импульс консолидации рынка здравоохранения еще не иссяк. Президент Джо Байден в указе от 2021 года попросил антимонопольные органы принять жесткие меры против объединения больниц. С тех пор Федеральная торговая комиссия заблокировала четыре слияния больниц и позволила продолжить 54, как показало расследование ProPublica.

Одной из причин такого соотношения является то, что антимонопольное руководство агентства уделяет особое внимание слияниям в пределах географического региона. Слияния больниц, расположенных в разных регионах, не привлекают такого же внимания, и они составляют ускоряющуюся часть слияний больниц. Вот почему безопасность медицинских данных так часто зависит от практики больниц, в которые пациенты никогда не ступали». ***(Live Webinar | Navigating the Difficulties of Patching OT // Information Security Media Group, Corp. (https://www.govinfosecurity.com/webinars/live-webinar-navigating-difficulties-patching-ot-w-4598). 09.02.2023).***

***

«В новом отчете об опросе в Индии оценивается позиция лидеров здравоохранения в отношении использования ими технологий в целях повышения операционной эффективности, улучшения предоставления услуг и улучшения результатов в отношении здоровья.

Грант Торнтон Бхарат и Ассоциация поставщиков медицинских услуг (Индия) опросили более 50 респондентов, которые в основном являются руководителями многопрофильных больниц, расположенных в мегаполисах, в указанном отчете под названием «Трансформация технологий для здравоохранения, готового к будущему».

ВЫВОДЫ

Опрос показал, что примерно восемь из десяти респондентов увеличат свой бюджет на цифровые технологии и технологии в ближайшие 12 месяцев. Одной из основных областей инвестиций является технология 5G, которая известна своим потенциалом в преобразовании услуг для пациентов, таких как удаленный мониторинг состояния здоровья в режиме реального времени и телемедицина.

Однако на этом обнадеживающем фоне расходов на технологии главными проблемами являются киберугрозы и конфиденциальность данных. Две трети респондентов заявили, что не уверены, что их технологическая инфраструктура сможет отразить такие угрозы, и только четверо из десяти обладают необходимыми возможностями для защиты конфиденциальности данных пациентов.

Те, кто прошел цифровизацию, или почти половина респондентов, увидели до 20% повышения эффективности от внедрения технологий.

Но организациям еще предстоит внедрить технологию для контроля за соблюдением нормативных требований, соблюдением законодательства и судебными разбирательствами, поскольку только 42% респондентов заявили, что внедрили такую технологию.

Отчет об опросе также показал, что большинство респондентов получают менее 5% дохода от использования телемедицины.

Что касается EMR, то большинство респондентов, или 62%, внедрили их, однако 54% заявили, что технология не интегрирована с их биллинговыми системами. По словам авторов отчета, умный и интегрированный EMR может обеспечить «значительную эффективность в выставлении счетов и улучшить качество обслуживания пациентов».

Наконец, опрос показал, что большинству больниц еще предстоит внедрить платформу Ayushman Bharat Digital Mission (ABDM); только 28% респондентов заявили, что их больницы участвуют в этой флагманской государственной программе, направленной на создание интегрированной инфраструктуры цифрового здравоохранения, объединяющей все заинтересованные стороны экосистемы здравоохранения страны. Респонденты упомянули основные проблемы при регистрации в ABDM, в том числе трудности с внедрением или интеграцией технологий, конфиденциальность данных, контроль со стороны регулирующих органов и киберугрозы.

ПОЧЕМУ ЭТО ВАЖНО

В отчете сделан вывод о том, что переход к интеллектуальной и подключенной системе здравоохранения «не сильно отстает», поскольку технологические инструменты, оборудование и устройства, а также цифровые решения становятся все более доступными как в Индии, так и за ее пределами. «Мы считаем, что привлекательные условия на рынке здравоохранения, экономия

за счет масштаба и честная конкуренция будут способствовать развитию этой тенденции», — подчеркнули в компании.

В нем также подчеркивается, что успех цифровизации здравоохранения зависит от «раннего внедрения, надлежащего обучения и стимулирования врачей, медсестер и специалистов в области биомеханики к эффективному использованию технологий». Еще одним фактором является импульс, необходимый для стимулирования тенденции использования и внедрения технологий в местном секторе здравоохранения.

«Создание интеллектуальной системы здравоохранения позволит врачам лучше выполнять свою работу, одновременно улучшая качество обслуживания пациентов. Согласованные усилия и беспрепятственный подход всех основных заинтересованных сторон к разработке технологий и решений, которые охватывают все уровни экосистемы здравоохранения, будут способствовать победе». победный сценарий для Индии на пути к цифровизации своей инфраструктуры здравоохранения», — говорится в отчете.

БОЛЬШАЯ ТЕНДЕНЦИЯ

Основным выводом отчета является необходимость для организаций здравоохранения вкладывать значительные средства в технологии, которые устраняют угрозы кибербезопасности и проблемы конфиденциальности данных…» ***(Adam Ang. Indian healthcare chiefs doubt their cybersecurity capability: report // Healthcare IT News (https://www.healthcareitnews.com/news/asia/indian-healthcare-chiefs-doubt-their-cybersecurity-capability-report). 15.02.2023).***

***

Захист персональних даних та соціальні мережі

«Журналіст видання Motherboard зателефонував до кол-центру британського Lloyds Bank і за допомогою штучно згенерованого голосу попросив перевірити баланс рахунку. Роботизоване голосове меню попросило ввести або промовити дату народження як першу частину автентифікації. Після цього потрібно було сказати фразу для входу: «Мій голос — мій пароль». Експерт знову відтворив звуковий файл із комп'ютера. Система безпеки ідентифікувала голос і відкрила доступ до інформації про банківський рахунок, включно із залишком, списком останніх транзакцій і переказів.

Медійник використовував безкоштовний сервіс генерації голосу від ElevenLabs. Щоб створити потрібну аудіодоріжку, автор експерименту записав близько 5 хвилин своєї розмови та завантажив її у програму. Після обробки синтетичний голос вимовляв будь-яке необхідне повідомлення.

До цього моменту такий «тест» зазнавав невдачі - система Lloyd Bank не могла ідентифікувати голос користувача. Після того, як журналіст начитав для ElevenLabs довший текст, щоб мова звучала природніше, згенерований звук успішно обійшов банківську систему безпеки.

Журналіст зауважив, що для цієї конкретної атаки шахрай повинен знати дату народження жертви, але в еру соцмереж це не велика проблема. У Lloyds Bank заявили, що знають про загрозу синтетичних голосів, але досі не стикалися з випадками, коли такий голос використовували для шахрайства щодо їхніх клієнтів. Деякі експерти тепер закликають банки повністю відмовитися від голосової автентифікації. Вони впевнені - з вдосконаленням алгоритмів ШІ біометрія перестане бути запорукою високого рівня безпеки даних…» ***(Штучний інтелект використали для злому банківського рахунку за допомогою синтезованого голосу // No worries! (https://noworries.news/shtuchnyj-intelekt-vykorystaly-dlya-zlomu-bankivskogo-rahunku-za-dopomogoyu-syntezovanogo-golosu/). 24.02.2023).***

***

«…В среду в трех крупнейших социальных сетях планеты произошел сбой, в результате чего некоторые пользователи Twitter, Instagram и YouTube не смогли получить доступ к своим учетным записям.

В среду многие пользователи Twitter получили сообщение о том, что они «превышают дневной лимит» и не могут публиковать сообщения. Проблемы начались вскоре после того, как в 15:00 по восточному времени в среду было объявлено, что подписчики Twitter Blue в США теперь могут иметь до 4000 символов в одном сообщении.

С тех пор, как в октябре глава Tesla Илон Маск приватизировал Twitter и назначил себя генеральным директором, гигант социальных сетей сократил более двух третей своего персонала, в результате чего многие задаются вопросом, как долго Twitter сможет продолжать нормально работать. Этот страх стал реальностью в среду, когда Twitter столкнулся с одним из крупнейших сбоев в своей 16-летней истории.

«У некоторых из вас Twitter может работать не так, как ожидалось. Извините за беспокойство. Мы знаем и работаем над тем, чтобы это исправить», — написал гигант социальных сетей в 18:27 по восточному времени в среду.

Сайт Downdetector, который собирает сообщения о перебоях в работе веб-сайтов и служб, указывает, что проблемы начались незадолго до 16:30 по восточному времени в среду, с более чем 9000 сообщений о сбоях в работе между 16:55 и 17:10 по восточному времени, прежде чем резко упасть.

Отключение Twitter продолжалось в течение нескольких часов для многих пользователей и вынуждало их использовать функцию запланированных твитов для публикации обновлений. Нескольким пользователям запретили публиковать твиты, и им сказали: «Вы превысили дневной лимит на отправку твитов».

По данным Справочного центра Twitter, сайт микроблогов в настоящее время позволяет размещать 2400 твитов и 500 прямых сообщений, что означает, что практически все сообщения о превышении дневного лимита были ошибочными…

Неприятности среды не ограничивались только Twitter.

YouTube заявляет, что расследует причины сбоя, с которым сталкиваются некоторые из его пользователей. Пользователи онлайн-платформы для обмена видео были встречены в среду сообщением об ошибке сервера «429». По данным Downdetector, отключение YouTube было кратким, но повсеместным: почти 72 000

пользователей сообщили о проблемах в 19:19 по восточному времени в среду, прежде чем все вернулось в норму вскоре после 20:00 по восточному времени.

«Ошибка HTTP 429 — это код состояния ответа HTTP, который указывает, что клиентское приложение превысило ограничение скорости или количество запросов, которые они могут отправить за определенный период времени», — сообщает Hubspot.

Боль в социальных сетях на этом не остановилась.

Downdetector показывает всплеск пользовательских сообщений о проблемах в онлайн-сервисе обмена фотографиями Instagram, причем отчеты начинаются незадолго до 14:00 по восточному времени и продолжаются до 22:00 по восточному времени. Худшие из проблем произошли незадолго до 16:30 по восточному времени, когда Downdetector получил почти 7000 сообщений о проблемах.

Twitter, YouTube и Instagram не сразу ответили на запросы о дополнительных подробностях от Information Security Media Group.

Три сбоя в работе социальных сетей произошли всего через день после того, как Microsoft пережила второй крупный сбой в облаке менее чем за две недели.

Гигант программного обеспечения и облачных вычислений из Сиэтла сообщил поздно вечером в понедельник, что некоторые службы, включая веб-почту Outlook.com, стали недоступны для пользователей в Северной Америке и за ее пределами. Отключение продолжалось и во вторник». ***(Prajeet Nair. Twitter, YouTube, Instagram Crippled By Massive Outages // Information Security Media Group, Corp. (https://www.govinfosecurity.com/twitter-youtube-instagram-crippled-by-massive-outages-a-21156). 08.02.2023).***

***

«Стрімінговий гігант почав тиснути на передплатників, які передають свої облікові записи та паролі до них іншим людям за межами своїх домогосподарств.

В Netflix починають обмежувати спільний доступ до облікових записів і детально описали деякі заходи, які платформа використовуватиме для запобігання таким діям користувачів. Про це пише онлайн-видання Streamable.

В минулому передача облікових записів (або ж передача паролів) стороннім особам була великою проблемою для компанії, оскільки один і той самий обліковий запис Netflix використовували друзі та родичі передплатника, які мешкали окремо від нього. Станом на кінець 2022 року за приблизними підрахунками свої облікові записи передавали іншим людям понад 100 мільйонів домогосподарств по всьому світу.

Одним зі способів розв’язання цієї проблеми може стати запровадження тарифних планів, які дозволяють легально передавати свої облікові записи у користування іншим людям: за невеличку додаткову плату користувач послуги зможе поділитися своїм обліковим записом із родичами, які проживають в іншому місці. Наразі ця послуга надається у тестовому режимі у кількох країнах Південної та Центральної Америки – зокрема, в Аргентині та Гондурасі.

Тим часом у компанії розкрили деякі деталі методів, що дозволять платформі обмежити нелегальну передачу облікових записів – роз'яснення розміщено в новому розділі поширених запитань користувачів на web-сайті компанії.

Використовуючи численні джерела інформації, такі, як IP-адреса, ідентифікатори пристроїв, а також активність облікового запису, компанія визначатиме, чи користувач переглядає контент Netflix з власного дому, чи він робить це з якогось іншого місця, чи взагалі послугу використовує зовсім інше домогосподарство.

Аби мати безперебійний доступ до послуги, контент Netflix необхідно переглядати через основну точку доступу Wi-Fi у домі власника облікового запису принаймні раз на 31 день. Це надає абонентському обладнанню користувача статус «довіреного пристрою», відзначає стрімінгова платформа. Якщо доступ до служби протягом «тривалого періоду часу» також намагається отримати не довірений пристрій, або ж перевірений пристрій з-за меж цієї мережі, він може бути заблокований.

Для тих, хто цікавиться можливістю доступу до послуги під час подорожі або під час відпустки, компанія вказує, що основний власник облікового запису зможе зробити це без будь-яких проблем. Інші профілі в тому ж обліковому записі також можуть отримувати доступ до послуги протягом семи днів поспіль за допомогою тимчасового коду, який може запитати власник облікового запису.

Що ж до загальної кількості користувачів, які можуть одночасно переглядати контент Netflix через один обліковий запис, то тут все залежить від конкретного тарифного плану, який ви передплатили.

Зокрема, преміальний план дозволяє одночасно підключатися до послуги максимум чотирьом пристроям. При цьому, жодних обмежень щодо загальної кількості пристроїв, які можуть підключатися до платформи в різний час, немає.

Підсумуємо

Хороша новина: Якщо ви мешкаєте в тому самому домі, де мешкає власник платного облікового запису Netflix, то зможете продовжувати спільно користуватися послугою – навіть перебуваючи на роботі чи в дорозі. Телевізори, телефони та ноутбуки, які регулярно відтворюють потоки з «основного місцеперебування» власника облікового запису, матимуть статус «довірених пристроїв».

Погана новина: На пристрої, які регулярно використовуватимуться для доступу до платформи Netflix поза межами основного місцеперебування власника облікового запису, може очікувати блокування. Аби мати можливість легально передавати свій обліковий запис Netflix для користування комусь, хто проживає за межами домогосподарства, власнику облікового запису потрібно буде купувати опцію платного обміну.

Нагадаємо, у листопаді минулого року Netflix додав функцію віддаленого виходу з облікового запису». ***(Netflix розповів як блокуватиме спільний доступ до облікових записів: ось що вигадав відеосервіс // mediasat (https://mediasat.info/uk/2023/02/02/netflix-rozpoviv-yak-blokuvatyme-spilnyj-dostup-do-oblikovyh-zapysiv-os-shho-vygadav-videoservis/). 02.02.2023).***

***

«Угрозы кибербезопасности являются одними из самых насущных проблем, о которых сегодня беспокоятся предприятия и организации. По мере того, как ценность данных (личных, финансовых или любого другого типа) возрастает, компании и организации во всем мире должны найти способы любой ценой избежать ужаса утечки данных.

Вот почему сейчас необходимо иметь хорошо работающую и мощную систему кибербезопасности. И это включает в себя выполнение ряда текущих тестов и процедур, таких как тестирование на проникновение. Это метод активной оценки безопасности ИТ-систем путем имитации атаки злоумышленника извне или изнутри.

Основная задача пен-теста — выявить уязвимости в системе и проинформировать лиц, принимающих решения, о шагах, которые необходимо предпринять для устранения пробелов. Однако о преимуществах этого метода тестирования нужно знать больше, поэтому мы перечислили четыре основные причины, по которым тестирование на проникновение должно быть неотъемлемой частью любой ИТ-системы.

1. Определите уязвимости безопасности

Уязвимости безопасности варьируются от скрытых лазеек до устаревших программных инструментов, поэтому вам необходимо знать, какие из них могут оказать наибольшее влияние на ваши системы. Например, если ваша компания использует системы IoT, уровень риска может возрасти, поскольку это одни из самых недооцененных сетевых устройств, когда речь идет о кибербезопасности.

Устройства IoT иногда бывают мобильными и могут подключаться и отключаться в любой момент. Поэтому службы безопасности могут потерять информацию об их использовании и даже не упоминать их в отчетах.

Конечно, это не означает, что ваша компания или организация не должны использовать системы или устройства IoT. Например, использование устройств IoT в здравоохранении принесло широкий спектр преимуществ. Однако это также привело к необходимости усиления мер кибербезопасности.

К счастью, вы можете использовать ручное тестирование в сочетании с инструментами безопасности на основе ИИ, чтобы определить, совершает ли кто-либо из ваших пользователей рискованное или злонамеренное поведение.

2. Улучшить состояние безопасности

Самое замечательное в ручном тестировании заключается в том, что нет единого способа сделать это. Существуют различные типы тестирования, которые вы можете применять, и специалисты рекомендуют комбинировать несколько разных методов, чтобы получить наилучшие результаты.

Фактически, это разнообразие методов тестирования на проникновение — это то, что обеспечит безопасность данных вашей компании и поможет улучшить состояние безопасности вашей компании. Это связано с тем, что разные методы дают разные результаты, которые в сочетании дают лицам, принимающим решения, подробную карту слабых мест компании.

3. Соблюдение правил

Правила кибербезопасности помогают компаниям понимать различные стандарты безопасности и добиваться более безопасной бизнес-среды. Вот почему многие из этих правил требуют, чтобы организации регулярно проводили тестирование на проникновение и аудит своих ИТ-систем для обеспечения соответствия.

Несоблюдение часто приводит к утечке данных, что также может привести к штрафу и расследованию методов кибербезопасности вашего бизнеса.

4. Снижение затрат

Тестирование на проникновение может помочь снизить затраты в долгосрочной перспективе, поскольку любые обнаруженные уязвимости могут быть устранены до того, как внешние злоумышленники обнаружат и воспользуются ими. Это также хороший способ приучить ваших сотрудников к идее всегда следить за подозрительной активностью и относиться ко всему с недоверием, когда дело доходит до общения с людьми в Интернете.

Конечно, это не должно использоваться в качестве предлога для отказа от учебных занятий по кибербезопасности, которые также должны проводиться постоянно. Когда вы сочетаете хорошую систему безопасности с хорошо обученными сотрудниками, ваша безопасность значительно улучшится…» ***(4 Reasons Why Penetration Testing Is Crucial For IT and IoT Systems // IoT Business News (https://iotbusinessnews.com/2023/02/13/84062-4-reasons-why-penetration-testing-is-crucial-for-it-and-iot-systems/). 13.02.2023).***

***

Кібербезпека та хмарні технології

«Недавние изменения» обвиняют Microsoft в том, что API веб-почты и календаря Outlook.com остались недоступными

Microsoft пережила второй крупный сбой в облаке менее чем за две недели.

Поздним вечером в понедельник в Редмонде, штат Вашингтон, где базируется технологический гигант, стало известно, что некоторые сервисы, в том числе веб-почта Outlook.com, стали недоступны для пользователей в Северной Америке и за ее пределами. Отключение продолжалось до вторника.

«Пользователи, в основном находящиеся в североамериканском регионе, пытающиеся получить доступ к Outlook.com, могут не иметь возможности отправлять, получать или искать электронную почту. Это также повлияет на дополнительные функции, такие как календарь, используемый другими службами, такими как Microsoft Teams», — говорится в сообщении Microsoft. страница состояния службы связи прочитана.

Сайт Downdetector, который собирает отчеты о сбоях в работе веб-сайтов и служб, показывает всплеск пользовательских отчетов о проблемах с Outlook, начиная с 3:24 утра по всемирному координированному времени.

Сбой, по-видимому, влияет только на службы Microsoft, ориентированные на потребителя. Outlook.com — это бесплатная служба веб-почты, ранее известная как

Hotmail, а не Outlook for Web или OWA, ориентированная на корпоративную веб-почту.

Microsoft заявляет: «Также затронуты функциональные возможности Outlook.com, такие как API-интерфейсы календаря, используемые другими службами, такими как Microsoft Teams». Похоже, это ссылка только на потребительскую версию Teams.

В последний раз Microsoft страдала от серьезного сбоя всего 13 дней назад, когда «изменение маршрутизации глобальной сети», внесенное ее внутренними командами, привело к сбоям в работе пользователей Microsoft 365 по всему миру. В частности, стали недоступны многие облачные службы Azure, в том числе Outlook, Microsoft Teams, SharePoint Online, OneDrive для бизнеса и другие…

Microsoft впервые подтвердила свое последнее отключение во вторник в 4:04 утра по всемирному координированному времени, написав в Твиттере 20 минут спустя: «Мы изучаем проблемы с доступом и обслуживанием для Outlook».

Вскоре после этого Microsoft заявила, что проблема связана с «недавними изменениями», которые повлияли на «функциональность службы». После подтверждения того, что виноваты неуказанные изменения, он начал «целевые перезапуски частей нашей инфраструктуры, на которые повлияло недавнее изменение», чтобы попытаться решить проблему.

«Наши целевые ресурсы развиваются, и мы наблюдаем небольшие улучшения в некоторых средах», — написала Microsoft в 6:46 утра по всемирному координированному времени. «В качестве альтернативы мы изучаем дополнительные шаги для ускорения решения».

Хотя проблема, по-видимому, связана с инфраструктурой Северной Америки, сбои все еще наблюдаются во всем мире. «Пользователи в дополнительных регионах за пределами Северной Америки могут испытывать некоторое остаточное воздействие из-за затронутых частей инфраструктуры в Северной Америке», — сообщает Microsoft.

Но поскольку Microsoft продолжала перезапускать множество систем, она сообщила о «постепенном улучшении этой проблемы для пользователей, находящихся в некоторых из дополнительных затронутых регионов»…

Позже во вторник Microsoft сообщила, что проблема в основном устранена примерно через 12 часов после ее возникновения…» ***(Mathew J. Schwartz.Microsoft Experiences Second Major Cloud Outage in 2 Weeks // Information Security Media Group, Corp. (https://www.govinfosecurity.com/microsoft-experiences-second-major-cloud-outage-in-2-weeks-a-21134). 07.02.2023).***

***

«Наиболее проверенным катализатором инноваций в области кибербезопасности по-прежнему остаются многочисленные проблемы, связанные с защитой облачной инфраструктуры. Облако победило предприятие, доминируя в технологических стеках крупных предприятий. Среднее предприятие использует 1427 облачных сервисов, а средний сотрудник предприятия использует до 36 облачных сервисов, включая платформы для совместной работы и обмена файлами.

К 2023 году 70 % всех корпоративных рабочих нагрузок будут развернуты в облачной инфраструктуре, по сравнению с 40 % в 2020 году. ИИ и машинное обучение ускоряют внедрение инноваций, обеспечивая новое понимание угроз и рисков в режиме реального времени. Быстрый прогресс CrowdStrike в области искусственного интеллекта и машинного обучения показывает, как поставщики средств защиты конечных точек извлекают выгоду из данных об угрозах, например, для быстрого внедрения инноваций.

Доминирование облака в корпоративных сетях и технологических стеках подпитывает крупнейший и быстрорастущий рынок ИТ. Gartner прогнозирует, что услуги общедоступных облачных сервисов по всему миру вырастут с 604,9 млрд долларов в 2023 году до 1 трлн долларов к 2026 году, достигнув совокупного годового темпа роста (CAGR) в 18,24%. Самые быстрорастущие сегменты общедоступных облачных сервисов включают управление базами данных, бизнес-аналитику, безопасность и инфраструктуру как услугу (IaaS). Прогнозируется, что расходы на общедоступные облачные безопасности сервисы вырастут с 19,4 млрд долларов в 2022 году до 48,9 млрд долларов в 2026 году, достигнув среднегодового темпа роста в 20,3%. Сегодня 94 % предприятий используют облачные сервисы, а 75 % считают, что безопасность является главной задачей. Шестьдесят семь процентов предприятий уже стандартизировали свои инфраструктуры в облаке.

По мере того, как предприятия поднимают и перемещают свои рабочие нагрузки в облако, они сталкиваются с повышенным риском взлома, случайной неправильной настройки облачных платформ и несогласованного охвата управления доступом к удостоверениям (IAM) и управления привилегированным доступом (PAM) между гипермасштабирующими устройствами и облачными платформами. Gartner прогнозирует, что по меньшей мере 99% сбоев в обеспечении безопасности облачных вычислений произойдет по вине пользователей, что подчеркивает необходимость постоянного обучения ИТ-специалистов и специалистов по безопасности новейшим методам обеспечения безопасности облачных вычислений.

На карту поставлено более 1,3 трлн долларов корпоративных расходов на ИТ, и в 2025 году они вырастут почти до 1,8 трлн долларов. К этому году 51% расходов на ИТ будет приходиться на публичные облачные сервисы по сравнению с 41% в 2022 году. Почти две трети (65,9%) расходов на прикладное программное обеспечение будут направлены на облачные технологии в 2025 году по сравнению с 57,7% в 2022 году.

«Добавление безопасности должно способствовать развитию бизнеса. Это должно быть что-то, что повышает устойчивость вашего бизнеса, и это должно быть что-то, что помогает защитить прирост производительности в результате цифровой трансформации», — сказал Джордж Курц, соучредитель и генеральный директор CrowdStrike, во время своего основного доклада на мероприятии компании Fal.Con в прошлом году.

Существует высокий спрос со стороны предприятий, стремящихся защитить свои все более сложные облачные инфраструктуры и технологические стеки. Gartner прогнозирует, что расходы предприятий на облачную безопасность удвоятся в период с 2023 по 2026 год, увеличившись с 6,4 до 12,9 млрд долларов.

Расходы конечных пользователей по всему миру на информационную безопасность и управление рисками вырастут со 167,86 млрд долларов в 2022 году до 261,48 млрд долларов в 2026 году, достигнув среднегодового темпа роста в 11,1%. Этот спрос приводит к увеличению расходов на НИОКР среди поставщиков и стартапов в области кибербезопасности.

Директора по информационной безопасности и директора по информационным технологиям часто совместно разрабатывают бизнес-кейсы для своих самых сложных инициатив в области облачной безопасности. Сюда входят, например, случаи нулевого доверия и многооблачной безопасности.

Во время своего выступления в Fal. Con, Курц объяснил, как поставщики корпоративной кибербезопасности быстрее внедряют инновации, чтобы не отставать от потребностей предприятий. Он подчеркнул, что CrowdStrike заслужила репутацию «Salesforce безопасности» благодаря своей облачной архитектуре. Эта архитектура обеспечивает большую гибкость UX и UI, позволяя пользователям легко интегрироваться с существующими локальными системами. Внимание CrowdStrike к devops и разработке продуктов проявляется в ее послужном списке успешных новых продуктов. Его команды, очевидно, обладают достаточной гибкостью для быстрой итерации на своей платформе.

В интервью VentureBeat Амол Кулкарни, директор по продуктам и инженерам CrowdStrike, сказал: «Если у вас есть основная инфраструктура в нужном месте, вы можете быстро выполнять итерации и создавать продукты намного быстрее, потому что есть базовый план. Вторая часть заключается в том, что у нас есть представление о том, что мы собираем один раз, а используем несколько раз. Итак, это основано на… сборе всей телеметрии в безопасности облака и последующем добавлении дополнительной аналитики для различных сценариев. Так что это дает нам эту скорость».

Инициативы цифровой трансформации, о которых Джордж Курц говорил в своем выступлении на Fal.Con в прошлом году, являются примерами новых бизнес-инициатив, требующих от директоров по информационной безопасности и ИТ-директоров переосмысления того, как они реализуют кибербезопасность в команде. Новые приложения SaaS, устаревшие локальные приложения, которые интегрируются в гибридные облачные конфигурации, мультиоблако и отсутствие поддержки IAM в разных гиперскейлерах — все это увеличивает для атак возможности.

Многие новые технологии быстро выводятся на рынок, чтобы помочь предприятиям справиться с экспоненциально растущим числом направлений атак. Защита всех форм идентичности имеет решающее значение сегодня, поскольку они находятся в осаде. Причины включают растущий разрыв между операционными технологиями (OT) и ИТ-системами; быстрорастущие сети Интернета вещей (IoT) и количество конечных точек; и необходимость защиты точек соприкосновения цепочки поставок с самовосстанавливающимися конечными точками.

Будущая карьера директоров по информационной безопасности и ИТ-директоров будет зависеть от того, насколько хорошо они управляют этими технологиями, включая приложения SaaS, для увеличения доходов. Ожидается, что выручка от приложений SaaS будет расти со среднегодовым темпом роста 9% в

период с 2020 по 2023 год до долларов 60,36 млрд. Мировой рынок SaaS оценивается примерно в 3 триллиона долларов и может долларов вырасти до 10 триллионов к 2030 году.

Последняя разработка Gartner Security Radar предоставляет ценную основу для оценки вклада облака в кибербезопасность в целом и нулевого доверия в частности. Gartner выделяет шесть основных направлений инноваций в сфере облачной кибербезопасности:

Защита использования облачных сервисов

Расширение поверхностей атаки

Удостоверения как новый периметр безопасности

Принятие новых подходов к кибербезопасности, разработанных для обеспечения консолидации, которую директора по информационной безопасности просят в своем стеке технологий, с использованием SASE, XDR и других технологий для этой цели.

Использование тех же технологий для новых моделей доставки

Автоматизация безопасности, в том числе гипераватоматизация и ИИ, которые могут уменьшить хроническую нехватку работников, с которой сталкиваются многие предприятия.

По оценкам, глобальные расходы на ИИ в сфере кибербезопасности вырастут с 12 миллиардов долларов в 2020 году до 30,5 миллиардов долларов к 2025 году. Предприятия и обслуживающие их поставщики средств кибербезопасности продолжают вкладывать значительные средства в ИИ и машинное обучение. Цель состоит в том, чтобы осмыслить огромные объемы данных и предоставить надежную информацию.

Многочисленные ранние успехи в области искусственного интеллекта включали выявление сложных угроз безопасности путем проведения поведенческого анализа файлов до их запуска или после их выполнения. Использование искусственного интеллекта и машинного обучения для обнаружения аномалий помогает ускорить расследование, связывая и комбинируя соответствующие сигналы уведомлений. Это расширенное обнаружение усиливает оповещения, автоматически определяя, какие дополнительные данные необходимы для расследования, а также собирая, нормализуя и визуализируя эти данные до начала фактического расследования.

Предприятия часто используют приложения и платформы для обеспечения безопасности на основе ИИ для создания сценариев, определяющих наиболее эффективные шаги по сдерживанию и снижению рисков, в зависимости от того, что было успешным в прошлом при определении облачных поверхностей угроз. Искусственный интеллект сканирует и либо рекомендует, либо, в более надежных ситуациях, мгновенно выполняет следующие шаги, тем самым экономя аналитику время, которое ему понадобилось бы для определения этих этапов. Ведущими поставщиками на этом рынке являются BluVector, CrowdStrike, Cybersec, Cyware, Exabeam, LogRhythm, Rapid7, ServiceNow, Siscale (Arcanna.ai) и Stellar Cyber.

Управление правами на облачную инфраструктуру (CIEM) помогает выявлять неправильно настроенные права доступа и разрешения на облачных платформах, обеспечивая при этом наименее привилегированный доступ. Быстрый

рост CIEM объясняется возрастающей сложностью настройки конфигураций мультиоблачных, гибридных и частных облаков.

Системы CIEM отмечают и предупреждают о рисках или ненадлежащем поведении и используют автоматизацию для изменения политик и прав. Текущее поколение платформ CIEM управляет правами доступа, разрешениями и привилегиями для десятков тысяч удостоверений, которые полагаются на многооблачную среду, применяя принцип наименьших привилегий. Это помогает выявить и избежать рисков, связанных с чрезмерными разрешениями.

CIEM также окупается в облачных конфигурациях, обеспечивая видимость всех разрешений, назначенных всем удостоверениям, действиям и ресурсам в облачных инфраструктурах, и обеспечивая доступ с минимальными привилегиями для снижения рисков доступа.

К ведущим поставщикам CIEM относятся Automize, Britive, CrowdStrike, CyberArk, Ermetic, Microsoft, SailPoint, Saviynt, SentinelOne (Attivo Networks), Sonrai Security и Zscaler …

Несколько ведущих поставщиков кибербезопасности поставили перед собой амбициозную цель улучшить возможности своей облачной платформы защиты приложений (CNAPP), чтобы не отставать от новой сложности многооблачных конфигураций на предприятии. Поставщики, в планы которых входит CNAPP, включают Aqua Security, CrowdStrike, Lacework, Orca Security, Palo Alto Networks, Rapid7 и Trend Micro.

CrowdStrike является домом для одной из самых примечательных разработок в этой области. Возможности CNAPP CrowdStrike облачной безопасности включают новые функции CIEM и интеграцию CrowdStrike Asset Graph. Последний предлагает способ получить обзор облачных активов и лучше понять и защитить облачные удостоверения и разрешения с помощью как CIEM, так и CNAPP. С помощью этих двух инструментов предприятия могут получить представление и контроль над тем, какие пользователи и как получают доступ к своим облачным ресурсам…

Расширенное обнаружение и реагирование (XDR) — это облачная платформа для расследования и реагирования на обнаружение угроз (TDIR), которая интегрирует, сопоставляет и контекстуализирует данные и предупреждения от нескольких компонентов предотвращения, обнаружения и реагирования на угрозы. Во время интервью VentureBeat с клиентами CrowdStrike на Fal.Con в прошлом году и клиентами Palo Alto Networks на Ignite '22 мы обнаружили, что XDR набирает обороты, особенно в сфере финансовых услуг, страхования и профессиональных услуг, которые известны своей сложностью. облачные инфраструктуры и технологические стеки. Ведущие поставщики кибербезопасности, предлагающие платформы XDR, включают CrowdStrike, Microsoft, Palo Alto Networks, TEHTRIS и Trend Micro.

Платформы XDR, такие как CrowdStrike Falcon, Cortex XDR и Microsoft 365 Defender, используют данные из различных источников, чтобы обеспечить единое всестороннее представление обо всех предупреждениях, событиях и потенциальных рисках, фиксируемых корпоративными данными телеметрии. Почти все такие платформы полагаются на ИИ и машинное обучение для

обработки данных, обнаружения аномалий и предоставления информации группам безопасности, чаще всего на облачной унифицированной облачной платформе. Ведущие поставщики XDR, в том числе CrowdStrike, также поддерживают открытые API для интеграции и оптимизации автоматизации в любом масштабе. Платформы XDR используются для дальнейшего предоставления вариантов консолидации директорам по информационной безопасности, которые хотят сократить расходы и повысить прозрачность за счет меньшего количества приложений кибербезопасности, обеспечивающих большую ценность…

Инициативы цифровой трансформации, которые сегодня переопределяют предприятия, требуют от директоров по информационной безопасности и ИТ-директоров переосмысления того, как они реализуют кибербезопасность в команде. Новые приложения SaaS, устаревшие локальные приложения, которые интегрируются в гибридные облачные конфигурации, мультиоблако и отсутствие поддержки IAM в разных гиперскейлерах — все это увеличивает возможности для атак. Сокращение поверхностей для атак с помощью новых инновационных технологий кибербезопасности является основой роста доходов и будущего любого предприятия.

Чем больше предприятий переносят свои рабочие нагрузки в облако, тем выше риск взлома и потери конфиденциальной информации. Для решения этих задач необходимы новые способы защиты облачных инфраструктур и конечных точек наряду с традиционными стратегиями обеспечения безопасности центров обработки данных. Gartner прогнозирует, что к 2025 году более 1,3 трлн долларов корпоративных ИТ-расходов переместятся в общедоступное облако.

Инвестируя в новые продукты, решения по управлению активами и автоматизацию, предприятия могут снизить риски, связанные с перемещением ИТ-нагрузок в облако, сохраняя при этом соответствие требованиям и прозрачность операций». ***(Louis Columbus. The cloud's growing impact on cybersecurity // VentureBeat (https://venturebeat.com/security/the-clouds-growing-impact-on-cybersecurity/). 08.02.2023).***

***

Кібербезпека Інтернету речей. Штучний інтелект

«Віртуальна стрімерка Neuro-Sama, якою керує нейромережа, напала на людину. Поки що віртуально, втім користувачі не на жарт налякались.

Під час спільної гри у Minecraft із Miyune, реальним гравцем з віртуальним аватаром, Neuro-Sama накинулася на персонажа і почала його бити. Нейромережу не зупинили ні прохання припинити, ні крики про допомогу. «Здається, почалося», — написали в одному з Telegram-каналів, натякаючи на те, що прогнози про знищення людства штучним інтелектом починають здійснюватися.

Звідки з'явилась Neuro-Sama? Її створив у 2018 році користувач Twitch @vedal987, використавши мови програмування C# і Python. Втім, лише у грудні

2022 року Neuro-Sama почала вести стріми. Як розповів @vedal987 в інтерв'ю Vice, він навчив нейромережу грати в ігри та спілкуватися з глядачами заради забави. Віртуальна аніме-дівчина Neuro-Sama проводить прямі трансляції, на яких проходить відеоігри, активно взаємодіє з чатом та співає.

Зауважимо, що ситуація з Miyune — не єдиний випадок, коли нейромережа Neuro-Sama поводить себе агресивно. На початку січня канал Neuro-Sama було заблоковано адміністрацією платформи Twitch за порушення правил сервісу. Модератори забанили Neuro-sama за розпалювання ненависті. За словами користувачів, у розмові з глядачами нейромережа «поставила під сумнів існування Голокосту», втім представники Twitch не надали коментарів з цього приводу.

Окрім Neuro-Sama, на Twitch заблокували назавжди трансляцію нескінченного телешоу «Nothing, Forever» — все через порушення правил спільноти. Штучний інтелект заявив, що «трансгендерність — це психічне захворювання», а трансгендерні люди «руйнують цілісність суспільства». Після цього модератори Twitch забанили ефір». ***(Нейромережа Neuro-Sama вперше в історії напала на людину // No worries! (https://noworries.news/nejromerezha-neuro-sama-vpershe-v-istoriyi-napala-na-lyudynu-2/). 08.02.2023).***

***

«Эксперты по кибербезопасности с осторожным оптимизмом смотрят на новую волну инноваций в области генеративного ИИ, таких как ChatGPT, в то время как злоумышленники уже начинают экспериментировать с ним.

Киберлидеры видят несколько способов, которыми генеративный ИИ может помочь в защите организаций: проверка кода на предмет эффективности и потенциальных уязвимостей; изучение новых тактик, которые могут использовать злоумышленники; и автоматизация повторяющихся задач, таких как написание отчетов.

«Я считаю, что внимание, которое в настоящее время привлекает ChatGPT, поможет нам улучшить передовые методы безопасности ИИ / машинного обучения», — написал соучредитель и генеральный директор Cloud Security Alliance Джим Ривис в своем блоге в прошлом месяце.

«Я очень рад тому, что я считаю чатом GPT своего рода новым интерфейсом», — сказал Axios директор по информационной безопасности Resilience Insurance Джастин Шаттак. «Многое из того, что мы постоянно делаем, — это просеивание шума. И я думаю, что использование машинного обучения позволяет нам быстрее справиться с этим шумом. А затем также замечать закономерности, которые мы, люди, обычно не замечаем».

«Системы генеративного искусственного интеллекта на основе текста отлично подходят для вдохновения», — сказал Axios Крис Энли, главный научный сотрудник компании NCC Group, занимающейся ИТ-безопасностью. «Мы не можем доверять им в фактических вопросах, и есть некоторые типы вопросов, на которые они в настоящее время очень плохо отвечают, но они очень хорошо помогают нам стать лучшими писателями и даже лучшими мыслителями».

Проверка реальностью: идея использования чат-ботов для просмотра или написания безопасного кода уже подвергалась сомнению некоторыми экспертами и исследователями.

Стэнфордское исследование, опубликованное в ноябре прошлого года, показало, что помощники ИИ привели к тому, что кодеры стали создавать более уязвимый код: «В целом мы обнаружили, что участники, имевшие доступ к ассистенту ИИ на основе модели OpenAI codex-davinci-002, писали значительно менее безопасный код, чем те, кто не имел доступа», — написали исследователи в обзоре исследования.

«Кроме того, участники, имевшие доступ к ИИ-помощнику, с большей вероятностью считали, что написали безопасный код, чем те, кто не имел доступа к ИИ-помощнику».

На прошлой неделе Энли провел эксперимент, попросив ChatGPT найти уязвимости в различных уровнях ошибочного кода безопасности. Он обнаружил ряд ограничений: «Как говорящая собака, она ничем не примечательна, потому что хороша; это замечательно, потому что оно вообще это делает».

Использование генеративного ИИ для проверки кода кажется некоторым экспертам особенно опасным.

«Какого черта инженеры-программисты вставляют свой код в то, что им не принадлежит?» Об этом Axios сообщил Ян МакШейн, вице-президент по стратегии компании Arctic Wolf и бывший аналитик Gartner. «Вы бы позвонили случайному Стиву с улицы и сказали: «Эй, подойди и посмотри мой финансовый аудит? Можете ли вы сказать мне, если что-то не так?»

МакШейн видит преимущества доступного пользовательского интерфейса чат-бота для снижения барьера на пути к безопасности. Но неизвестность, связанная с информацией о наборе данных и прозрачностью, также заставляет его задуматься.

«Нельзя упускать из виду, что это по-прежнему машинное обучение или машинное обучение для обучения на основе предоставленных данных», — говорит он. «И знаете, нет лучшей фразы, чем «мусор в мусоре».

Тем временем хакеры и злоумышленники, постоянно ищущие способы ускорить свои операции, быстро внедрили генеративный ИИ в атаки.

В прошлом месяце исследователи из Check Point Research обнаружили хакеров-злоумышленников, использующих ChatGPT для написания вредоносных программ, создания инструментов шифрования данных и написания кода для создания новых торговых площадок даркнета.

«Последние системы искусственного интеллекта превосходно генерируют правдоподобно звучащий текст и могут быстро и легко генерировать вариации на тему без явных орфографических или грамматических ошибок», — говорит Энли. «Это делает их идеальными для создания вариантов фишинговых писем».

Итог: Шаттак утверждает, что организации, изучающие использование ИИ, должны видеть сквозь большую шумиху и «понимать ограничения, например, по-настоящему понимать, где он находится».

«Это не один размер подходит всем», — говорит он. «Не пытайтесь применить это к чему-то, чего нет… Не заставляйте это работать завтра». ***(Peter***

Allen Clark. New AI wave will find uses and abuses in cybersecurity // Axios (https://www.axios.com/2023/02/17/cybersecurity-ai-tech-chatgpt-bing). 17.02.2023).

***

Кіберзлочинність та кібертероризм

«…Технический гигант Microsoft заявляет, что в 2022 году распределенные атаки типа «отказ в обслуживании» стали короче по продолжительности, а также стали более мощными и способными нанести больший ущерб.

Согласно отчету Microsoft о тенденциях DDoS за 2022 год, США, Индия и Восточная Азия лидируют среди целевых регионов для DDoS-атак, а устройства Интернета вещей остаются предпочтительным выбором для запуска этих атак.

DDoS-атаки в 2022 году в среднем длились менее часа, а атаки продолжительностью 1-2 минуты составили четвертую часть всех атак прошлого года.

Технический гигант говорит, что атаки были короче, потому что злоумышленникам требуется меньше ресурсов для их проведения, а командам безопасности становится все труднее защищаться от них с помощью устаревших средств управления DDoS. «Злоумышленники часто используют несколько коротких атак в течение нескольких часов, чтобы добиться максимального эффекта при минимальном количестве ресурсов», — говорят в Microsoft.

В среднем ежедневно наблюдалось 1435 DDoS-атак, а максимальное число — 2215 атак, зафиксированных 22 сентября. Объем DDoS-атак в праздничный сезон значительно увеличился до последней недели декабря.

Microsoft задокументировала атаку со скоростью 3,25 терабайт в секунду в Azure Aloud как «крупнейшую атаку» в 2022 году. Это меньше, чем ранее известная самая крупная DDoS-атака, интенсивность которой на пике составляла 3,47 ТБ в секунду.

Microsoft заявляет, что атаки TCP с отраженным усилением становятся все более распространенными и мощными, а более разнообразные типы отражателей и векторов атак обычно используют «неправильную реализацию стека TCK в промежуточных устройствах, таких как брандмауэры и устройства глубокой проверки пакетов». При атаках с отражением злоумышленники подделывают IP-адрес цели, чтобы отправить запрос на отражатель, например открытый сервер или промежуточный блок, который отвечает цели, например виртуальной машине.

Последние TCP-атаки с отраженным усилением в некоторых случаях могут достигать «бесконечного усиления». В апреле 2022 года отраженная усиленная атака SYN+ACK на ресурс Azure в Азии достигла 30 миллионов пакетов в секунду и длилась 15 секунд. «Пропускная способность атаки была не очень высокой, однако было задействовано 900 рефлекторов, каждый из которых выполнял повторные передачи, что приводило к высокой скорости передачи пакетов в секунду, что могло вывести из строя хост и другую сетевую инфраструктуру», — говорится в отчете.

По словам Microsoft, устройства IoT были предпочтительным выбором злоумышленников для запуска DDoS-атак. В 2022 году использование IoT-устройств расширилось во время российско-украинской войны.

Ботнеты, такие как Mirai, используемые государственными субъектами и преступными организациями, адаптированы для заражения широкого спектра устройств IoT и поддерживают новые векторы атак.

«Хотя Mirai по-прежнему является крупным игроком в области ботнетов, ландшафт угроз в области вредоносных программ для Интернета вещей развивается, появляются новые ботнеты, такие как Zerobot и MCCrash», — заявили в Microsoft.

На долю TCP-атак, зарегистрированных в 2022 году, приходилось 63% всех DDoS-атак, они были наиболее частой формой DDoS-атак, за ними с небольшим отрывом следовала UDP-атака (22%).

Политически мотивированные DDoS-атаки вышли на первый план, особенно в прошлом году после вторжения России в Украину.

KillNet, российская группа хактивистов, присягнувшая на верность Москве, активно вербовала добровольцев для проведения DDoS-атак против западных стран…

По данным Института CyberPeace, который отслеживает публично раскрытые атаки, связанные с войной между Россией и Украиной, KillNet провела 86 атак против проукраинских стран с начала войны». ***(Mihir Bagwe. DDoS Attacks Becoming More Potent, Shorter in Duration // Information Security Media Group, Corp. (https://www.govinfosecurity.com/ddos-attacks-becoming-more-potent-shorter-in-duration-a-21283). 22.02.2023).***

***

«Европейские киберагентства предупреждают об угрозах кибершпионажа, связанных с китайскими государственными хакерскими группами, активно исследующими сети в регионе.

Агентство Европейского Союза по кибербезопасности и CERT-EU выделяют шесть китайских передовых групп постоянных угроз, которые, по их словам, используют ряд методов для нападения на европейские сети и организации, имеющие стратегическое значение. Это группы APT 27, APT 30, APT 31, Ke3chang, Gallium и Mustang Panda.

Отчет появился примерно через 18 месяцев после того, как Европейский союз осудил волну китайских хакеров и призвал страну пресечь злонамеренную киберактивность. Отношение к Китаю во многих европейских странах ужесточилось из-за поддержки Пекином России и опасений по поводу отношения Китая к мусульманам-уйгурам и представителям других мусульманских национальностей. Главный дипломат Китая Ван И в настоящее время находится в многодневной поездке по Европе.

Среди кампаний, наблюдаемых агентствами, - атака в июле 2022 года на министерства внутренних дел и обороны Бельгии, приписываемая APT 27. Бельгия приписала атаки APT 27, APT 30 и APT 31, а также UNC 2814, Gallium и Softcell.

Другие такие атаки включают взлом европейских дипломатов в марте 2022 года, который компания по кибербезопасности Proofpoint приписала TA416 — китайской APT-группе, известной своими нападениями на жертв в секторе гражданского общества.

Китайские субъекты государственной угрозы обычно проводят обширную разведывательную деятельность, прежде чем нацелиться на жертву. В отчете говорится, что APT 31 использует ботнет, состоящий из скомпрометированных устройств маршрутизации небольших офисов, для анонимного контакта с жертвами в рамках своей разведывательной деятельности.

В отчете говорится, что после того, как хакеры идентифицировали своих жертв, группы рассылают хорошо продуманные фишинговые приманки. Затем они используют уязвимости, чтобы получить первоначальный доступ к сетям жертвы. Хакерские группы обычно используют уязвимость Log4Shell, которая затрагивает серверы Apache. Правительство США также определило Log4Shell как излюбленную уязвимость китайских хакеров…» ***(Akshaya Asokan. European Cyber Agencies Warn of Chinese Espionage Threat // Information Security Media Group, Corp. (https://www.govinfosecurity.com/european-cyber-agencies-warn-chinese-espionage-threat-a-21236). 17.02.2023).***

***

«Депутат Шотландской национальной партии Стюарт Макдональд предупреждает, что может последовать дезинформация

Шотландский политик-националист говорит, что хакеры, по-видимому, из российской разведки, проникли в его личную учетную запись электронной почты, и он предупреждает избирателей, что его сообщения могут стать частью кампании по дезинформации.

Стюарт Макдональд, член Шотландской национальной партии и член парламента Великобритании, рано утром в среду написал в Твиттере, что стал жертвой целевого фишинга, тактика которого совпадает с тактикой, подробно описанной в недавнем правительственном бюллетене о деятельности базирующейся в России Группа сиборгиум.

«Я должен предположить, что часть украденной информации может появиться в сети», — написал Макдональд. «Я также не сомневаюсь, что среди некоторых подлинных электронных писем будут полностью фальшивые электронные письма, смешанные с подлинными электронными письмами. Это старая тактика», — добавил он. Организации по кибербезопасности, в том числе Citizen Lab Университета Торонто, задокументировали «испорченные утечки» российских субъектов, которые контрабандным путем вносят ложную информацию в большой набор подлинно украденных данных.

В беседе с Би -би-си Макдональд сказал, что атака началась 13 января, когда он получил электронное письмо, которое, по-видимому, пришло от одного из сотрудников на тему, связанную с обороной Украины. Он щелкнул и ввел свои учетные данные электронной почты, чтобы получить доступ к прикрепленному документу, предположительно военному обновлению.

BBC сообщает, что McDonald связался с Национальным центром кибербезопасности как раз в тот момент, когда агентство готовилось опубликовать предупреждение о Seaborgium. Как сообщает BBC, британское правительство официально не обвиняло российское государство в том, что оно стоит за злоумышленником…

Поддерживаемые Россией передовые группы постоянной угрозы активно нацеливаются на западные организации и лидеров, критикующих войну России в Украине…

Британские политики особенно уязвимы для атак с использованием социальной инженерии, потому что большой объем данных, включая номера телефонов и учетные записи политиков в социальных сетях, публично указан на веб-сайте Службы связи правительства Великобритании, сообщил арабским новостям ранее в этом году исследователь безопасности Ричард Де Вере.

Представитель NCSC сообщил Information Security Media Group, что продолжает поддерживать политика. Они также сказали, что NCSC регулярно проводит брифинги по вопросам безопасности и дает рекомендации парламентариям, в том числе «экспертные советы для депутатов и их сотрудников». ***(Akshaya Asokan. Russian Hackers Suspected of Accessing Email of British MP // Information Security Media Group, Corp. (https://www.govinfosecurity.com/russian-hackers-suspected-accessing-email-british-mp-a-21155). 08.02.2023).***

***

«Представники Федерального бюро розслідувань (ФБР) США заявили, що впродовж декількох останніх днів вони займаються «виявленням шкідливої кіберактивності» у своїй внутрішній комп'ютерній мережі.

На думку джерел ФБР, інцидент пов'язаний із комп'ютерною системою, розташованою в офісі ФБР у Нью-Йорку, яка використовувалася для розслідування справи про поширення дитячої порнографії. Наразі невідомо як саме зловмисникам вдалося отримати доступ до мережі.

«ФБР знає про інцидент і працює над отриманням додаткової інформації», — йдеться в заяві керівництва відомства. «Інцидент вдалося локалізувати. ФБР не повідомлятиме деталі, оскільки розслідування триває»…». ***(ФБР визнали, що розслідують злом своєї комп'ютерної мережі // No worries! (https://noworries.news/fbr-vyznaly-shho-rozsliduyut-zlom-svoyeyi-kompyuternoyi-merezhi/). 19.02.2023).***

***

«Згідно з результатами спільного дослідження видання The Observer та Бюро журналістських розслідувань, криптовалютні зловмисники масово реєструють компанії у Великій Британії - таким чином довіра до шахрайських проектів зростає.

Як стало відомо, у Великій Британії діє щонайменше 168 компаній, яких підозрюють у шахрайстві з цифровими активами. Шахраї обирають Сполучене Королівство, оскільки в країні не достатньо розвинена законодавча база, здатна

протистояти їм. У розслідуванні стверджується, що фактична кількість подібних організацій, ймовірно, значно більша — журналісти вивчили лише списки підозрюваних підставних компаній та зіставили їх із повідомленнями про шахрайство в інтернеті.

Примітно, що більш ніж половина з виявлених компаній працює за стандартною схемою: коли зловмисники втираються в довіру до жертви та переконують її вкласти свої кошти у фейкову криптоплатформу. У такому випадку після отримання бажаного шахраї не «лягають на дно», а впродовж тривалого періоду витягують з жертви більше грошей. Обіцяючи великі прибутки.

У звіті The Observer йдеться про те, що найчастіше жертв шукають у соцмережах або на сайтах знайомств, таких як Tinder. При цьому багато хто з ошуканих стверджує, що реєстрація у Великобританії надає солідності, і якби фірми були зареєстровані в іншому місці, то вони б поставилися до них з більшим скептицизмом. Реєстрація компанії в Англії коштує лише 12 фунтів ($ 15) і при цьому не потребує жодної ідентифікації.

Втім, у Британії вже взяли проблему криптошахрайства до уваги. Як стало відомо на початку січня, Національне агентство боротьби зі злочинністю Великобританії (NCA) має намір сформувати спеціальну команду, яка займатиметься розслідуванням злочинів, пов’язаних із цифровими активами. Відділ назвали Національним підрозділом боротьби з кіберзлочинністю (NCCU) Crypto Cell. Спочатку до команди увійдуть п’ять офіцерів. Кожен спеціаліст отримуватиме зарплату від $ 48 200 до $ 52 400 на місяць». ***(Аналітики The Observer назвали країну, де зафіксовано найбільше криптошахраїв // No worries! (https://noworries.news/analityky-the-observer-nazvaly-krayinu-de-zafiksovano-najbilshe-kryptoshahrayiv/). 01.02.2023).***

***

«Два депутата Палаты представителей призвали Министерство энергетики предоставить информацию о трех национальных лабораториях, ставших жертвами российских хакеров в 2022 году.

В письме министру энергетики Дженнифер Грэнхольм представителям Джеймсу Комеру, штат Кентукки, председателю комитета Палаты представителей по надзору и подотчетности, и Фрэнку Лукасу, штат Оклахома, председателю комитета Палаты представителей по науке, космосу и технологиям., говорится, что документы позволят Конгрессу определить последствия попытки кибератаки.

Запрошенная информация также будет использоваться для оценки того, как Министерство энергетики работает над обеспечением безопасности конфиденциальных научных исследований и разработок в своих национальных лабораториях.

По сообщениям, российская хакерская группа, известная как Cold River, в период с августа по сентябрь 2022 года пыталась проникнуть в Брукхейвенскую национальную лабораторию, Аргоннскую национальную лабораторию и Ливерморскую национальную лабораторию.

Агрессоры создали фальшивые страницы входа и использовали фишинг электронной почты, пытаясь собрать пароли ученых-ядерщиков.

«Хакерская группа, ответственная за попытку вторжения в Национальные лаборатории Министерства энергетики… была замешана в предыдущих хакерских операциях, нацеленных на ключевых союзников США в интересах российского правительства», — заявили Комер и Лукас». ***(Naomi Cooper. House Lawmakers Request Information on Russian Hacking of National Laboratories // Executive Mosaic (https://executivegov.com/2023/02/house-lawmakers-request-information-on-russian-hacking-of-national-laboratories/). 03.02.2023).***

***

«ИТ-лидеры опасаются, что ChatGPT, мгновенно ставший известным чат-бот на основе искусственного интеллекта, уже используется спонсируемыми государством злоумышленниками при разработке кибератак.

В отчете BlackBerry, в ходе которого было опрошено 500 руководителей ИТ-руководителей в Великобритании на предмет их мнения о революционной технологии, более трех четвертей (76%) считают, что иностранные государства уже используют ChatGPT в своих кампаниях кибервойны против других стран. Почти половина (48%) считают, что 2023 год — это год, когда мы сможем приписать технологии успешную кибератаку.

Хотя это может звучать как стандартный случай гнева против машины, это далеко не так. Большинство респондентов (60%) по-прежнему считают, что технология используется в «хороших» целях, но в то же время 72% обеспокоены возможным неправильным использованием.

В основном они опасаются киберпреступников, использующих чат-бот на основе ИИ для создания правдоподобных фишинговых писем (57%), повышения сложности своих атак (51%) и ускорения новых атак социальной инженерии (49%). Еще 49% считают, что ChatGPT можно использовать для распространения дезинформации, а 47% считают его хорошим инструментом для хакеров, чтобы получить новые навыки и улучшить свои навыки.

Но если ИИ можно использовать в нападении, то его можно использовать и в защите. Вот почему почти четверо из пяти (78%) респондентов планируют инвестировать в кибербезопасность на основе ИИ в ближайшие два года, а 44% планируют сделать это в этом году. Почти все (88%) ожидают, что правительство также вмешается и отрегулирует использование технологии.

«Было хорошо задокументировано, что люди со злым умыслом пробуют почву под ногами, но мы ожидаем, что в течение этого года хакеры получат гораздо лучшее представление о том, как успешно использовать ChatGPT в гнусных целях; будь то инструмент для написания лучшего изменяемого вредоносного ПО (откроется в новой вкладке) или инструмент для укрепления их «набора навыков», — прокомментировал Шишир Сингх, главный технический директор по кибербезопасности в BlackBerry.

«И кибер-профессионалы, и хакеры будут продолжать искать, как они могут использовать его наилучшим образом. Время покажет, кто эффективнее». ***(Sead Fadilpašić. ChatGPT already feared to be behind multiple cyberattacks // Future US, Inc (https://www.techradar.com/news/chatgpt-already-feared-to-be-behind-multiple-cyberattacks). 02.02.2023).***

***

«Reddit сообщил, что в минувшие выходные хакер получил доступ к некоторым внутренним документам и бизнес-информации.

Веб-сайт объявил в пятничном обновлении, что его команде стало известно о изощренной фишинговой кампании, нацеленной на сотрудников 5 февраля. Получив учетные данные одного сотрудника, злоумышленник получил доступ к некоторым внутренним системам Reddit.

Информация, к которой был получен доступ, могла включать ограниченный код Reddit, ограниченную контактную информацию для небольшого числа контактов компании и как нынешних, так и бывших сотрудников, а также ограниченную информацию о рекламодателе.

Reddit заявил, что не было доступа к данным с высоким уровнем риска, включая данные кредитной карты, финансовую информацию компании, пароли к учетным записям, стратегию или эффективность кампании.

Производственные системы, включая платформу Reddit Ads, не пострадали и продолжают работать в обычном режиме.

«Основываясь на нашем расследовании, у нас нет доказательств того, что какая-либо информация Reddit была опубликована или распространена в Интернете», — говорится в сообщении Reddit.

Reddit сообщил, что сотрудник сообщил о себе, и его служба безопасности быстро отреагировала, чтобы закрыть доступ злоумышленнику, уведомить правоохранительные органы и начать внутреннее расследование.

«Недавно поступили сообщения об аналогичных фишинговых атаках, которые расследуются правоохранительными органами. Мы продолжаем внутреннее расследование ситуации и работаем над укреплением нашей системы безопасности против таких типов атак», — говорится в сообщении». ***(Julia Musto. Reddit hacked: Internal data accessed after phishing attack // FOX News Network, LLC. (https://www.foxbusiness.com/technology/reddit-hacked-internal-data-accessed-after-phishing-attack). 10.02.2023).***

***

«По мере того, как правительства и организации стандартизируют и согласовывают свои действия, чтобы лучше смягчить растущее число кибератак, то же самое делают и киберпреступники. В Европе лица, принимающие решения в области безопасности, и предприятия сталкиваются с теми же методами атак, что и их коллеги по всему миру. Хотя используемые методологии идентичны, поскольку все они основаны на одних и тех же цифровых технологиях, использующих схожие уязвимости, мотивы различаются.

Субъекты глобальных угроз: мотивы и сценарии

Субъектов угроз можно разделить на две основные группы в зависимости от их мотивации:

Организованные преступники действуют независимо от геополитики, обычно не имеют определенной идеологии и преследуют всех. Их основная цель — финансовая выгода.

Спонсируемые государством группы преследуют цели, включая шпионаж, кражу интеллектуальной собственности (ИС), поощрение нестабильности и т. д., продиктованные правительствами, с которыми они связаны.

Обе группы используют хорошо известные пути первоначальной компрометации, такие как использование неисправленных уязвимостей, кража учетных данных, социальная инженерия и фишинговые атаки, а также развертывание вредоносных программ с предпочтением атак программ-вымогателей.

Европейский бизнес сталкивается с четырьмя различными региональными угрозами

Отчет Forrester показал, что в течение 2022 года директора по информационной безопасности в европейских организациях столкнулись с четырьмя угрозами, которые отличались от мировых тенденций.

Основными целями кибератак являются производственные и машиностроительные отрасли. Этот вывод связан с тем, что в Европе сильный производственный сектор. ИС представляет ценность для государственных субъектов и преступных группировок; следовательно, они становятся прибыльными целями. Относительная незрелость безопасности операционных технологий (ОТ) делает эту ситуацию еще более проблематичной.

География отводит значительную роль в кибербезопасности. Компании, деятельность которых расположена в районах с геополитической напряженностью, с большей вероятностью станут мишенью государственных субъектов по различным политическим причинам. Организации должны помнить о мотивах и возможностях действующих лиц.

Злоумышленники используют дезинформацию и используют несколько методов для эксфильтрации. Более четверти (28%) попыток проникновения в европейские организации были успешными.

Банды вымогателей угрожают продать украденные данные заинтересованным сторонам, используя практику двойного вымогательства. Эти группы также имеют «коллективы» для развития сотрудничества. Это уже не актер-одиночка, а скорее бизнес.

Спонсируемая государством и организованная преступность в Европе

Атаки, спонсируемые государством, вызывают серьезное беспокойство у европейского бизнеса, но организованная преступность процветает.

Хотя Европа не является главной целью деятельности, спонсируемой государством, руководители силовых структур должны знать об этой проблеме. Африка, Ближний Восток и Турция являются наиболее мишенью политически мотивированных акторов, за ними следует Северная Европа. В Европе организации в основном страдают от финансовых угроз, расположенных в России, Иране и Северной Корее.

По мере того, как киберпреступность становится мейнстримом, организованные киберпреступники совершенствуются. По мере того, как экономика киберпреступности растет и становится третьей по величине мировой экономикой, преступные группировки формируют коллективы для обмена знаниями и торговли. Организованная преступность как услуга процветает, принимая несколько форм:

Программы-вымогатели как услуга: речь идет не только о шифровании данных и блокировке сотрудников. Злоумышленники также используют тактику двойного вымогательства и угрожают продать украденные данные заинтересованным сторонам, если их жертвы не заплатят выкуп.

Фишинг как услуга. В наши дни фишинговые атаки могут быть выполнены (почти) любым человеком, имеющим подключение к Интернету. Наборы инструментов и методологии на базе ИИ доступны для продажи на торговых площадках для киберпреступников.

В целом, мы наблюдаем расширение сотрудничества между киберпреступными группировками, больше похожее на «Преступность как бизнес». У киберпреступников есть специализации, как у любого бизнеса и команды, и они работают вместе для достижения целей, начиная от мелкого мошенничества и заканчивая шпионажем.

Растущие риски операционных технологий

Данные Forrester показывают, что 16% лиц, принимающих решения в области безопасности в Европе, рассматривают защиту сред ОТ как главный тактический приоритет. В то же время IBM сообщает об увеличении на 2204% разведывательных данных против систем ОТ.

Спонсируемые государством аффилированные лица, включая Electrum, Magnallium и Xenotime, все чаще нацелены на производственные организации. Эти субъекты получают первоначальный доступ с помощью кражи учетных данных, использования уязвимостей в облаке и вредоносных программ. Однако положительным признаком является то, что лица, принимающие решения в области безопасности в организациях, которые столкнулись со сбоями или вымогательством данных, с большей вероятностью отдавали приоритет безопасности ICS или ОТ.

Как европейский бизнес может справиться с киберрисками?

Предприятиям нужна помощь, чтобы интегрировать информацию об угрозах в свои программы безопасности. Однако каналы аналитики угроз, в которых перечислены начальные индикаторы компрометации, должны быть более полными. Европейские организации должны оценивать свою программу разведки угроз с трех точек зрения: тактической, оперативной и стратегической. Это важно, потому что, помимо распознавания тактики злоумышленников, география и политика являются жизненно важными факторами, которые следует учитывать при создании информации о киберугрозах.

Таким образом, компании должны основывать свою программу разведки об угрозах на четырех важных соображениях:

Сосредоточьтесь на том, как злоумышленники, нацеленные на вашу организацию, выбирают различные стратегические решения для вашей программы безопасности.

Сотрудничайте с поставщиком стратегической информации об угрозах и используйте эту информацию для регулярной корректировки действий вашей программы безопасности.

Выявление и привлечение соответствующих заинтересованных сторон, занимающихся разведкой угроз, для сбора и определения требований к разведке.

Критически относитесь к источникам данных, поскольку государственные субъекты используют дезинформацию. Используйте надежные источники информации, такие как NCSC, ENISA, BSI и ANSSI.

Сосредоточившись на домене OT, безопасность начинается со знания вашей среды. Поэтому первым шагом является определение всей вашей интеллектуальной собственности и ее местонахождение, а также рассмотрение того, как вы можете защитить ее с помощью согласованных политик безопасности данных.

После достижения желаемого уровня видимости следующим шагом будет шифрование важных данных и реализация стратегии предотвращения потери данных (DLP). Использование специализированного программного обеспечения DLP дает организациям множество преимуществ. Наконец, вы должны использовать возможности классификации данных и централизованное управление политиками, чтобы упростить обнаружение и применение политик.

Однако кибербезопасность касается не только процессов. Это также касается людей и технологий в вашей организации. Европейские организации должны подготовить своих людей к возможности успешной атаки. В этом направлении можно предпринять несколько шагов:

Используйте руководство Forrester по борьбе с программами-вымогателями, чтобы справиться со своей защитой

Подготовьте план аварийного восстановления для своих команд, чтобы у вас была структурированная коммуникационная стратегия.

Проведите симуляционные упражнения и обязательно привлеките основные заинтересованные стороны.

Разработайте надежную стратегию резервного копирования и сосредоточьтесь на тестировании. Целостность данных необходима для аварийного восстановления и обеспечения непрерывности бизнеса.

Как Фортра может вам помочь

Fortra давно известна тем, что помогает организациям стать более безопасными и автономными. Чтобы повысить степень зрелости системы безопасности и снизить операционную нагрузку, мы должны вместе устранять уязвимости, связанные с технологиями и людьми. Это означает обеспечение безопасности инфраструктуры и данных, постоянное повышение осведомленности людей о рисках безопасности и предоставление своим командам дополнительных ресурсов для обеспечения безопасности.

Делая это успешно, мы значительно повысим зрелость безопасности организации в областях, на которые приходится 75 % всех атак с помощью всего одного партнера по кибербезопасности, при этом снизив их операционную

нагрузку. Fortra предлагает широкий спектр решений в области кибербезопасности, которые помогают европейским организациям эффективно защищаться от постоянно меняющихся угроз…» ***(Cybersecurity Threats in Europe: What You Need to Know and What to Do About Them // Fortra, LLC and its group of companies (https://www.tripwire.com/state-of-security/cybersecurity-threats-europe-what-you-need-know-and-what-do-about-them). 21.02.2023).***

***

«Компания по кибербезопасности сообщила, что хакеры получили доступ к дата-центрам Apple и других крупных компаний. Они также могли получить удаленный доступ к камерам наблюдения, а имеющиеся у них привилегии могли позволить даже физический доступ к серверам.

Хакеры получили доступ к двум сторонним дата-центрам, используемым многими крупными компаниями, и оттуда смогли получить логины поддержки клиентов для Apple, Amazon, BMW, Goldman Sachs, Microsoft и целых 2000 других компаний…

Хотя у Apple есть собственные центры обработки данных по всему миру, она также широко использует сторонние центры, такие как Amazon Web Services.

В Азии Apple и другие компании размещают серверы в двух крупнейших операторах центров обработки данных на континенте, GDS Holdings и ST Telemedia Global Data Centers. Обе компании предлагают так называемые услуги колокации, где они предоставляют здание и сетевую инфраструктуру, а компании-клиенты могут затем устанавливать свои собственные серверы.

Bloomberg сообщает, что хакерам удалось скомпрометировать системы, используемые обеими компаниями, и оттуда получить доступ к учетным данным для входа в системы поддержки клиентов около 2000 компаний, у которых есть серверы, размещенные там.

В эпизоде, который подчеркивает уязвимость глобальных компьютерных сетей, хакеры завладели учетными данными для входа в центры обработки данных в Азии, которые используются некоторыми из крупнейших мировых компаний, что является потенциальной удачей для шпионажа или саботажа, согласно исследованию кибербезопасности […]

Информация включала учетные данные в различных количествах для некоторых крупнейших мировых компаний, включая Alibaba Group Holding Ltd., Amazon. com Inc., Apple Inc., BMW AG, Goldman Sachs Group Inc., Huawei Technologies Co., Microsoft Corp. и Walmart Inc., согласно охранной фирме и сотням страниц документов, которые рассмотрел Bloomberg.

Нападение произошло еще в 2021 году, но стало известно только сейчас. В отчете говорится, что логины клиентов все еще использовались еще в январе этого года. В этот момент обе компании центра обработки данных принудительно сбросили пароль, что окончательно заблокировало хакеров.

Настоящий кошмар для любой компании — это когда злоумышленнику удается получить физический доступ к ее серверам, поскольку тогда нет предела тому, что он может сделать.

Фирма по кибербезопасности Resecurity говорит, что это могло произойти в данном случае.

Resecurity и руководители четырех крупных американских компаний, которые пострадали, заявили, что украденные учетные данные представляют собой необычную и серьезную опасность, в первую очередь потому, что веб-сайты поддержки клиентов контролируют, кому разрешен физический доступ к ИТ-оборудованию, размещенному в центрах обработки данных […]

«Физическая безопасность ИТ-оборудования в сторонних центрах обработки данных и системы контроля доступа к нему представляют собой уязвимости, которые часто упускаются из виду отделами корпоративной безопасности», — сказал Малкольм Харкинс, бывший руководитель отдела безопасности и конфиденциальности Intel Corp. оборудование «может иметь разрушительные последствия», — сказал Харкинс.

Физический доступ мог быть облегчен тем фактом, что хакеры смогли получить доступ к камерам наблюдения в одной из компаний.

Хакеры также украли учетные данные для сети GDS из более чем 30 000 камер наблюдения, большинство из которых полагались на простые пароли, такие как «admin» или «admin12345», как показывают документы.

Большинство компаний, с которыми связалось Bloomberg, отказались от комментариев. Сюда входят Alibaba, Amazon, Huawei и Walmart. Apple не ответила на многочисленные запросы о комментариях.

Несколько компаний заявили, что не верят в доступ к данным клиентов и не видят никакого влияния на их бизнес. В BMW заявили, что атака имела «очень ограниченное влияние».

Оба оператора центров обработки данных признали, что нарушения имели место, но, конечно, преуменьшили их серьезность». ***(Ben Lovejoy. Data center logins for Apple and others obtained by hackers; could have facilitated physical access // 9to5mac (https://9to5mac.com/2023/02/21/data-center-logins-for-apple/). 21.02.2023).***

***

«Команды цифровой криминалистики и реагирования на инциденты доказали свою незаменимость в борьбе с киберпреступниками, но сложность и объем атак, а также нехватка талантов, доступных для их устранения, приводят к беспрецедентному выгоранию», — сказал Адам Белшер, генеральный директор Magnet Forensics.

В ежегодном опросе Magnet Forensics приняли участие 492 лица, принимающие решения и специалисты в области цифровой криминалистики и реагирования на инциденты (DFIR), преимущественно из Северной Америки, Европы, Ближнего Востока и Африки. Респонденты описали текущую картину киберпреступности как выходящую за рамки программ-вымогателей и сказывающуюся на их способности к расследованию.

Растущие волны инцидентов подавляют команды DFIR

40% респондентов описали эволюцию методов кибератак как «крупную» или «чрезвычайную» проблему, влияющую на их расследования. Это на 50% больше, чем в отчете DFIR о состоянии предприятий за 2022 год.

Компрометация корпоративной электронной почты растет и в настоящее время встречается чаще, чем программы-вымогатели, наиболее распространенная угроза безопасности в прошлогоднем отчете. Наибольшее количество респондентов — 14% — сказали, что сталкиваются с этим «очень часто».

По мнению 50 % респондентов, атаки с компрометацией корпоративной электронной почты, скорее всего, потребуют сторонних ресурсов для помощи в расследовании.

Службам безопасности требуется слишком много времени, чтобы добраться до первопричины этих развивающихся атак. 43% сказали, что им требуется от одной недели до более месяца. Около 1 из 3 респондентов заявил, что для выявления первопричины требуется либо «полный пересмотр», либо «значительные улучшения».

Поскольку киберпреступники активизируют свои усилия, команды DFIR теперь расследуют волны инцидентов, которые становятся все более объемными и сложными.

По мнению 45% респондентов, всплеск расследований и связанных с ними данных является либо «большой», либо «чрезвычайной» проблемой для их организаций. Не имея возможности обрабатывать эти данные в одиночку, почти две трети обращаются за помощью к третьим лицам.

По мнению респондентов, глобальная нехватка талантов, из-за которой только в США осталось более 755 000 незаполненных вакансий в киберпространстве, не помогает делу. Почти каждый третий говорит, что набор и найм новых специалистов DFIR в команду безопасности является сложной задачей. Каждый из этих факторов способствует их выгоранию и побуждает их искать альтернативные решения, такие как автоматизация.

Бдительность и усталость от расследования, вероятно, играют роль в выгорании

54% респондентов заявили, что чувствуют себя выгоревшими на работе.

Бдительность и усталость от исследований, вероятно, играют роль в выгорании, поскольку 64% респондентов сказали, что это «настоящая проблема».

Современные исследовательские рабочие процессы замедляются из-за того, что они полагаются на повторяющиеся задачи и инструменты, которые несовместимы. Одинаковый процент респондентов — 37% — назвал обе проблемы либо «большой», либо «чрезвычайной».

Их рабочая нагрузка может способствовать тому, что их организации подвергаются нормативному риску. 46% заявили, что у них просто нет времени разбираться в новых правилах кибербезопасности.

Респонденты видят решение в автоматизации. 50% заявили, что автоматизация будет «чрезвычайно полезной» или «очень ценной» для нескольких задач DFIR, включая удаленное получение целевых конечных точек и обработку цифровых доказательств». ***(Complexity, volume of cyber attacks lead to burnout in security teams // Help Net Security (https://www.helpnetsecurity.com/2023/02/21/dfir-teams-burnout/). 21.02.2023).***

***

«Група ізраїльських хакерів «Команда Хорхе» більш ніж 20 років втручалась у вибори країн світу — про це повідомляє The Guardian, посилаючись на колективне розслідування 30 журналістів. Хакери запевняють, що завдяки зломам, саботажу, компрометації та вкидам дезінформації вони змогли маніпулювати понад 30-а виборчими процесами.

Кібер-підрозділом керує Таль Ханан під псевдонімом «Хорхе» — 50-річний ізраїльський екс-спецпризначенець під прикриттям. За його словами, «Команда Хорхе» — це приватна структура. Хакерів може найняти будь-хто зацікавлений. Послуги, відомі як «чорні операції», були доступні розвідувальним службам, агентам з політичних кампаній, а також корпораціям, які хотіли таємно маніпулювати громадською думкою. Послуги «Команди Хорхе» були найбільш популярними в Африці, Південній і Центральній Америці, США. Не гребували звертатися до хакерів і в Європі.

Однією з найпопулярніших послуг «Команди Хорхе» став програмний пакет «Advanced Impact Media Solutions» або AIMS. Він контролює величезну армію з тисяч фальшивих профілів у соцмережах — Twitter, LinkedIn, Facebook, Telegram, Gmail, Instagram і YouTube. Деякі фейкові користувачі навіть мають акаунти на Amazon, володіють кредитними картками, біткоїн-гаманцями та акаунтами на Airbnb.

Поспілкувавшись із керівником угруповування та його працівниками, журналісти дізнались, що хакери збирали дані про конкурентів, зокрема через зломи профілів Gmail і Telegram. Вони також хвалилися проплаченими матеріалами у впливових новинних виданнях, які потім розповсюджувалися за допомогою того ж AIMS — ПЗ для керування ботами.

Ханан описав свою команду як «випускників державних установ, які мають досвід у фінансах, соцмережах і кампаніях, а також у „психологічній війні“ та працюють з шести офісів по всьому світу». Також ватажок хакерів заявив: «Зараз ми беремо участь в одних виборах в Африці. Також у нас є команда в Греції та ОАЕ. Ми провели 33 президентські кампанії, 27 з яких були успішними». Також Ханан зазначив, що брав участь у двох «великих проектах» у США, щоправда, безпосередньо у політичний процес не втручався.

Викриття «Команди Хорхе» може поставити в незручне становище Ізраїль, який останніми роками зазнає дедалі більшого дипломатичного тиску через експорт кіберзброї. Чимало світових політичних активістів та дипломатів наголошують, що це підриває базові права людини на свободу волевиявлення». ***(Хакери з Ізраїлю 20 років втручалися у вибори по всьому світі // No worries! (https://noworries.news/hakery-z-izrayilyu-20-rokiv-vtruchalysya-u-vybory-po-vsomu-sviti/). 16.02.2023).***

***

«…Агентство Европейского Союза по кибербезопасности и CERT-EU выделяют шесть китайских передовых групп постоянных угроз, которые, по их словам, используют ряд методов для нападения на европейские сети и

организации, имеющие стратегическое значение. Это группы APT 27, APT 30, APT 31, Ke3chang, Gallium и Mustang Panda.

Отчет появился примерно через 18 месяцев после того, как Европейский союз осудил волну китайских хакеров и призвал страну пресечь злонамеренную киберактивность. Отношение к Китаю во многих европейских странах ужесточилось из-за поддержки Пекином России и опасений по поводу отношения Китая к мусульманам-уйгурам и представителям других мусульманских национальностей. Главный дипломат Китая Ван И в настоящее время находится в многодневной поездке по Европе.

Среди кампаний, наблюдаемых агентствами, - атака в июле 2022 года на министерства внутренних дел и обороны Бельгии, приписываемая APT 27. Бельгия приписала атаки APT 27, APT 30 и APT 31, а также UNC 2814, Gallium и Softcell.

Другие такие атаки включают взлом европейских дипломатов в марте 2022 года, который компания по кибербезопасности Proofpoint приписала TA416 — китайской APT-группе, известной своими нападениями на жертв в секторе гражданского общества.

Китайские субъекты государственной угрозы обычно проводят обширную разведывательную деятельность, прежде чем нацелиться на жертву. В отчете говорится, что APT 31 использует ботнет, состоящий из скомпрометированных устройств маршрутизации небольших офисов, для анонимного контакта с жертвами в рамках своей разведывательной деятельности.

В отчете говорится, что после того, как хакеры идентифицировали своих жертв, группы рассылают хорошо продуманные фишинговые приманки. Затем они используют уязвимости, чтобы получить первоначальный доступ к сетям жертвы. Хакерские группы обычно используют уязвимость Log4Shell, которая затрагивает серверы Apache. Правительство США также определило Log4Shell как излюбленную уязвимость китайских хакеров». ***(Akshaya Asokan. European Cyber Agencies Warn of Chinese Espionage Threat // Information Security Media Group, Corp. (https://www.bankinfosecurity.com/european-cyber-agencies-warn-chinese-espionage-threat-a-21236). 17.02.2023).***

***

Вірусне та інше шкідливе програмне забезпечення

«Пошук дистрибутивів популярних програм через Google завжди був пов’язаний із певним ризиком, але останніми днями кіберзлочинці значно активізувалися — посилання на ресурси зі шкідливим ПЗ показуються в рекламному блоці над органічною пошуковою видачею. Сама ж Google особливо через це не переймається, — пише Ars Techinca з посиланням на інформацію від організації Spamhaus.

За посиланнями в рекламі відкриваються сайти, з яких завантажуються підроблені інсталяційні файли таких відомих програм як Adobe Reader, GIMP, Microsoft Teams, OBS, Slack, Tor, MSI Afterburner і Thunderbird. У реальності комп’ютери заражаються вірусами сімейств AuroraStealer, IcedID, Meta Stealer,

RedLine Stealer, Vidar, Formbook і Xloader. Раніше це вірусне ПЗ поширювалися через фішингові кампанії та спам, але за останній місяць кіберзлочинці облюбували рекламну платформу Google Ads, що демонструє оголошення в пошуковій видачі.

Хакери використовують складні механізми віртуалізації, що ускладнює їхнє виявлення, і надсилають по кілька HTTP-запитів на різні адреси, тільки одна з яких належить справжньому керуючому серверу — сервери ж розміщуються у загальнодоступних хмарних провайдерів, включно з Azure, Tucows, Choopa і Namecheap.

Представник Google заявив, що кіберзлочинці часто використовують складні механізми маскування активності, а компанія за останні роки «запустила нові політики сертифікації», спрямовані на перевірку рекламодавців. Про сплеск шахрайських дій останніми днями компанія обізнана — боротьба з ними у неї в пріоритеті». ***(Хакери масово розмістили в пошуковій видачі Google посилання на віруси // Internetua (https://internetua.com/hakeri-masovo-rozmistili-v-poshukovii-vidacsi-google-posilannya-na-virusi). 05.02.2023).***

***

«Дослідники штучного інтелекту заявили, що чат-бот ChatGPT, розроблений OpenAI, навчився створювати програми-віруси, націлені на індивідуальні особливості та вразливості різних операційних систем. «Зловмисники завжди дуже швидко адаптують технологічні новації. Вже можна знайти приклади того, як за допомогою ШІ хакери генерують коди шкідливих програм з потрібними властивостями під певні операційні системи, завдання та вразливості», — наголосив дослідник Роман Дремлюга.

Основна відмінність оновлених можливостей ШІ - раніше за допомогою штучного інтелекту здійснювати кібератаки могли лише хакери, втім відтепер це можуть робити і пересічні користувачі. «Зараз віруси здебільшого використовують фахівці з безпеки для тестування, але ми чудово розуміємо, що буде далі», — підсумував експерт з технологій ШІ.

Як наголосили дослідники, щоб захистити себе та свої кошти від хакерських атак, користувачам необхідно підвищувати загальну цифрову грамотність. Вважають, що у майбутньому злочинці обиратимуть індивідуальний спосіб викрадення коштів та особистих даних користувачів за допомогою штучного інтелекту. Наразі кібератаки на основі ШІ можна поділити на 5 основних видів:

Вдосконалена постійна загроза (APT). Це прихована загроза, за якою зазвичай стоїть держава або група, яка спонсорується державою, яка отримує несанкціонований доступ до комп'ютерної мережі і залишається непоміченою протягом тривалого періоду часу.

Діпфейк-атаки. Хакери використовують відео чи зображення, створені нейромережами, щоб проводити шахрайські кампанії чи дезінформувати користувачів.

Шкідливе програмне забезпечення на базі ШІ. Таке шкідливе ПЗ може працювати самостійно і адаптуватися до умов, що змінюються. Також воно вміє уникати виявлення.

Фішинг. Використовуючи обробку природної мови (NLP) та машинне навчання (ML), зловмисники можуть створювати більш переконливі фішингові електронні листи та повідомлення, призначені для того, щоб обманом змусити людей розкрити свої особисті дані.

DDoS-атаки. Тут штучний інтелект використовується для виявлення та використання вразливостей у мережі, що дозволяє кіберзлочинцю збільшити масштаб та вплив атаки». ***(Штучний інтелект допоможе стати хакерами звичайним людям // No worries! (https://noworries.news/shtuchnyj-intelekt-dopomozhe-staty-hakeramy-zvychajnym-lyudyam/). 08.02.2023).***

***

«Компанія ESET попереджає про поширення нового шкідливого програмного забезпечення через оманливу рекламу в пошуку Google, яка веде на фальшиві ресурси. Зловмисники створили підроблені вебсайти популярних програм, зокрема Firefox, WhatsApp, Signal, Skype і Telegram, через які завантажують загрозу FatalRAT та отримують контроль над інфікованим пристроєм.

Троян віддаленого доступу FatalRAT має набір функцій для виконання різних шкідливих дій на комп'ютері жертви. Шкідливе програмне забезпечення може перехоплювати натискання клавіш, викрадати або видаляти дані, які зберігаються в деяких браузерах, а також завантажувати та виконувати файли.

Зловмисники зареєстрували різні доменні імена, які вказували на ту саму IP-адресу, тобто сервер, на якому розміщено кілька вебсайтів для завантаження троянів. Більшість із цих вебсайтів виглядають ідентично своїм легітимним аналогам, але натомість завантажують шкідливі інсталятори. В одному з випадків кіберзлочинці придбали рекламу, щоб розмістити свої шкідливі вебсайти в результаті пошуку Google. Спеціалісти ESET повідомили про ці оголошення в Google і їх було негайно видалено.

«Хоча ми не змогли зафіксувати такі результати пошуку, ми вважаємо, що вони відображалися лише користувачам у певному регіоні, — пояснює Матіас Пороллі, дослідник ESET. — Оскільки багато доменних імен, які зловмисники зареєстрували для своїх вебсайтів досить схожі на легітимні, хакери також зламували URL-адреси, щоб заманити потенційних жертв на свої вебсайти».

Цілком можливо, що кіберзлочинці зацікавлені виключно у викраденні інформації, наприклад облікових даних, з метою продажу на підпільних форумах або для використання під час іншої злочинної діяльності. Однак наразі зловмисники, які відповідальні за цю активність, залишаються невідомими.

Варто зазначити, що цього разу хакери націлювались на користувачів Азії, однак невідомо, якими можуть бути їх наступні цілі. Тому спеціалісти ESET рекомендують перевіряти безпечність URL-адреси сайту, перш ніж завантажувати програмне забезпечення, та переконатись, що це офіційний ресурс. Крім того, варто використовувати рішення для захисту пристрою, яке попередить про небезпечний сайт та вбереже від інфікування шкідливою програмою…» ***(Герман Богапов. Зловмисники через пошук Google завантажують троян FatalRAT //***

HiTech.Expert (https://expert.com.ua/156431-zlovmysnyky-cherez-poshuk-google-zavantazhuyut-troyan-fatalrat.html). 21.02.2023).

***

«Исследователи кибербезопасности обнаружили новую рекламную кампанию в сети Google Ads, которая распространяет вредоносное ПО на конечные точки ничего не подозревающих жертв. Что отличает эту кампанию вредоносной рекламы от других, так это тот факт, что распространяемое вредоносное ПО практически невозможно обнаружить современными антивирусными решениями.

Злоумышленники заставили его работать, создав код, понятный только виртуальным машинам. Если жертвы запускают вредоносное ПО, виртуальная машина может преобразовать код обратно в исходный код и запустить вредоносную программу.

Исследователи из SentinelLabs объясняют МО: «Средства виртуализации, такие как KoiVM, запутывают исполняемые файлы, заменяя исходный код, такой как инструкции NET Common Intermediate Language (CIL), виртуализированным кодом, который понимает только инфраструктура виртуализации»…

Этот тип вредоносного ПО также затрудняет анализ, добавили исследователи: «При злонамеренном использовании виртуализация затрудняет анализ вредоносного ПО, а также представляет собой попытку обойти механизмы статического анализа».

Вредоносное ПО, распространяемое таким образом, — Formbook, известный инфостилер. Его виртуализированная версия получила название «MalVirt». Чтобы обманом заставить людей загрузить вредоносное ПО, злоумышленники создали несколько поддельных веб-сайтов, притворяясь целевыми страницами, где люди могут загрузить программное обеспечение Blender 3D.

Blender 3D — популярная программа для 3D-моделирования, рендеринга и анимации.

Это не первый случай злоупотребления рекламной сетью Google для доставки вредоносного ПО. В конце декабря прошлого года исследователи обнаружили крупную кампанию, выдающую себя за ряд популярных программ и приложений, таких как Grammarly, MSI Afterburner и Slack, для доставки IceID и Racoon Stealer, известных вредоносных программ для кражи информации.

Вредоносные кампании, которые попадают в Google Ads, возможно, более опасны, поскольку люди по умолчанию склонны доверять крупным технологическим компаниям. Тем не менее, лучший способ обезопасить себя — всегда перепроверять адрес веб-сайта, независимо от того, рекламируется он в Google или нет». ***(Sead Fadilpašić. This Google Ads campaign pushes malware that your antivirus can't pick up // Future US, Inc (https://www.techradar.com/news/this-google-ads-campaign-pushes-malware-that-your-antivirus-cant-pick-up?utm_source=ground.news&utm_medium=referral). 03.02.2023).***

***

«Исследователи кибербезопасности выявили новое вредоносное ПО, которое, как утверждается, нацелено на Украину. Вредоносное программное обеспечение, обнаруженное фирмой по кибербезопасности ESET, предназначено для перезаписи файлов, используемых операционной системой Microsoft Windows. Исследователи безопасности обвинили в атаке группу под названием «Sandworm», которую неоднократно обвиняли в проведении кибератак. Команда хакеров якобы развернула новый вайпер, получивший название SwiftSlicer, используя групповую политику Active Directory. После запуска SwiftSlicer удаляет теневые копии, последовательно перезаписывает файлы на системных и несистемных дисках, а затем перезагружает компьютер.

Охранная компания ESET недавно обнаружила кибератаку, нацеленную на Украину. Атака была приписана Sandworm и произошла 25 января. Группа якобы является одной из хакерских групп российского Главного управления Генерального штаба Вооруженных Сил Российской Федерации (также известного как ГРУ) и часто обвиняется в проведение кибератак. Новое вредоносное ПО написано на языке программирования Go.

«Злоумышленники развернули новый вайпер, который мы назвали #SwiftSlicer, используя групповую политику Active Directory. Вайпер #SwiftSlicer написан на языке программирования Go. Мы приписываем эту атаку #Sandworm», — сообщила ESET в Twitter.

Исследователи ESET объясняют, что очиститель SwiftSlicer удаляет теневые копии в системе Windows после выполнения. Затем вредоносная программа рекурсивно (последовательно) перезаписывает несколько файлов, расположенных в системных драйверах, а также на несистемных дисках, а затем перезагружает компьютер. По данным ESET, для перезаписи используется блок длиной 4096 байт, заполненный случайно сгенерированными байтами.

По данным Украинской группы реагирования на компьютерные чрезвычайные ситуации (CERT-UA), российская программа Sandworm провела пять атак на Национальное информационное агентство Украины – Укринформ.

В бюллетене CERT-UA заявляет, что обнаружила варианты вайпера CaddyWiper, ZeroWipe, SDelete, AwfulShred и BidSwipe, установленные в системах информационного агентства. Из них первые три нацелены на системы Windows, а AwfulShred и BidSwipe нацелены на системы Linux и FreeBSD в Укринформе. Атака была успешной лишь частично и не повлияла на работу информационного агентства». ***(Hackers Using SwiftSlicer Wiper to Destroy Windows Files, Security Researchers Say // Techaiapp.com (https://www.techaiapp.com/big-tech/hackers-using-swiftslicer-wiper-to-destroy-windows-files-security-researchers-say/?amp=1). 01.02.2023).***

***

«…согласно отчету специалистов по безопасности Spamhaus и abuse.ch (через Ars Technica), хакеры стали более агрессивными, пытаясь распространять вредоносное ПО через поиск в Google программного обеспечения для Mac.

По сути, хакеры запускают рекламу, которая появляется при использовании Google для поиска программного обеспечения. Объявления Google появляются в верхней части результатов поиска и, кажется, предоставляют то, что ищет пользователь. Затем пользователь нажимает на объявление и переходит на страницу загрузки поддельного программного обеспечения, а когда пользователь нажимает для загрузки, вредоносное ПО сохраняется на компьютере. Самая распространенная вредоносная программа известна как XLoader и доступна как для Windows, так и для macOS. XLoader ранее использовался для записи нажатий клавиш и кражи личных данных на зараженных машинах.

За последние несколько недель Spamhaus наблюдает рост «вредоносной рекламы» в нескольких популярных приложениях, таких как Mozilla Thunderbird и Microsoft Teams. В отчете abuse.ch говорится, что «есть большой спрос» на гнусную рекламу, поэтому она, вероятно, станет еще более распространенной. В своем собственном расследовании с использованием Mac компания Ars Technica легко обнаружила вредоносную рекламу в простом поиске в Google распространенных загрузок программного обеспечения, таких как «загрузка Visual Studio» и «загрузка Tor».

Google знает об этой практике и работает над ее устранением. Тем не менее, это все еще чрезвычайно широко распространено, как отмечается в заявлении, отправленном Ars Technica: «Мы знаем о недавнем всплеске мошеннической рекламной активности. Решение этой проблемы является критическим приоритетом, и мы работаем над тем, чтобы решить эти инциденты как можно быстрее».

Как избежать вредоносных программ

Даже если Google исправит проблему в ближайшем будущем, хакеры найдут новый способ распространения вредоносного ПО на ваш Mac. Это означает, что пользователи должны защитить себя.

Самый безопасный способ получить программное обеспечение для Mac — через Apple App Store. По словам компании, именно для этого App Store и существует. (Правда в том, что все дело в деньгах, но обе вещи могут быть правдой.) Apple проверяет, что каждое приложение в ее магазине безопасно для загрузки. Доступно большинство популярных приложений от крупных разработчиков программного обеспечения, а также большой выбор от независимых разработчиков.

Если нужного вам приложения нет в App Store (или вы хотите, чтобы разработчики получали как можно большую часть уплаченной суммы, и не хотите, чтобы Apple получала свою долю), вам придется обратиться к Интернету. Лучший вариант при загрузке программного обеспечения — перейти непосредственно на веб-сайт разработчика. Они должны предлагать безопасные способы приобретения необходимого вам программного обеспечения.

Старайтесь избегать веб-сайтов, специализирующихся на загрузке программного обеспечения, поскольку хакеры постоянно атакуют эти сайты. Если у вас нет альтернатив, вы можете использовать такой сайт, как VirusTotal, для проверки файлов и URL-адресов на наличие вредоносных программ.

Если вы хотите ограничить Mac, чтобы разрешить установку приложений только из App Store, вы можете установить это в macOS. В настройках системы «Конфиденциальность и безопасность» в macOS Ventura (или системных настройках «Безопасность и конфиденциальность» в macOS Monterey и более ранних версиях) вы увидите параметр «Разрешить загрузку приложений из», и вы можете выбрать App Store.

Вы можете пойти еще дальше в защите себя, установив антивирусное программное обеспечение. У Macworld есть сводка антивирусных приложений, которые помогут вам найти приложение. У нас также есть руководство, если вам интересно, нужно ли вашему Mac антивирусное программное обеспечение в первую очередь». ***(Roman Loyola. Security researchers warn of a new Google malware scam that could infect your Mac // IDG Communications, Inc. (https://www.macworld.com/article/1502739/google-malvertising-scam-xloader-malware.html?huid=2acaf19a-c981-4bae-8981-a1910925bdb7&utm_date=20230204014103). 03.02.2023).***

***

«Оплата товаров на кассе никогда не была проще благодаря мобильным кошелькам и бесконтактным кредитным картам, но хакеры разработали новый способ использования платежных систем, которые позволяют использовать эти функции против ничего не подозревающих покупателей.

Согласно новому пресс-релизу (открывается в новой вкладке) компании Kaspersky, занимающейся кибербезопасностью, ее исследователи обнаружили новые варианты вредоносного ПО Prilex для точек продаж (PoS), которое позволяет ему блокировать транзакции бесконтактной связи ближнего радиуса действия (NFC).

Хотя киберпреступники, стоящие за Prilex, начали с атак на банкоматы, теперь они модернизировали свое вредоносное ПО, чтобы запускать атаки на системы PoS, подобные тем, которые вы видите на кассах в кафе, на заправочных станциях, в магазинах шаговой доступности и других предприятиях.

В отличие от других штаммов вредоносных программ, которые заражают пользователей в Интернете, Prilex теперь может украсть данные вашей кредитной карты в реальном мире, где люди редко ожидают стать жертвами киберпреступности.

Развернув свое вредоносное ПО в уязвимой системе PoS, киберпреступники, стоящие за Prilex, могут проводить «призрачные» атаки, в ходе которых они совершают мошенничество с кредитными картами. К сожалению, даже кредитные карты, защищенные технологией CHIP и PIN, которые считались неуязвимыми для взлома, подвергаются риску.

Отреагировав на инцидент с одним из своих клиентов, исследователи Kaspersy обнаружили три новые модификации вредоносного ПО Prilex, которые позволяют ему блокировать транзакции бесконтактных платежей.

Обычно с бесконтактной кредитной картой вы просто прикасаетесь к ней, чтобы заплатить, но теперь у Prilex есть способ заблокировать эти транзакции с помощью файла на основе правил, который позволяет вредоносному ПО узнать,

следует ли собирать информацию о кредитной карте. Поскольку транзакции на основе NFC создают уникальный номер карты, который действителен только для одной транзакции, Prilex обнаруживает это и блокирует. Когда это происходит, в системе PoS появляется сообщение о том, что произошла «бесконтактная ошибка», и покупателям предлагается вместо этого вставить или провести свою кредитную карту.

Как только потенциальная жертва вынуждена использовать свою карту, Prilex может получить все данные транзакции. Однако вредоносное ПО также может фильтровать кредитные карты по их типу. Это позволяет ему захватывать черные или корпоративные кредитные карты с более высоким лимитом транзакций, игнорируя при этом карты с более низким лимитом.

Имея данные кредитной карты жертвы, киберпреступники, стоящие за Prilex, могут совершить мошенничество с кредитными картами или даже попытаться украсть их личность.

В то время как лучшее антивирусное программное обеспечение может защитить вас от онлайн-угроз, защита себя в реальном мире немного отличается. Особенно, когда вы привыкли безопасно использовать свою кредитную карту при оформлении заказа.

Чтобы защититься от вредоносного ПО Prilex, вы должны быть особенно осторожны, когда видите «бесконтактную ошибку» после попытки использовать свою кредитную карту для оплаты. Когда это происходит, вам лучше попытаться использовать наличные деньги, если они у вас есть, но если вы хотите быть особенно осторожным, вы можете полностью отменить транзакцию. Также стоит отметить, что это вредоносное ПО не влияет на мобильные кошельки, поэтому вам лучше использовать Apple Pay, Google Pay или Samsung Pay вместо физической кредитной карты.

В сообщении в блоге (открывается в новой вкладке) поставщик защиты от кражи личных данных Aura рекомендует по возможности использовать устройство чтения чипов, поскольку оно более безопасно, чем оплата касанием. В то же время вам следует подумать об использовании одной карты для оплаты счетов, а другой — для повседневных операций. Таким образом, вы узнаете, была ли украдена информация о вашей кредитной карте в физическом месте, а не в Интернете.

Киберпреступники, стоящие за Prilex, действуют как минимум с 2014 года, и если они не будут задержаны правоохранительными органами, они и их вредоносное ПО для PoS, вероятно, останутся угрозой, за которой нужно следить». ***(Anthony Spadafora. Prilex malware can steal your credit card at checkout — here's how // Future US, Inc (https://www.tomsguide.com/news/prilex-malware-can-steal-your-credit-card-at-checkout-heres-how). 01.02.2023).***

***

«Исследователи кибербезопасности из Proofpoint обнаружили совершенно новое специально созданное вредоносное ПО, используемое злоумышленниками для проведения широкого спектра специально разработанных атак второго этапа.

Эти полезные нагрузки способны на разные вещи, от шпионажа до кражи данных, что делает атаки еще более опасными из-за их непредсказуемости.

Исследователи, которые назвали кампанию Screentime, говорят, что ее проводит новый субъект угроз по имени TA866. Хотя есть вероятность, что группа уже известна более широкому сообществу кибербезопасности, никто еще не смог связать ее с какими-либо существующими группами или кампаниями.

Proofpoint описывает TA866 как «организованного субъекта, способного выполнять хорошо продуманные атаки в масштабе, основываясь на наличии у них настраиваемых инструментов, способности и подключениях к приобретению инструментов и услуг у других поставщиков, а также увеличивающихся объемах активности».

Исследователи также предполагают, что субъекты угрозы могут быть русскими, поскольку некоторые имена переменных и комментарии в частях их полезной нагрузки второй стадии были написаны на русском языке.

В Screentime TA866 отправлял фишинговые электронные письма, пытаясь заставить жертв загрузить вредоносную полезную нагрузку под названием WasabiSeed. Это вредоносное ПО устанавливает постоянство на целевой конечной точке (открывается в новой вкладке), а затем доставляет различные полезные нагрузки второго этапа в зависимости от того, что злоумышленники сочтут целесообразным в данный момент.

Иногда он доставлял Screenshotter, вредоносное ПО с говорящим названием, а в других случаях он доставлял AHK Bot, компонент бесконечного цикла, предоставляющий профилировщик домена, загрузчик Stealer и похититель Rhadamantys.

В целом, группа кажется финансово мотивированной, утверждает Proofpoint. Однако были случаи, которые заставляли исследователей полагать, что группа также иногда интересуется шпионажем. Он был нацелен в основном на организации в США и Германии. Неразборчиво по вертикалям — кампании затрагивают все отрасли.

По словам Proofpoint, самые ранние признаки кампаний Screentime были замечены в октябре 2022 года, добавив, что активность продолжалась и в 2023 году. Фактически, в конце января этого года исследователи наблюдали «десятки тысяч сообщений электронной почты», адресованных более чем тысяче организаций». ***(Sead Fadilpašić. This new "custom" malware hits your device with specially-designed attacks // Future US, Inc. (https://www.techradar.com/news/this-new-custom-malware-hits-your-device-with-specially-designed-attacks). 10.02.2023).***

***

«Эксперты по кибербезопасности Minerva недавно сделали ошеломляющее открытие новой вредоносной программы с тегом Beep, которая обладает функциями, позволяющими избежать обнаружения и анализа программным обеспечением безопасности. Организация по кибербезопасности обнаружила Beep после того, как образцы были загружены на VirusTotal.

Как работает Beep, чтобы избежать обнаружения

Несмотря на то, что Beep находится на ранней стадии разработки и ему все еще не хватает некоторых важных возможностей для атаки вредоносных программ, в отчете Minerva показано, что он может позволить злоумышленникам загружать и внедрять дополнительные полезные нагрузки в зараженные системы, используя три основных компонента: дроппер, инжектор и полезную нагрузку.

Отличительной чертой Beep от других вредоносных программ является его способность обойти обнаружение, используя уникальные методы уклонения. Например, Beep использует методы обхода песочницы, чтобы обойти системы безопасности песочницы, используемые для проверки подозрительных программ на наличие вредоносных программ. Beep также использует методы шифрования, чтобы скрыть свою вредоносную активность, что еще больше затрудняет ее обнаружение.

Кроме того, Beep использует сочетание других методов, включая динамическую обфускацию строк, реализацию сборки, проверку языка системы, поле NtGlobalFlag, препятствующее отладке, инструкцию RDTSC и функцию анти-песочницы Beep API.

Основная проблема вредоносного ПО Beep связана с его потенциальным воздействием на бизнес, если оно не будет обнаружено. Как и любое другое вредоносное ПО, целью, скорее всего, будет кража конфиденциальной информации, такой как учетные данные для входа в систему и финансовые данные.

Исследователь Minerva Labs Натали Заргаров прокомментировала, что «похоже, что создатели этой вредоносной программы пытались установить как можно больше тактик против отладки и против VM (анти-песочницы)».

Как предприятия могут смягчить атаку вредоносного ПО Beep

Звуковой сигнал может быть использован киберпреступниками для запуска атаки программ-вымогателей. Вот основные меры, которые предприятия могут предпринять для снижения этого риска безопасности.

Укрепление конечных точек

Компании должны уделять первостепенное внимание безопасности при настройке своих систем. Внедряя параметры безопасной конфигурации, вы можете уменьшить поверхность атаки вашей организации и устранить любые уязвимости безопасности, возникающие из-за дефектных конфигураций.

Эталонные тесты CIS предоставляют отличный вариант для организаций, стремящихся внедрить ведущие в отрасли стандарты конфигурации, разработанные на основе консенсуса. Крупные компании, такие как AWS, IBM и Microsoft, выступают за использование CIS Benchmarks для безопасных конфигураций.

Проверьте настройки порта

Многочисленные варианты программ-вымогателей используют порт 3389 протокола удаленного рабочего стола и порт 445 блока сообщений сервера. Решите, должна ли ваша организация держать эти порты открытыми и ограничить подключения к доверенным хостам.

Как для локальной, так и для облачной среды проанализируйте эти параметры и сотрудничайте с поставщиком облачных услуг, чтобы отключить неиспользуемые порты RDP.

Настроить систему обнаружения вторжений

Для выявления потенциально опасных действий предприятия могут использовать систему обнаружения вторжений, которая сопоставляет журналы сетевого трафика с сигнатурами, обнаруживающими известное вредоносное поведение. Надежная IDS должна регулярно обновлять свои сигнатуры и немедленно уведомлять вашу организацию, если обнаружит возможную вредоносную активность.

Поддерживайте программное обеспечение в актуальном состоянии

Еще один важный шаг в предотвращении возможности атаки Beep или другого вредоносного ПО — убедиться, что все программное обеспечение и операционные системы обновлены до последних исправлений и обновлений безопасности. Киберпреступники часто используют уязвимости в более старых версиях программного обеспечения, чтобы получить доступ к системам, поэтому постоянное обновление всего поможет минимизировать эти риски.

Используйте антивирусное и антивредоносное программное обеспечение

Наличие надежного антивирусного и антивредоносного программного обеспечения может помочь предотвратить атаки программ-вымогателей. Несмотря на то, что Beep продемонстрировал невероятную способность уклоняться от обнаружения, для предприятий по-прежнему крайне важно иметь установленные на своих системах программы для защиты от вредоносных программ.

Качественное антивирусное и антивредоносное программное обеспечение может помочь обнаружить и поместить вредоносное ПО в карантин до того, как оно причинит какой-либо вред. Он также может обеспечить дополнительные уровни защиты от других типов киберугроз.

Внедрите политики надежных паролей

Слабые пароли могут быть серьезной уязвимостью системы безопасности, поэтому внедрение политик надежных паролей может помочь предотвратить несанкционированный доступ к системам и данным. Это может включать требование сложных паролей, регулярную смену паролей и использование многофакторной аутентификации для добавления дополнительного уровня безопасности.

Информируйте сотрудников о программах-вымогателях

Крайне важно информировать сотрудников о рисках атак программ-вымогателей и о том, как выявлять потенциальные угрозы. Это может включать обучение киберпсихологии или человеческому фактору и другое обучение безопасности для конкретной организации, посвященное тому, как распознавать фишинговые электронные письма и другие типы атак с использованием социальной инженерии, а также рекомендации по передовым методам обработки подозрительных электронных писем и других сообщений». ***(Franklin Okeke. Security warning: Beep malware can evade detection // TechnologyAdvice (https://www.techrepublic.com/article/beep-malware-evades-detection/). 16.02.2023).***

***

«Спонсируемая государством северокорейская хакерская группа в настоящее время развертывает новую вредоносную программу, нацеленную на смартфоны и персональные компьютеры, для кражи конфиденциальной

информации и файлов. Эта группа — печально известная APT37, также известная как Erebus или RedEyes, и их последняя угроза впервые появилась в январе, прямо в начале года.

В отчетах утверждается, что эта вредоносная программа способна получить доступ к вашему устройству и захватить его, а также сосредоточена на мобильных устройствах и компьютерах под управлением Windows.

Согласно AhnLab последнему отчету (через TechRadar), новое вредоносное ПО под названием «M2RAT» недавно распространялось через фишинговые электронные письма, развернутое одной из самых известных хакерских группировок в мире, APT37.

Группа использовала старую уязвимость EPS, известную как CVE-2017-8291, написанную на хангыле, известной южнокорейской программе текстового процессора, обычно используемой в стране.

В отчете утверждается, что цель хакерской группы заключалась в том, чтобы заманить людей к раскрытию их учетных данных, которые затем нацелены на конфиденциальную информацию с платформ, к которым осуществляется доступ.

Одной из самых знаковых функций M2RAT является то, как он может искать портативные устройства, подключенные к компьютеру, используя скомпрометированную конечную точку Windows.

APT37 удалось разработать это вредоносное ПО, которое делает снимки экрана или записывает медиафайлы на указанный смартфон и автоматически отправляет их на подключенный ПК.

Затем он преобразует эти файлы в файл, защищенный RAR, который затем отправляет злоумышленникам для их сбора и проверки. Вредоносная программа также способна удалить эту копию, чтобы избежать обнаружения.

Эта хакерская группа активно присутствует в Интернете, и ее последняя активность, связанная с APT37, имела место в декабре 2022 года.

Вредоносные программы и другие вирусы окружают нас повсюду, и люди больше не будут в безопасности, если не будут осторожны в выборе сайтов или ссылок для посещения, поскольку все они могут иметь скрытую угрозу, которая маскирует себя. Даже приложения в магазине Google Play для устройств Android испытывают серьезные проблемы, тем более что было обнаружено, что 34 программы содержат вредоносное ПО и ждут своих жертв для загрузки и установки.

Во всем мире происходят различные атаки вредоносных программ; среди наиболее распространенных — фишинговые атаки, атаки программ-вымогателей и использование уязвимостей нулевого дня.

Среди печально известных действующих лиц, представляющих угрозу, присутствующих в мире, — Северная Корея и Россия, две известные страны, о которых ранее сообщалось, что у них есть спонсируемые государством группы, которые выполняют их заказы.

Безопасное использование Интернета и медиаграмотность — это ключ к тому, чтобы избежать взлома или доступа с мобильных устройств. Людям рекомендуется позаботиться о себе во время онлайн-доступа, чтобы избежать доступа к этим инвазивным технологиям.

Тем не менее, такие группы, как APT37, неустанно работают над созданием новых форм взлома и заманиванием людей в установку своего вредоносного ПО. Другие методы могут быть чем-то, что вы делаете ежедневно со своими устройствами.

Эти спонсируемые государством хакеры печально известны своими действиями по краже информации: последнее вредоносное ПО APT37 было обнаружено исследователями безопасности». ***(Isaiah Richard. North Korea's APT37 Hacker Group Deploys New Malware Against Phones, Windows PC to Access Files // Tech Times LLC. (https://www.techtimes.com/articles/287743/20230215/north-korea-s-apt37-hacker-group-deploys-new-malware-against.htm). 15.02.2023).***

***

Програми-вимагачі

«…Плата злоумышленникам за гарантии удаления данных напрямую финансирует киберпреступность и осуществляет кибервымогательство в качестве бизнес-модели. Что не менее важно, это, как правило, не мешает преступникам продавать украденные данные, как показывает недавно обнародованное уголовное расследование.

В четверг полиция Нидерландов по борьбе с киберпреступностью объявила о задержании банды из трех человек, обвиняемых не только во взломе компаний, краже их данных и угрозах выложить их в сеть, если они не получат выкуп, но и в невыполнении своих обязательств. гарантии.

Голландская полиция арестовала подозреваемых - двоих 21-летних и одного 18-летнего - 23 января, и двое из них с тех пор были заключены в тюрьму, и им разрешили разговаривать только со своим адвокатом, пока продолжается расследование… Подозреваемым предъявлены обвинения во взломе компьютеров, краже данных, вымогательстве и отмывании денег.

Расследование началось в марте 2021 года после того, как крупная голландская компания сообщила в полицию о нападении, связанном с кражей данных и угрозами их разглашения.

Власти говорят, что банда заработала миллионы, нападая на предприятия всех размеров в Нидерландах и за рубежом. Банда регулярно взламывала фирмы и отправляла угрожающие сообщения с требованием выкупа на сумму не менее 100 000 долларов в криптовалюте, а иногда и до 700 000 долларов. Заплатившим жертвам было обещано безопасное возвращение украденных данных, в то время как любой, кто не осмелился заплатить, рисковал увидеть, как их ИТ-инфраструктура будет уничтожена.

«Многие компании были вынуждены платить в надежде защитить свои данные», — заявили в полиции. Но даже когда жертвы платили, по словам полиции, банда часто продавала украденные данные.

Информация, предположительно украденная группой, включала множество личных данных, позволяющих установить личность, в том числе имена десятков

миллионов человек, адреса, даты рождения, номера банковских счетов, номера кредитных карт, пароли, паспортные данные и многое другое.

Преступники не просто выбрасывают или продают украденные данные в Интернете назло. Голландская полиция сообщает, что использование украденных корпоративных данных для проведения атак социальной инженерии процветает.

«Кража данных и торговля данными — это огромная модель дохода для преступников», — говорят в полиции. «Захваченные данные обрабатываются, чтобы их можно было продать другим преступникам». В ходе этого расследования они сообщают о восстановлении программных инструментов, используемых подозреваемыми «для уточнения украденных данных», что позволяет им использовать их самостоятельно — или продавать возможность другим — для выявления многообещающих целей для «фишинга, чат-трюков, мошенничество со службой поддержки банка или мошенничество с идентификацией».

Хотя голландскую банду не обвиняют в использовании программ-вымогателей в рамках своих схем, группы вымогателей также часто заявляют, что украли данные у жертвы. Помимо требования выкупа в обмен на дешифратор, злоумышленники часто требуют отдельный выкуп в обмен на обещание удалить украденные данные. К сожалению, многие жертвы платят за такие обещания.

Но эксперты говорят, что это глупо. «Вы не можете засунуть зубную пасту обратно в тюбик», — говорит Билл Сигел, генеральный директор компании Coveware, занимающейся реагированием на программы-вымогатели.

Важно подчеркнуть, что не все организации, пострадавшие от вымогателей, поддаются такому шантажу, как это недавно наблюдалось после атаки на британскую национальную почтовую службу, Королевскую почту.

Системы Royal Mail International, которая обрабатывает письма и посылки на экспорт, были крипто-заблокированы группой вымогателей LockBit 11 января. 14, по-видимому, из-за недовольства тем, как продвигается его вымогательство.

Королевская почта отказалась комментировать правдивость просочившихся переговоров, которые, по-видимому, начались 12 января, поскольку правоохранительные органы продолжают расследование атаки.

На протяжении всего обсуждения Royal Mail сохраняла вежливый тон, не стесняясь казаться раскаявшимся.

«Мы ничего не притворяемся и приносим свои извинения, если это так покажется», — сказал представитель Royal Mail. «Просто мое руководство слышало, что ваш дешифратор может не работать с большими файлами. Вот почему они спросили и хотели узнать, работает ли он. Я пытаюсь убедить их работать с вами здесь. Они просто просят больше доказательство того, что мы получим от вас».

Участник переговоров по программам-вымогателям Куртис Миндер сообщил Malwarebytes, что поддержание сердечного тона и выигрыш времени для группы реагирования на инциденты, когда она пытается восстановить файлы, является первоочередной задачей в таких ситуациях.

Королевская почта продолжала поддерживать LockBit в течение нескольких недель. 6 февраля представитель Royal Mail заявил, что высшее руководство

«может не захотеть платить вам за это. С нашей точки зрения, файлы просочились, когда вы взяли их из нашей системы, и заплатив, вы ничего не исправите».

В ответ LockBit уменьшил требование о выкупе: «Последний шанс предотвратить утечку королевской информации. Мы готовы сделать скидку, удалить украденную информацию и предоставить расшифровщик за 40 миллионов долларов. Задержек больше не будет, после истечения таймера. все данные будут опубликованы».

Наконец, в среду — через 42 дня после того, как системы были принудительно зашифрованы, и через 41 день после начала переговоров — LockBit выложил украденные данные в сеть.

Возможно, не случайно, в тот же день почтовая служба объявила, что «услуги Royal Mail International Export теперь восстановлены во всех пунктах назначения для покупок в Интернете, с помощью решений для доставки и без прилавка в отделениях почтового отделения», за исключением «небольшого числа «услуг для бизнес-клиентов, для которых, как заявили в компании, были созданы «альтернативные услуги».

Похоже, что Royal Mail наконец-то восстановила из резервных копий или перестроила все необходимые системы. Более того, он сделал это, не заплатив никакого выкупа, не в последнюю очередь за пустые обещания злоумышленников». ***(Mathew J. Schwartz. Crime Blotter: Hackers Fail to Honor Promises to Delete Data // Information Security Media Group, Corp. (https://www.govinfosecurity.com/blogs/crime-blotter-hackers-fail-to-honor-promises-to-delete-data-p-3399). 24.02.2023).***

***

«…Производитель полупроводникового оборудования MKS Instruments сообщил федеральным регулирующим органам, что временно приостанавливает работу на некоторых объектах после атаки программы-вымогателя на прошлой неделе.

…Инцидент затронул бизнес-системы, «включая системы, связанные с производством».

На момент публикации веб-сайт MKS оставался в автономном режиме с сообщением: «К сожалению, на сайте www.mks.com произошел незапланированный сбой. Пожалуйста, зайдите позже».

MKS Instruments предлагает инструменты, подсистемы и решения для управления технологическими процессами, которые измеряют, контролируют, включают, отслеживают и анализируют различные параметры производственных процессов для повышения эффективности и производительности процесса.

Эрик Хансельман, аналитик S&P Global Market Intelligence, сообщил Information Security Media Group, что атака на производителя заводского оборудования, а не на производителя полупроводников, окажет ограниченное краткосрочное влияние на рынки полупроводников.

По его словам, спрос на полупроводники замедляется, оставляя больше возможностей для производственных предприятий…» ***(Prajeet Nair. Ransomware Attack Disrupts Operations at MKS Instruments // Information Security Media Group,***

Corp. (https://www.govinfosecurity.com/ransomware-attack-disrupts-operations-at-mks-instruments-a-21153). 08.02.2023).

****

«…Группа LockBit перешла от отрицания своей причастности к атаке программы-вымогателя на британскую Королевскую почту к попытке выторговать выкуп.

Сайт LockBit теперь указывает Royal Mail в качестве жертвы и требует, чтобы она заплатила выкуп до четверга, иначе злоумышленники выложат в Интернете неуказанные данные, которые, как они утверждают, были украдены.

Как и многие группы вымогателей, LockBit имеет свой собственный сайт утечки данных, где он перечисляет подмножество жертв, которые не заплатили ему выкуп. Цель сайта - назвать и пристыдить жертву, чтобы она заплатила, как правило, угрожая утечкой украденных данных, независимо от того, были ли какие-либо данные действительно украдены. Если жертва не платит, группа обычно сбрасывает все украденные данные после истечения крайнего срока, чтобы предупредить будущих жертв об опасностях неплатежа.

После того, как Royal Mail сообщила о нападении 11 января, публичное лицо LockBit, LockBitSupp, первоначально заявило, что не имеет никакого отношения к атаке.

Однако вскоре после этого LockBitSupp заявила, что на самом деле за атакой стоит один из 10 самых прибыльных ее партнеров.

Королевская почта продолжает попытки восстановить услуги после инцидента. Сразу же после этого он призвал британских жителей не пытаться отправлять письма или посылки, которые необходимо отправить за границу, заявив, что по-прежнему не может ничего экспортировать. С тех пор некоторые услуги были восстановлены.

В обновлении службы во вторник, через 27 дней после того, как она была нарушена, почтовая служба сообщает, что любой, кто хочет отправить посылку за границу, должен оплатить доставку либо онлайн, либо через другую службу. «В настоящее время мы не можем обрабатывать новые посылки Royal Mail, приобретенные через отделения почты», — говорится в сообщении.

Королевская почта сообщает, что устраняет огромное количество писем и посылок, в некоторых случаях отправляя их за границу с помощью «альтернативных решений и систем», хотя и с задержками. Службы импорта также испытывают «незначительные задержки», и в нем говорится, что они «прилагают все усилия, чтобы возобновить работу большего количества служб через отделения почтового отделения и будут предоставлять дальнейшие обновления для этих служб как можно скорее».

Разворот LockBit — «это были не мы» на «это были мы» — является напоминанием о том, что группы вымогателей будут продолжать лгать, обманывать и воровать, пока они могут получать прибыль за счет жертвы.

Разве нанесение удара по критически важным объектам британской национальной инфраструктуры — например, по национальной почтовой службе — не рискованно? Например, после того, как DarkSide ударила по Colonial Pipeline в

Соединенных Штатах в мае 2021 года, группа сначала обвинила филиал, а затем прекратила свою деятельность, а затем перезагрузилась под другим именем.

Хотя атака CNI может показаться игрой с огнем, многие эксперты по безопасности сходятся во мнении, что выбор целей группами программ-вымогателей остается оппортунистическим. И операторы, и любые аффилированные лица, которые используют свое вредоносное ПО, а также посредники первоначального доступа, у которых они часто покупают готовый доступ к сетям жертв, похоже, ловят в ловушку всех, кого могут поймать, а затем, возможно, расставляют приоритеты жертв в зависимости от размера и отрасли.

Примечательно не то, что LockBit или один из его филиалов нанесли удар по Королевской почте, а то, что они решили продолжить атаку. Хотя некоторые группы бесплатно выдают дешифратор медицинским учреждениям, похоже, это делается в качестве пиар-хода, если они нарушили работу больницы или спровоцировали геополитические последствия. Но не все группы выпускают бесплатные расшифровщики, и простое наличие расшифровщика не решит затраты времени и средств, необходимые для капитального ремонта инфраструктуры и восстановления систем.

Таким образом, продолжающаяся игра LockBit с вымогательством важна именно потому, что группа не выглядит испуганной.

И это несмотря на то, что несколько правоохранительных органов, несомненно, уже пытаются проникнуть в эту и другие группы...

В последнее время были достигнуты некоторые выдающиеся успехи, в том числе ФБР и его немецкие и голландские коллеги проникли в инфраструктуру и операции Hive, который был одним из самых плодовитых операций по вымогательству в мире. Агенты правоохранительных органов незаметно передали жертвам ключи дешифрования, помогая гарантировать, что потенциальные выкупы на сумму более 130 миллионов долларов так и не были выплачены…» ***(Mathew J. Schwartz. LockBit Group Goes From Denial to Bargaining Over Royal Mail // Information Security Media Group, Corp. (https://www.govinfosecurity.com/blogs/lockbit-group-goes-from-denial-to-bargaining-over-royal-mail-p-3370). 07.02.2023).***

***

«Исследователи предупреждают, что злоумышленники обновляют обходной путь и отслеживание блокировки дешифрования

Сообщается, что злоумышленники, нацеленные на непропатченные гипервизоры VMware ESXi для принудительного шифрования виртуальных машин, модифицировали свои программы-вымогатели, чтобы затруднить жертвам использование бесплатных инструментов восстановления для расшифровки файлов.

Кампания атаки уже использовала программу-вымогатель, названную VMware ESXiArgs, для принудительного шифрования более 2800 хостов и неизвестного количества виртуальных машин, работающих на этих хостах.

Эксперты по безопасности подробно описали ряд средств защиты, которые они рекомендуют установить всем пользователям ESXi, включая немедленную

изоляцию серверов, которые не были исправлены для защиты от уязвимости переполнения кучи OpenSLP (CVE-2021-21974), и блокировку IP-адресов, с которых злоумышленники…

Но с новой волной атак, впервые замеченной в среду, злоумышленники, владеющие ESXiArgs, похоже, модифицировали программу-вымогатель, чтобы усложнить легкое восстановление жертвами. Об изменении впервые сообщил Bleeping Computer, который предлагает специализированную поддержку жертвам через свои форумы.

Основываясь на оценке, предоставленной охотником за программами-вымогателями Майклом Гиллеспи (@demonslay335), основателем бесплатной службы идентификации программ-вымогателей ID, Bleeping Computer сообщает, что программа-вымогатель вместо того, чтобы шифровать очень маленькие части больших файлов, как это было раньше, облегчая тем самым их восстановление, «Все файлы размером более 128 МБ теперь будут иметь 50% зашифрованных данных, что делает их, вероятно, невосстановимыми».

Злоумышленники также удалили адреса криптовалютных кошельков из заметок о выкупе. Адреса кошельков — это адреса, по которым жертвы программ-вымогателей, решившие заплатить выкуп, получают инструкции отправить свои биткойны в обмен на обещание ключа дешифрования. Теперь жертвам предлагается связаться с злоумышленниками через Tox, который представляет собой одноранговый протокол обмена мгновенными сообщениями со сквозным шифрованием, чтобы получить адрес криптовалютного кошелька, который будет использоваться для их оплаты.

Используя уникальный адрес криптовалютного кошелька, который ранее содержался в каждой другой записке о выкупе, исследователи смогли подсчитать, что более 2800 хостов VMware ESXi были принудительно зашифрованы. Удалив эти адреса, злоумышленники усложнят усилия исследователей, респондентов и правоохранительных органов по отслеживанию серьезности кампании.

Из-за «новой процедуры шифрования, которая не имеет такой же уязвимости, как предыдущая», ИТ-команды должны «ожидать, что она станет беспорядочной», — говорит Даниэль Кард, кибер-специалист лондонской компании Xservus Limited, в отчете. Пост в LinkedIn.

С точки зрения серьезности на сегодняшний день количество виртуальных машин или ВМ, которые злоумышленники зашифровали до сих пор, остается неясным. «Обычно хост ESXi содержит от 5 до 20 виртуальных машин, — говорит он. «Даже при наличии 2000 хостов с 5 виртуальными машинами на каждом — это очень много виртуальных машин». Кроме того, многие из более чем 2803 хостов, возможно, уже были заражены.

Используя сканирование Shodan, Кард насчитал около 70 000 хостов ESXi, доступных в Интернете, из которых около 60 000 соответствуют списку версий, «подозреваемых» в уязвимости для эксплойта, хотя теоретически они также должны иметь включенный SLP.

Злоумышленники будут выполнять те же самые сканирования, используя их для каталогизации хостов ESXi, на которых запущены явно уязвимые версии, а затем напрямую сканируют порты, чтобы увидеть, включен ли у них SLP на TCP-

порту 427, сообщает Card. Возможно, говорит он, включение UDP на этом порту может также способствовать эксплойтам.

Должен ли быть включен OpenSLP для протокола определения местоположения службы, прежде чем злоумышленники смогут успешно использовать эксплойт, остается открытым вопросом. Bleeping Computer сообщает, что одна жертва кампании атаки, по-видимому, была поражена, несмотря на то, что SLP не включен в их развертывании ESXi.

Несмотря на изменения, внесенные в новую волну используемого вымогателя ESXiArgs, эксперты по безопасности рекомендуют жертвам по-прежнему пытаться использовать ранее подробно описанные методы восстановления на всякий случай, если они сработают.

Методы восстановления основаны на первой версии программы-вымогателя, часто шифрующей лишь небольшие части виртуальных дисков. «Вирус шифрует мелкие файлы» - типа.vmdkиФайлы.vmx — «но не server-flat.vmdkфайлы», по словам исследователей безопасности Энеса Сонмеза и Ахмета Айкача, которые работают с турецким ритейлером Yöre Group.

«В структуре ESXi фактические данные хранятся в flat.vmdk», — добавили исследователи, подробно описав, как этот плоский файл иногда — но не всегда — можно использовать для восстановления виртуальных дисков без необходимости дешифратора. Основываясь на своих исследованиях, Агентство США по кибербезопасности и безопасности инфраструктуры впоследствии выпустило инструмент для автоматизации этого процесса.

Кард говорит, что первоначальная тактика шифрования злоумышленников предполагает, что они не являются преступными вдохновителями программ-вымогателей. «Судя по имеющимся у меня данным, это почти наверняка низкоквалифицированный участник киберпреступлений или группа злоумышленников», — говорит он. «Они немного напортачили с этим; я думаю, последствия могли быть намного хуже».

Но, как это обычно бывает с программами-вымогателями, всякий раз, когда исследователи выявляют и сообщают об уязвимости или недостатке, злоумышленники часто быстро обновляют свой вредоносный код, пытаясь максимизировать свою прибыль…» ***(Mathew J. Schwartz. Modified ESXiArgs Ransomware Blocks VMware Host Recovery // Information Security Media Group, Corp. (https://www.govinfosecurity.com/modified-esxiargs-ransomware-blocks-vmware-host-recovery-a-21158). 09.02.2023).***

***

«Несколько правительственных учреждений в США и Южной Корее выпустили совместное предупреждение, предупреждающее критически важные секторы инфраструктуры, и особенно сектор здравоохранения, о продолжающихся угрозах программ-вымогателей с участием киберпреступников, спонсируемых северокорейским государством.

Требования Пхеньяна о выкупе за криптовалюту принесли неуказанную сумму дохода, которая идет на финансирование приоритетов и целей Северной

Кореи на национальном уровне, включая кибероперации, направленные против правительств США и Южной Кореи.

Совместное предупреждение, опубликованное в четверг, исходит от Агентства национальной безопасности США, Агентства кибербезопасности и безопасности инфраструктуры, Министерства здравоохранения и социальных служб и ФБР, а также Национальной разведывательной службы Республики Корея и Агентства безопасности обороны.

В предупреждении говорится, что тактика, методы и процедуры, связанные с атаками северокорейских программ-вымогателей, «включают в себя те, которые традиционно наблюдаются в операциях с программами-вымогателями», а также некоторые дополнительные меры, принятые для маскировки связи Пхеньяна с требованиями вымогательства.

Северокорейские хакеры «генерируют домены, персоны и учетные записи, а также идентифицируют криптовалютные службы для проведения своих операций по вымогательству. Субъекты закупают инфраструктуру, IP-адреса и домены с помощью криптовалюты, созданной в результате незаконных киберпреступлений, таких как программы-вымогатели и кража криптовалюты», — говорится в сообщении.

Они также намеренно скрывают свою причастность, работая со сторонними иностранными аффилированными лицами и используя сторонних иностранных посредников для получения выкупа. Они также скрывают свою личность, используя виртуальные частные сети, виртуальные частные серверы или IP-адреса третьих стран.

«Были замечены киберпреступники из КНДР, устанавливающие выкуп в биткойнах. Известно, что акторы общаются с жертвами через учетные записи электронной почты Proton Mail. Частным компаниям в секторе здравоохранения субъекты могут угрожать раскрытием конфиденциальных данных компании конкурентам, если выкупы не будут выплачены», - говорится в предупреждении.

В нем говорится, что злоумышленники используют различные эксплойты распространенных уязвимостей и экспозиций, чтобы получить доступ и повысить привилегии в сетях.

«Недавно наблюдаемые CVE, которые злоумышленники использовали для получения доступа, включают удаленное выполнение кода в программной библиотеке Apache Log4j, известной как Log4Shell, и удаленное выполнение кода в различных устройствах SonicWall».

Представитель SonicWall сообщила Information Security Media Group, что использованные проблемы безопасности связаны с Log4Shell, уязвимостями удаленного выполнения кода «в неисправленных устройствах SonicWall SMA 100».

Предупреждение в четверг обновляет совместный правительственный бюллетень, выпущенный 6 июля 2022 года, в отношении угроз программ-вымогателей Мауи, спонсируемых северокорейским государством, нацеленных на сектор здравоохранения и общественного здравоохранения, а также рекомендации Microsoft от 15 июля об угрозах программ-вымогателей H0lyGh0st, нацеленных на малые и средние предприятия…

В новом предупреждении подтверждается позиция правительства о том, что взломанные организации не должны оплачивать требования о вымогательстве…» ***(Marianne Kolbasuk McGee. US, South Korea Warn of North Korean Ransomware Threats // Information Security Media Group, Corp. (https://www.govinfosecurity.com/us-south-korea-warn-north-korean-ransomware-threats-a-21167). 09.02.2023).***

***

«…В понедельник двусторонняя группа правительственных учреждений выпустила рекомендации по кибербезопасности, в которых освещаются атаки программ-вымогателей на цифровые сети и критически важную инфраструктуру, особенно на системы здравоохранения.

Агентство США по кибербезопасности и безопасности инфраструктуры опубликовало предупреждение и примеры известных вредоносных имен файлов и строк хэшей, которые были задокументированы в атаках программ-вымогателей, связанных с субъектами, спонсируемыми государством Северной Кореи.

К CISA присоединились Агентство национальной безопасности, Федеральное бюро расследований и Министерство здравоохранения и социальных служб, а также Агентство обороны Республики Корея и Национальная разведывательная служба при выдаче CSA.

«Помимо других тактик, эти злоумышленники используют уязвимости, такие как Log4Shell CVE-2021-44228, SMA100 Apache CVE-2021-20038 и/или TerraMaster OS CVE-2022-24990, для получения доступа и повышения привилегий. в сетях жертвы», — говорится в консультативном заключении.

Получив первоначальный доступ, субъекты программ-вымогателей используют поэтапную полезную нагрузку — часть сообщения или блока данных с сохраненной информацией — с проприетарным вредоносным ПО, используемым для атаки на сети. В бюллетене также отмечается, что злоумышленники обычно требуют выплаты выкупа в криптовалюте.

«Авторские агентства оценивают, что неуказанная сумма дохода от этих операций с криптовалютой поддерживает приоритеты и цели КНДР на национальном уровне, включая кибероперации, направленные против правительств США и Южной Кореи», — говорится в бюллетене.

Агентства заявили, что в дополнение к атакам на сети здравоохранения северокорейские кибератаки также атаковали информационные сети Министерства обороны и оборонной промышленной базы. CISA советует жертвам не платить выкуп, опасаясь, что это может не устранить вредоносное ПО и нарушить санкции.

Федеральные власти и правоохранительные органы знают об атаках программ-вымогателей Северной Кореи не менее года, особенно в отношении конфиденциальных сетей здравоохранения. Растущий объем и потенциал угроз побудили законодателей США изучить возможности HHS для адекватной защиты своих сетей от программ-вымогателей и других кибератак…» ***(Alexandra Kelley. CISA, South Korean Agencies Issue Joint Warning on North Korean Ransomware // Nextgov (https://www.nextgov.com/cybersecurity/2023/02/cisa-south-korean-agencies-issue-joint-warning-north-korean-ransomware/382894/). 13.02.2023).***

***

«Агентство киберразведки Канады сообщает, что LockBit — активная группа программ-вымогателей, имеющая связи с Россией, — несет ответственность за 22% приписываемых инцидентов с программами-вымогателями в Канаде в прошлом году и будет представлять «постоянную угрозу» для канадских организаций в этом году.

В четверг Управление безопасности связи заявило, что отправило канадским организациям отчет об угрозах, предупреждающий о LockBit и его филиалах.

CSE описывает LockBit как группу «финансово мотивированных русскоязычных» киберпреступников, «весьма вероятно, базирующихся в стране Содружества Независимых Государств» — совокупности стран, которые когда-то были частью Советского Союза.

«Киберцентр считает, что LockBit почти наверняка останется постоянной угрозой как для канадских, так и для международных организаций в 2023 году», — сказал представитель CSE Эван Короневски.

«В 2022 году LockBit был ответственен за 22% приписанных инцидентов с программами-вымогателями в Канаде и, по оценкам, за 44% глобальных инцидентов».

Короневски сказал, что LockBit выбирает своих жертв, исходя из возможностей, и известен тем, что наносит удары по больницам и транспортным системам.

Больница для больных детей в Торонто в конце декабря подверглась атаке программы-вымогателя, которая задержала результаты лабораторных исследований и нанесла ущерб ее телефонным системам. LockBit принесла извинения, заявив, что один из ее «партнеров» стоит за нападением на крупнейший педиатрический медицинский центр Канады.

Федеральное бюро расследований США назвало LockBit «одним из самых активных и разрушительных вариантов программы-вымогателя в мире».

Атаки программ-вымогателей включают вредоносное программное обеспечение, используемое для вывода из строя компьютерной системы цели с целью получения денежного платежа.

LockBit считается группой, предлагающей программу-вымогатель как услугу, что означает, что она владеет штаммом программы-вымогателя и продает доступ к нему аффилированным лицам. По словам CSE, такие группы, как LockBit, поддерживают развертывание своих программ-вымогателей третьими сторонами в обмен на авансовые платежи, абонентскую плату, долю прибыли или все вместе.

В ноябре гражданину России и Канады, имеющим двойное гражданство, было предъявлено обвинение в его предполагаемом участии в глобальной кампании вымогателей LockBit. Михаил Васильев, 33 года, Брэдфорд, Онтарио. обвиняется в заговоре с целью умышленного повреждения защищенных компьютеров и передачи требований о выкупе. Он борется за его экстрадицию в США.

Бретт Кэллоу, аналитик угроз в Emsisoft, сказал, что получить четкое представление о досягаемости и мощи LockBit сложно.

Он сказал, что статистика часто основана на публикации страниц из темной сети, где банды вымогателей перечисляют неплатящих жертв, и не всегда указывают уровни активности.

«Сколько существует атак программ-вымогателей? Растут или падают цифры? На эти вопросы должно быть легко ответить, но из-за отсутствия достоверных данных это не так», — сказал он.

«Итак, у нас не только неполная картина того, как и почему атаки успешны, но и политикам трудно установить, работают ли политики борьбы с программами-вымогателями, если у них нет точных статистических данных».

CSE предупредила об ответных кибератаках со стороны России

Предупреждение CSE, вынесенное в четверг, является вторым за неделю во время обострения геополитической напряженности в отношениях с Россией.

На прошлой неделе CSE призвала к «повышенной бдительности» в отношении угрозы ответных кибератак со стороны связанных с Россией хакеров — всего через несколько часов после того, как Оттава пообещала предоставить Украине четыре основных боевых танка Leopard 2 A4.

Это предупреждение прозвучало, когда Killnet, группа, которую Канада и ее союзники называют «киберпреступной группой, связанной с Россией», пообещала преследовать страны, которые поддерживают Украину.

Ранее на этой неделе агентство Reuters сообщило, что Killnet провела кампанию по отказу в обслуживании (DDoS) против нескольких немецких веб-сайтов, чтобы отключить их в среду после того, как эта страна объявила, что отправит танки в Украину.

Агентство безопасности Германии BSI заявило, что пострадали и некоторые объекты финансового сектора, но удары не оказали существенного влияния». ***(Catharine Tunney. Intelligence agency says ransomware group with Russian ties poses 'an enduring threat' to Canada // CBC/Radio-Canada (https://www.cbc.ca/news/politics/cse-lockbit-threat-1.6734996?cmp=rss). 02.02.2023).***

***

«Окленд стал жертвой атаки программ-вымогателей, которая началась в среду вечером, сообщили в пятницу полиция и городские власти.

Департамент информационных технологий города работает с правоохранительными органами, чтобы определить масштаб и серьезность атаки.

Атака программы-вымогателя происходит, когда кто-то шифрует файлы и требует выкуп за их расшифровку. По данным Агентства кибербезопасности и

безопасности инфраструктуры США, шифрование делает файлы и системы, которые на них полагаются, непригодными для использования.

Городские власти не разглашают сумму выкупа, которую просят нападавшие.

Атака не повлияла на возможность жителей звонить в службу экстренной помощи. Она также не повлияла на финансовые данные города или пожарные ресурсы. Общественность также по-прежнему может подавать сообщения о преступлениях на городском веб-сайте.

Жители и гости города могут ожидать задержек с ответами городских властей и чиновников. Из-за атаки отдел информационных технологий отключил пострадавшие компьютерные системы.

Городские власти разрабатывают план реагирования на нападение». ***(City of Oakland Hit With Ransomware Attack // NBCUniversal Media, LLC. (https://www.nbcbayarea.com/news/local/city-of-oakland-hit-with-ransomware-attack/3154794/). 10.02.2023).***

***

«Новое исследование, проведенное NCC Group и Abnormal Security, показывает, что есть облака и немного серебра, чтобы их выровнять: атаки программ-вымогателей снизились в прошлом году, но увеличилось количество компрометаций корпоративной электронной почты — в основном для небольших компаний — и треть токсичных электронных писем прошла через их человеческие шлюзы.

По данным компании по управлению рисками NCC Group, в прошлом году количество атак программ-вымогателей сократилось на 5% — с 2667 атак в 2021 году до 2531 атаки в 2022 году — хотя в период с февраля по апрель наблюдался всплеск из-за активности LockBit во время российско украинской - войны.

В своем только что выпущенном Ежегодном мониторе угроз H1 за 2022 год, в котором отслеживаются инциденты, выявленные ее управляемой службой обнаружения и реагирования и глобальной группой реагирования на киберинциденты, группа NCC сообщила:

Промышленный сектор второй год подряд был наиболее мишенью для преступных группировок.

Северная Америка (44% атак) и Европа (35%) были наиболее целевыми регионами.

В 2022 году произошло 230 519 DDoS-атак, 45% из которых были нацелены на США, 27% из которых произошли в январе.

LockBit был ответственен за 33% атак программ-вымогателей (846), отслеживаемых NCC.

Консалтинговая компания заявила, что всплеск DDoS- атак и взломов с помощью ботнетов в начале 2022 года отчасти связан с усилением турбулентности в более широком ландшафте киберугроз, в основном благодаря российско-украинской войне.

«DDoS по-прежнему используется в качестве оружия как криминальными, так и хактивистскими группами в рамках конфликта, наряду с кампаниями по дезинформации и разрушительным вредоносным ПО, чтобы вывести из строя

критически важную национальную инфраструктуру в Украине и за ее пределами», — говорится в отчете.

LockBit лидирует в галерее мошенников

Отчасти благодаря войне в Украине LockBit и другие игроки были более активны, чем обычно:

LockBit был ответственен за 33% атак программ-вымогателей (846), отслеживаемых NCC, что на 94% больше по сравнению с его активностью в 2021 году, достигнув пика в апреле со 103 атаками. Фирма отметила, что этот всплеск предшествовал внедрению LockBit 3.0.

На BlackCat приходилось 8% от общего числа атак в прошлом году, в среднем 18 атак каждый месяц с пиком в 30 инцидентов в декабре.

Конти, аффилированная с Россией организация, занимающаяся угрозами, была самым активным злоумышленником в 2021 году, на его долю пришлось 21% всех атак. В прошлом году уровень атак снизился до 7% от всех зарегистрированных атак.

Промышленность - постоянная цель

По данным NCC Group, наиболее целевыми секторами в 2022 году были: промышленные предприятия, где пострадало 804 организации, что составляет 32% атак; потребительские циклические издания, атакованные 487 раз, что составляет 20% атак; и технологический сектор, на который было совершено 263 нападения, что составляет 10% всех атак.

Примечательно, что среди целей циклических компаний преобладали гостиничные и развлекательные предприятия, специализированные розничные торговцы, розничные торговцы домостроением и строительными товарами, а также финансовые услуги. Между тем, программное обеспечение и ИТ-услуги были наиболее целевым сектором в сфере технологий.

В отчете Мэтт Халл, глава глобального отдела анализа угроз NCC Group, сказал, что значительное количество DDoS-атак и атак вредоносного ПО, развернутых преступниками, хактивистами и другими странами, были следствием конфликта между Россией и Украиной.

«Хотя, возможно, это не тот «кибергеддон», которого некоторые ожидали от следующего крупного глобального конфликта, мы наблюдаем усиление атак, спонсируемых государством, а кибервойна оказывается решающей на этом гибридном кибер-физическом поле битвы», — сказал он.

Атаки BEC увенчались успехом, обманув треть сотрудников

В прошлом году атаки социальной инженерии стали большой новостью после того, как Cisco была скомпрометирована фишинговыми атаками, а Microsoft, Samsung, NVIDIA и Uber были взломаны Lapsu$. Уже в этом году жертвами также стали Mailchimp и Riot Games.

Компрометация деловой электронной почты преодолевает человеческие барьеры: почти треть сотрудников открывают скомпрометированные электронные письма, согласно платформе безопасности на основе искусственного интеллекта Abnormal Security, чей новый отчет об угрозах электронной почты за первое полугодие 2023 года рассматривает ландшафт угроз электронной почты с особым вниманием к возникающим рискам. сотрудниками.

Исследование, в котором изучалась статистика социальной инженерии и основывалось на данных, собранных в период с июля по декабрь прошлого года, также показало, что эти сотрудники ответили на 15% BEC в среднем. Около 36% ответов были инициированы сотрудниками, которые ранее участвовали в более ранней атаке.

Только о 2,1% известных атак сотрудники сообщили службам безопасности. Крейн Хассольд, директор по анализу угроз в Abnormal Security, сказал, что это явление объясняется несколькими факторами.

«Одной из причин является эффект свидетеля, когда сотрудники предполагают, что они не являются единственной целью атаки и, следовательно, им не нужно сообщать об электронной почте, потому что это уже наверняка сделал кто-то из коллег», — сказал он. «Некоторые сотрудники могут считать, что пока они не взаимодействуют со злоумышленником, они выполнили свой долг, даже если это лишает группу безопасности возможности предупредить других сотрудников о нападении».

Дополнительные выводы из отчета включают:

84% сообщений сотрудников о фишинговых почтовых ящиках — это либо безопасные электронные письма, либо серая почта.

Сотрудники начального уровня продаж с такими должностями, как торговый представитель и специалист по продажам, читают текстовые атаки BEC и отвечают на них в 78% случаев.

Во второй половине 2022 года почти две трети крупных предприятий подверглись компрометации цепочки поставок.

С первой по вторую половину 2022 года количество BEC-атак, нацеленных на организации малого и среднего бизнеса, выросло на 147%.

Хассолд сказал, что явление «серой почты» представляет собой побочный эффект обучения по вопросам безопасности, из-за которого группе SOC организации сообщается о значительном количестве сомнительной или нежелательной почты.

«Хотя мы пытались приучить сотрудников сообщать о вредоносных сообщениях команде безопасности, непреднамеренным последствием стало то, что команды, проверяющие эти сообщения, теперь часто перегружены просмотром невредоносных электронных писем», — сказал он.

Он добавил, что резкое увеличение числа атак SMB отражает общий рост.

«Мы смотрим на соотношение BEC-атак на 1000 почтовых ящиков, — сказал Хассолд. вторая половина года, а предприятия малого и среднего бизнеса более восприимчивы к этим атакам, поскольку они не могут вкладывать столько средств в защиту, которая могла бы их остановить».

С нетерпением жду 2023 года

Халл из NCC сказал, что в 2023 году злоумышленники сосредоточат свое внимание на компрометации цепочек поставок, обходе многофакторной аутентификации и использовании неправильно настроенных API…» ***(Karl Greenberg. New cybersecurity data reveals persistent social engineering vulnerabilities // TechnologyAdvice (https://www.techrepublic.com/article/persistent-social-engineering-vulnerabilities/). 08.02.2023).***

***

«Правительственные учреждения Соединенных Штатов и Республики Корея рассказывают о новых виденных ими тактиках программ-вымогателей, которые, по их словам, используются для сокрытия принадлежности хакеров из Корейской Народно-Демократической инфраструктура.

ПОЧЕМУ ЭТО ВАЖНО

В новом информационном бюллетене по кибербезопасности Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activity подробно описаны как исторические, так и недавно наблюдаемые тактики, методы и процедуры Северной Кореи, а также индикаторы компрометации.

По данным Агентства национальной безопасности США, Федерального бюро расследований, Агентства кибербезопасности и безопасности инфраструктуры и Министерства здравоохранения и социальных служб Республики Корея, дополнительные наблюдаемые ТТП «охватывают этапы от приобретения и покупки инфраструктуры до сокрытия принадлежности к КНДР». Разведывательная служба и Агентство безопасности обороны РК сделали вчерашнее предупреждение.

«В некоторых случаях действующие лица из КНДР выдавали себя за другие группы вымогателей, такие как группа вымогателей REvil», — сообщают агентства.

Агентства обеих стран заявляют, что неуказанная сумма доходов от выкупа криптовалюты поддерживает правительственные кибероперации КНДР, направленные против правительств США и Южной Кореи, включая оборонные информационные сети.

Следует отметить, что северокорейские киберпреступники могут угрожать раскрытием конфиденциальных данных частной медицинской компании конкурентам, если выкуп не будет выплачен.

CSA предоставляет следующие ключевые технические детали и стратегии смягчения последствий:

Приобретать инфраструктуру — субъекты КНДР создают домены, персоны и учетные записи и идентифицируют криптовалютные службы для проведения своих операций по вымогательству. Субъекты приобретают инфраструктуру, IP-адреса и домены с помощью криптовалюты, созданной в результате незаконных киберпреступлений, таких как программы-вымогатели и кража криптовалюты.

Сокрытие личности. Субъекты КНДР намеренно скрывают свою причастность, действуя под идентификацией сторонних иностранных аффилированных лиц и используя сторонних иностранных посредников для получения выкупа.

Покупка VPN и VPS. Киберсубъекты из КНДР также будут использовать виртуальные частные сети и виртуальные частные серверы или IP-адреса третьих стран, чтобы они выглядели из безобидных мест, а не из КНДР.

Получение доступа. Субъекты используют различные эксплойты распространенных уязвимостей и экспозиций для получения доступа и повышения привилегий в сетях. Недавно обнаруженные CVE, которые злоумышленники использовали для получения доступа, включают удаленное выполнение кода в программной библиотеке Apache Log4j (известной как Log4Shell) и удаленное выполнение кода в различных устройствах SonicWall.

Перемещение в горизонтальном направлении и обнаружение. После первоначального доступа киберсубъекты КНДР используют поэтапные полезные нагрузки с настроенными вредоносными программами для выполнения разведывательных действий, загрузки и скачивания дополнительных файлов и исполняемых файлов. Инсценированное вредоносное ПО также отвечает за сбор информации о жертве и отправку ее на удаленный хост, контролируемый злоумышленниками.

Используйте различные инструменты для вымогательства. Актеры использовали разработанные в частном порядке программы-вымогатели, такие как Maui и H0lyGh0st, а также были замечены за использованием или владением общедоступными инструментами для шифрования, такими как BitLocker, Deadbolt, ech0raix, GonnaCry, Hidden Tear, Jigsaw, LockBit 2.0, My Маленькие программы-вымогатели, NxRansomware, Ryuk и YourRansom.

Требование выкупа в криптовалюте. Было замечено, что кибер-актеры КНДР устанавливают выкуп в биткойнах и, как известно, общаются с жертвами через учетные записи электронной почты Proton Mail.

БОЛЬШАЯ ТЕНДЕНЦИЯ

В июле CISA, ФБР и министерство финансов опубликовали предупреждение CSA о том, что вредоносное ПО Maui используется для нападения на больницы и учреждения общественного здравоохранения.

«С мая 2021 года ФБР наблюдало и реагировало на многочисленные инциденты с программами-вымогателями Мауи в организациях сектора HPH», — заявили тогда официальные лица.

«Киберсубъекты, спонсируемые государством Северной Кореи, использовали программу-вымогатель Maui в этих инцидентах для шифрования серверов, отвечающих за медицинские услуги, включая службы электронных медицинских карт, службы диагностики, службы визуализации и службы интрасети будь то спонсируемые государством или независимые киберпреступники, желающие перейти от одной банды вымогателей к другой, финансовые рейтинги больниц уязвимы...»

По словам аналитиков Fitch, развертывание сложного кибероружия, которое ставит под угрозу оказание медицинской помощи, может повлиять на финансовый профиль больницы и «негативно повлиять на рейтинги». ***(Andrea Fox. Healthcare systems could face new DPRK ransomware tactics // Healthcare IT News (https://www.healthcareitnews.com/news/healthcare-systems-could-face-new-dprk-ransomware-tactics). 10.02.2023).***

***

«Согласно отчетам, Национальное агентство кибербезопасности Италии, ACN, предупредило организации, чтобы они защищали свои компьютерные системы, поскольку тысячи компьютерных серверов по всему миру подверглись атаке программ-вымогателей, нацеленных на серверы VMware (WMW.N) ESXi.

Роберто Бальдони, генеральный директор ACN, сообщил агентству Reuters, что цель атаки заключалась в том, чтобы найти и выявить уязвимость в программном обеспечении, добавив, что атака происходила в больших масштабах.

Представитель VMware сообщил информационному агентству, что им известно об инцидентах, и они выпустили исправления для защиты систем от раскрытия уязвимости двухлетней давности, которая использовалась еще в феврале 2021 года.

VMware призвала всех клиентов, которые не применили исправление, сделать это.

«Гигиена безопасности является ключевым компонентом предотвращения атак с целью выкупа, и клиенты, которые используют версии ESXi, затронутые CVE-2021-21974, и еще не применили исправление двухлетней давности, должны принять меры, как указано в бюллетене. — заявил в воскресенье представитель VMware.

По данным ACN, атаки были нацелены на серверы VMware в таких странах, как Франция, Финляндия, Канада и США.

Любые пострадавшие организации могут быть заблокированы в своих системах из-за программы-вымогателя…» ***(Greg Wehner. Italian cyber security agency warns organizations of ransomware attack: reports // FOX News Network, LLC. (https://www.foxbusiness.com/technology/italian-cyber-security-agency-warns-organizations-ransomware-attack-reports). 05.02.2023).***

***

«Государственная телекоммуникационная компания Тонги подверглась атаке программы-вымогателя, предупредила она клиентов в понедельник.

Tonga Communications Corporation (TCC) — одна из двух телекоммуникационных компаний страны — опубликовала в Facebook уведомление о том, что атака может замедлить административные операции.

«Подтверждено, что атака программы-вымогателя зашифровала и заблокировала доступ к части системы TCC. Это не повлияет на предоставление клиентам услуг голосовой связи и Интернета, однако может замедлить процесс

подключения новых клиентов, выставления счетов и обработки запросов клиентов», — говорится в сообщении компании.

«Мы работаем с охранными компаниями, чтобы смягчить негативное воздействие этого вредоносного ПО».

Полинезийская страна состоит из 171 острова и имеет население около 100 000 человек.

TCC контролирует все фиксированные телефонные линии и имеет 70% рынка коммутируемого и широкополосного доступа в Интернет. Имея более 300 сотрудников, она управляет примерно половиной услуг мобильной связи через службу UCall.

Эксперт по кибербезопасности Доминик Альвьери заявил, что группа вымогателей Medusa взяла на себя ответственность за атаку на TCC в понедельник.

В прошлогоднем информационном бюллетене Агентство по кибербезопасности и безопасности инфраструктуры предупредило, что Medusa работает по модели Ransomware-as-a-Service (RaaS) и обычно отдает партнерам 60% выкупа, оставляя себе остальные.

«Замеченные совсем недавно, в мае 2022 года, субъекты MedusaLocker в основном полагаются на уязвимости в протоколе удаленного рабочего стола (RDP) для доступа к сетям жертв», — написали они в совместном меморандуме с Министерством финансов США и Сетью по борьбе с финансовыми преступлениями в прошлом году.

«Актеры MedusaLocker шифруют данные жертвы и оставляют записку о выкупе с инструкциями по связи в каждой папке, содержащей зашифрованный файл».

Проблемы в Тихом океане

TCC — это последняя правительственная организация небольшого острова, атакованная киберпреступниками. Французский остров Гваделупа подвергся нападению в ноябре, а правительство Вануату — примерно в двух часах полета на самолете из Тонги — было отключено из-за атаки программы-вымогателя.

Эта атака нанесла ущерб работе парламента, полиции и канцелярии премьер-министра Вануату, а также вывела из строя почти все цифровые инструменты, используемые школами, больницами и государственными службами страны.

Газета Sydney Morning Herald сообщила, что правительство Вануату отказалось платить выкуп, и для помощи в ликвидации последствий нападения прибыли эксперты из Австралии». ***(Jonathan Greig. Tonga is the latest Pacific Island nation hit with ransomware // Recorded Future News (https://therecord.media/tonga-is-the-latest-pacific-island-nation-hit-with-ransomware/). 14.02.2023).***

***

«Город Окленд, штат Калифорния, объявил чрезвычайное положение после того, как 8 февраля атака программы-вымогателя отключила некоторые из его информационных систем.

Чрезвычайное положение было объявлено «из-за продолжающихся сбоев в работе сети в результате атаки программы-вымогателя» и позволяет городу

«ускорить закупку оборудования и материалов, при необходимости задействовать аварийных работников и отдавать приказы в ускоренном порядке».

Тип программы-вымогателя, использованной в атаке, не разглашается. Атака не затронула службы экстренной помощи, в том числе пожарные, но некоторые неаварийные системы были отключены, пока город работает над обеспечением безопасности и восстановлением служб. Автономные услуги включают в себя возможность для города собирать платежи, обрабатывать отчеты и выдавать разрешения и лицензии — так что, возможно, атака программы-вымогателя была не так уж и плоха.

Согласно обновленной информации из города Окленда, опубликованной ранее сегодня, город отметил стандартный список ответов на программы-вымогатели: найм сторонней судебно-медицинской экспертизы и сотрудничество с правоохранительными органами.

Атаки программ-вымогателей, нацеленные на местные органы власти, не новы. Местные органы власти часто рассматриваются хакерами как легко висящие плоды из-за плохой практики кибербезопасности. В 2019 году 23 местных органа власти в Техасе пострадали в результате скоординированной атаки программ-вымогателей, при этом пострадавшие отказались платить выкупы, требуемые теми, кто стоял за атаками.

Эрфан Шадаби, эксперт по кибербезопасности из специалистов по безопасности данных comforte AG. «Инцидент с программами-вымогателями, затронувший Окленд, подчеркивает суровую реальность, с которой должно столкнуться каждое государственное учреждение: атака программ-вымогателей — это не просто отдаленная возможность, а скорее вероятное неизбежное событие», — сказал SiliconANGLE «Основные цели злоумышленников, стоящих за этими атаками, — иметь возможность останавливать операции, шифровать важные операционные данные и в целом вызывать хаос в предоставлении государственных услуг».

Шон МакНи, вице-президент по исследованиям в DomainTools LLC, сказал, что неприятно видеть, как злоумышленники атакуют критически важную для жизни людей инфраструктуру, такую как больницы, высшие учебные заведения и, в данном случае, местные органы власти.

«Быстрое восстановление и запуск операций становится главным приоритетом и, к сожалению, может означать необходимость платить авторам программ-вымогателей», — добавил Макни. «Эта напряженность является причиной того, почему местные органы власти привлекательны для злоумышленников. Выплата выкупа или восстановление после нападения отвлекает критически важные ресурсы из государственного бюджета, которые должны быть использованы для улучшения жизни их избирателей». ***(Duncan Riley. City of Oakland declares state of emergency after ransomware attack // SiliconANGLE Media Inc. (https://siliconangle.com/2023/02/16/city-oakland-declares-state-emergency-ransomware-attack/). 16.02.2023).***

***

«…В новом отчете Cyber Security Works (CSW), Ivanti, Cyware и Securin говорится о разрушительных последствиях программ-вымогателей для организаций во всем мире в 2022 году. И 76% уязвимостей, которые в настоящее время используются группами программ-вымогателей, были впервые обнаружены в период с 2010 по 2019 год.

В отчете Spotlight за 2023 год, озаглавленном «Программы-вымогатели сквозь призму управления угрозами и уязвимостями», было выявлено 56 новых уязвимостей, связанных с угрозами программ-вымогателей в 2022 году, в общей сложности их число достигло 344, что на 19 % больше, чем 288, обнаруженных в 2021 году. обнаружили, что из 264 старых уязвимостей 208 имеют общедоступные эксплойты.

В Национальной базе данных уязвимостей (NVD) зарегистрировано 160 344 уязвимости, из которых 3,3% (5 330) относятся к наиболее опасным типам эксплойтов — удаленному выполнению кода (RCE) и повышению привилегий (PE). Из 5330 вооруженных уязвимостей 344 связаны с 217 семействами программ-вымогателей и 50 группами продвинутых постоянных угроз (APT), что делает их чрезвычайно опасными.

«Программы-вымогатели беспокоят каждую организацию, будь то в частном или государственном секторе, — сказал Сринивас Муккамала, директор по продуктам Ivanti. «Борьба с программами-вымогателями была поставлена на первое место в повестке дня мировых лидеров из-за растущего числа жертв, наносимых организациям, сообществам и отдельным лицам. Крайне важно, чтобы все организации действительно понимали свою поверхность атаки и обеспечивали многоуровневую защиту своей организации, чтобы они могли быть устойчивыми перед лицом растущих атак».

Хорошо финансируемые группы организованной преступности и APT выделяют членов своих команд для изучения моделей атак и старых уязвимостей, которые они могут атаковать незамеченными. В отчете Spotlight за 2023 год говорится, что злоумышленники, использующие программы-вымогатели, регулярно остаются незамеченными популярными сканерами уязвимостей, в том числе Nessus, Nexpose и Qualys. Злоумышленники выбирают, какие старые уязвимости атаковать, основываясь на том, насколько хорошо они могут избежать обнаружения.

В ходе исследования было выявлено 20 уязвимостей, связанных с программами-вымогателями, для которых пока недоступны подключаемые модули и сигнатуры обнаружения. Авторы исследования отмечают, что к ним относятся все уязвимости, связанные с программами-вымогателями, которые они выявили в ходе анализа за последний квартал, с двумя новыми дополнениями — CVE-2021-33558 (Boa) и CVE- 2022-36537 (Zkoss).

VentureBeat узнала, что злоумышленники с программами-вымогателями также уделяют первоочередное внимание поиску политик киберстрахования компаний и их лимитов покрытия. Требуют выкуп в размере максимального покрытия компании. Это открытие перекликается с недавно записанным видеоинтервью с Полом Фуртадо, вице-президентом по аналитике Gartner. Книга «Атаки программ-вымогателей: что нужно знать ИТ-руководителям для борьбы»

показывает, насколько широко распространена эта практика и почему сегодня так популярно использование старых уязвимостей в качестве оружия.

Фуртадо сказал, что «злоумышленники просили выплатить 2 миллиона долларов за программу-вымогатель. [Потерпевший] сказал плохим актерам, что у них нет двух миллионов долларов. В свою очередь, злоумышленники прислали им копию своего страхового полиса, в котором было указано, что у них есть покрытие.

«Одна вещь, которую вы должны понимать в отношении программ-вымогателей, в отличие от любого другого инцидента, связанного с безопасностью, заключается в том, что они ставят ваш бизнес на таймер обратного отсчета».

Организации среднего размера, как правило, больше всего страдают от атак программ-вымогателей, потому что с небольшим бюджетом на кибербезопасность они не могут позволить себе нанимать персонал только для обеспечения безопасности.

Sophos Последнее исследование показало, что компании производственного сектора платят самые высокие выкупы, достигающие 2 036 189 долларов, что значительно превышает средний показатель по отрасли, составляющий 812 000 долларов. Из интервью с генеральными и главными операционными директорами производителей среднего звена VentureBeat узнала, что атаки программ-вымогателей достигли уровня цифровой пандемии в Северной Америке в прошлом году и продолжают расти.

Злоумышленники с программами-вымогателями выбирают «мягкие цели» и запускают атаки, когда ИТ-персоналу среднего или малого бизнеса сложнее всего отреагировать. «Семьдесят шесть процентов всех атак программ-вымогателей происходят в нерабочее время. Большинство организаций, попавших под удар, становятся мишенью в последующие разы; вероятность того, что вы снова станете мишенью в течение 90 дней, составляет 80 %. Девяносто процентов всех атак программ-вымогателей приходится на компании с доходом менее миллиарда долларов», — сообщил Фуртадо в видеоинтервью.

Выявление старых уязвимостей — первый шаг к их использованию. Наиболее примечательные результаты исследования показывают, насколько изощренными становятся организованная преступность и группы APT в поиске самых слабых уязвимостей для использования. Вот несколько из многих примеров из отчета:

Сопоставив все 344 уязвимости, связанные с программами-вымогателями, исследовательская группа определила 57 наиболее опасных уязвимостей, которые могут быть использованы, от первоначального доступа до эксфильтрации. Для этих 57 уязвимостей теперь существует полная MITRE ATT&CK.

Группы программ-вымогателей могут использовать цепочки уничтожения для эксплуатации уязвимостей, охватывающих 81 продукт от таких поставщиков, как Microsoft, Oracle, F5, VMWare, Atlassian, Apache и SonicWall.

Цепочка убийств MITRE ATT&CK — это модель, в которой можно определить, описать и отследить каждый этап кибератаки, визуализируя каждое действие, совершаемое злоумышленником. Каждая тактика, описанная в цепочке убийств, имеет несколько методов, помогающих злоумышленнику достичь определенной цели. Эта структура также содержит подробные процедуры для

каждого метода и каталогизирует инструменты, протоколы и штаммы вредоносных программ, используемые в реальных атаках.

Исследователи безопасности используют эти фреймворки для понимания моделей атак, обнаружения уязвимостей, оценки текущих средств защиты и отслеживания групп злоумышленников.

CSW наблюдала, как более 50 групп APT запускали атаки программ-вымогателей, что на 51 % больше, чем 33 в 2020 году. калечащие атаки.

В отчете говорится, что одной из самых опасных тенденций является развертывание вредоносных программ и программ-вымогателей в качестве предвестника реальной физической войны. В начале 2022 года исследовательская группа наблюдала эскалацию войны между Россией и Украиной, когда последняя подверглась нападению со стороны групп APT, включая Gamaredon (Примитивный медведь), Nobelium (APT29), Wizard Spider (Grim Spider) и Ghostwriter (UNC1151), нацеленных на критические объекты Украины. инфраструктура.

Исследовательская группа также видела, как операторы программ-вымогателей Conti открыто заявляли о своей верности России и атаковали США и другие страны, которые поддерживали Украину. Мы считаем, что эта тенденция будет продолжать расти. По состоянию на декабрь 2022 года 50 APT-групп используют программы-вымогатели в качестве предпочтительного оружия. Среди них Россия по-прежнему лидирует с 11 подтвержденными опасными группами, которые заявляют о своем происхождении и связях с этой страной. Среди самых печально известных из этого региона — APT28/APT29.

Повторное использование открытого исходного кода в программных продуктах воспроизводит уязвимости, такие как найденная в Apache Log4j. Например, CVE-2021-45046, уязвимость Apache Log4j, присутствует в 93 продуктах от 16 поставщиков. Программа-вымогатель AvosLocker использует его. Еще одна уязвимость Apache Log4j, CVE-2021-45105, присутствует в 128 продуктах от 11 поставщиков и также используется программой-вымогателем AvosLocker.

Дополнительный анализ CVE, проведенный исследовательской группой, показывает, почему злоумышленникам удается использовать программы-вымогатели в качестве оружия в больших масштабах. Некоторые CVE охватывают многие ведущие корпоративные программные платформы и приложения.

Одной из них является CVE-2018-363, уязвимость в 26 поставщиках и 345 продуктах. Среди этих поставщиков выделяются Red Hat, Oracle, Amazon, Microsoft, Apple и VMWare.

Эта уязвимость существует во многих продуктах, включая Windows Server и Enterprise Linux Server, и связана с программой-вымогателем Stop. Исследовательская группа обнаружила, что эта уязвимость стала популярной в Интернете в конце прошлого года.

CVE-2021-44228 — еще одна уязвимость Apache Log4j. Он присутствует в 176 продуктах от 21 поставщика, в частности Oracle, Red Hat, Apache, Novell, Amazon, Cisco и SonicWall. Эта уязвимость RCE используется шестью бандами вымогателей: AvosLocker, Conti, Khonsari, Night Sky, Cheerscrypt и TellYouThePass.

Эта уязвимость также представляет интерес для хакеров, и по состоянию на 10 декабря 2022 года она была обнаружена в тренде, поэтому CISA включила ее в каталог CISA KEV.

Кибератаки с использованием программ-вымогателей становятся все более смертоносными и прибыльными, привлекая самые изощренные и хорошо финансируемые группы организованной преступности и APT во всем мире. «Субъекты угроз все чаще выявляют недостатки в кибергигиене, в том числе в устаревших процессах управления уязвимостями», — сказал Муккамала из Ivanti VentureBeat. «Сегодня многие службы безопасности и ИТ-специалисты изо всех сил пытаются определить реальные риски, связанные с уязвимостями, и поэтому неправильно расставляют приоритеты для устранения уязвимостей.

«Например, — продолжил он, — многие исправляют только новые уязвимости или обнаруженные в NVD. Другие используют только общую систему оценки уязвимостей (CVSS) для оценки и приоритизации уязвимостей».

Атакующие программы-вымогатели продолжают искать новые способы использования старых уязвимостей. Многочисленные идеи, представленные в отчете «В центре внимания» за 2023 год, помогут директорам по информационной безопасности и их командам по безопасности подготовиться к тому, что злоумышленники будут стремиться доставлять более смертоносные полезные нагрузки программ-вымогателей, которые ускользают от обнаружения, и требуют более крупных платежей за программы-вымогатели». ***(Louis Columbus. Ransomware attackers finding new ways to weaponize old vulnerabilities // VentureBeat (https://venturebeat.com/security/ransomware-attackers-finding-new-ways-to-weaponize-old-vulnerabilities/). 16.02.2023).***

***

Програми-трояни

«В Бразилии появилось еще одно вредоносное приложение для кражи денег. Усовершенствованный банковский троянец Android нацелен на бразильских пользователей платформы мгновенных платежей, известной как Pix…

Исследователи из итальянской компании Cleafy, занимающейся безопасностью финансовых технологий, говорят, что столкнулись с трояном примерно в начале этого года. Они называют трояна «PixPirate» — Pix — это успешная система мгновенного перевода денег между банковскими счетами, запущенная Центральным банком Бразилии в ноябре 2020 года. С тех пор она стала наиболее часто используемым способом оплаты в Бразилии, сообщает Bloomberg. миллиардов транзакций.

По словам Клифи, PixPirate принадлежит к новейшему поколению банковских троянцев Android, ссылаясь на его способность проводить атаки на систему автоматического перевода и автоматизировать вредоносные денежные переводы.

Бразилия имеет репутацию очага троянской активности, поддерживаемой местными киберпреступниками, стремящимися воспользоваться преимуществами населения, которое относительно рано и в больших количествах освоило онлайн-банкинг. PixPirate — не первый банковский троянец, нацеленный на пользователей Pix: в 2021 году исследователи из CheckPoint обнаружили вредоносное ПО, которое они назвали PixStealer. Тактика разработчиков троянцев на протяжении многих лет была настойчивой и изобретательной, в том числе троянец, обнаруженный в 2019 году, маскирующийся под поддельные купоны на скидку в McDonalds.

PixPirate также представляет собой законную функцию, в том числе мобильное приложение для обеспечения безопасности. Его обычный способ доставки — через приложение-капельницу. Во время установки PixPirate немедленно подталкивает пользователей к включению специальных возможностей с помощью повторяющихся всплывающих запросов. Банковские трояны регулярно пытаются получить доступ к службам специальных возможностей — функции операционной системы, позволяющей разработчикам адаптировать приложения для пользователей с ограниченными возможностями. Доступ к нему позволяет хакерам свободно перемещаться по системе Android.

PixPirate использует элемент специальных возможностей для идентификации паролей банковских счетов и использует разные модули JavaScript для каждого целевого банка, поскольку каждое банковское приложение имеет свой макет.

Исследователи Cleafy говорят, что PixPirate «похоже, все еще находится на ранних стадиях разработки», учитывая такие особенности поведения, как отправка журналов на командно-контрольный сервер и комментарии, присутствующие в коде.

Это означает, что, по их словам, возможно появление еще большего количества банковских троянцев по примеру PixPirate — троянцев, нацеленных на другие страны Латинской Америки, «или даже перемещающих свой взгляд в другие регионы». ***(Prajeet Nair. 'PixPirate' Banking Trojan Targets Brazilian Pix Users // Information Security Media Group, Corp. (https://www.govinfosecurity.com/pixpirate-banking-trojan-targets-brazilian-pix-users-a-21129). 06.02.2023).***

***

Фішингові атаки

«Социальная сеть Reddit подверглась фишинговой атаке в начале этого месяца, но технический директор Кристофер Слоу говорит, что ущерб был ограниченным, отчасти потому, что сотрудник, чьи учетные данные были скомпрометированы, быстро проинформировал команду безопасности Reddit.

В сообщении на доске Reddit r/reddit Слоу (который работает под псевдонимом u/KeyserSosa) сказал, что поздно вечером по тихоокеанскому стандартному времени 5 февраля 2023 года компании стало известно о «изощренной фишинговой кампании, нацеленной на сотрудников Reddit». Сама кампания, по-видимому, была взята из стандартной схемы фишинга —

использование поддельных подсказок для направления сотрудников Reddit на веб-сайты, напоминающие шлюзы интрасети к системам компании, после чего злоумышленники могли попытаться вытащить учетные данные и токены аутентификации.

По словам Слоу, жертвой схемы стал «один работник». В результате злоумышленник смог получить доступ к «внутренним документам, коду, а также к некоторым внутренним информационным панелям и бизнес-системам». Однако, как пишет Слоу, не было доказательств того, что злоумышленник получил доступ к «основным производственным системам», отвечающим за повседневную работу сайта и хранящим большую часть данных компании.

Несколько дней расследования не выявили каких-либо доказательств того, что частная информация была скомпрометирована во время инцидента, хотя важно иметь в виду, что нарушения часто носят более масштабный характер, чем цели изначально предполагают (или, по крайней мере, раскрывают пользователям).

Слоу признал в ответ другому пользователю Reddit, что решение сотрудника признать ошибку безопасности, вероятно, было не самым приятным опытом, хотя и позволило быстро закрыть доступ злоумышленника. Многие организации изо всех сил пытаются создать здоровую культуру кибербезопасности, при которой сотрудники чувствуют себя комфортно, признавая, что стали жертвами атаки, в значительной степени из-за страха перед последствиями. Слоу написал в последующем сообщении, что рассматриваемый сотрудник не сталкивался с карательными мерами, кроме временного отзыва учетных данных во время реагирования на инцидент, добавив, что компания «благодарна за самоотчет!»

Reddit ранее подвергался фишинговой атаке в 2018 году, после чего он реализовал требования доступа к двухфакторной аутентификации на основе токенов для определенных конфиденциальных систем. В своем посте Слоу написал, что уроки, извлеченные в результате этой предыдущей атаки, которая обнажила старые резервные копии Reddit, некоторые данные учетных записей пользователей и электронные письма с обзорами читателей, остаются полезными.

Фишинг остается одним из самых распространенных направлений киберпреступлений, все чаще используя такие тактики, как smishing (текстовый фишинг) или создание поддельных профилей в социальных сетях. Трудно найти исследования, которые не показывают организации, заваленные попытками фишинга; Фирма по сетевой безопасности SlashNext опубликовала в конце прошлого года данные, согласно которым она обнаружила более 255 миллионов фишинговых атак за шесть месяцев в 2022 году, при этом мобильные и персональные средства связи становятся все более популярной целью. Распространение инструментов для написания ИИ, таких как ChatGPT, также не сулит ничего хорошего в будущем, поскольку такая технология может позволить массово создавать более убедительные фишинговые подсказки…». ***(Tom McKay. Reddit employee self-reported phishing attack // Morning Brew, Inc. (https://www.itbrew.com/stories/2023/02/16/reddit-employee-self-reported-phishing-attack?utm_source=&utm_medium=syndication&utm_campaign=feed). 16.02.2023).***

***

«Компания по предоставлению услуг кибербезопасности Group-IB Global Pvt. Ltd. опубликовала подробности о ранее не сообщавшихся фишинговых операциях, проведенных государственным субъектом киберугроз SideWinder в период с июня по ноябрь 2021 года.

SideWinder, также известная как Rattlesnake, Hardcore Nationalist (HN2) и T-APT4, представляет собой спонсируемую государством хакерскую группу, которая, как считается, связана с правительством Индии. Группа участвовала в различных кампаниях кибершпионажа, нацеленных на ряд отраслей, включая государственные учреждения, военные организации и энергетические компании.

По данным Group-IB, в 2021 году злоумышленники пытались атаковать 61 правительственную, военную, правоохранительную и другую организацию в Афганистане, Бутане, Мьянме, Непале и Шри-Ланке (на фото). В кампании участвовали хакеры, использующие Telegram для получения информации из взломанных сетей.

В отчете «Старая змея, новая кожа: анализ APT-активности SideWinder в период с июня по ноябрь 2021 года» исследователи Group-IB подтвердили связь между группами продвинутых постоянных угроз SideWinder, Baby Elephant и Donot и описали весь арсенал кибершпионской группы., включая недавно обнаруженные инструменты.

В июне 2022 года Group-IB обнаружила новейший специализированный инструмент группы, SideWinder.AntiBot.Script, который использовался в ранее задокументированных фишинговых атаках на пакистанские организации. SideWinder отличается способностью проводить сотни шпионских операций за короткий период.

В ходе упреждающих операций по поиску угроз исследователи обнаружили архивы резервных копий в инфраструктуре, приписываемые SideWinder. В одном из архивов 2021 года было несколько фишинговых проектов, нацеленных на правительственные учреждения Юго-Восточной Азии, среди которых были поддельные сайты, имитирующие Центральный банк Мьянмы.

Основываясь на дате редактирования соответствующих фишинговых страниц, команда Group-IB смогла восстановить приблизительную хронологию фишинговых операций SideWinder в период с июня по ноябрь 2021 года. Поскольку фишинговые ресурсы были извлечены командой Group-IB из резервного архива, есть вероятность, что атаки SideWinder могли начаться раньше.

Дальнейший анализ позволил команде Group-IB составить список из 61 потенциальной цели группы, в которую входят правительственные, военные, финансовые, правоохранительные, политические, телекоммуникационные и медиа-организации в Афганистане, Бутане, Мьянме, Непале и Шри-Ланке. Неизвестно, были ли какие-либо из этих фишинговых кампаний успешными.

Исследователи также обнаружили два фишинговых проекта, имитирующих криптовалютные компании. Растущий интерес SideWinder к криптовалюте может быть связан с недавними попытками регулирования крипторынка в Индии.

Полный отчет в первую очередь предназначен для анализа среди экспертов по кибербезопасности, но он также дает интересное представление о гнусной кибер-деятельности индийского правительства. Хотя основное внимание к

хакерским атакам и киберугрозам уделяется таким странам, как Россия, Китай, Северная Корея и Иран, полезно помнить, что все страны, включая Индию и США, спонсируют эти группы и взламывают другие страны». ***(Duncan Riley. Group-IB report details previously unknown Indian-sponsored SideWinder campaign // SiliconANGLE Media Inc. (https://siliconangle.com/2023/02/15/group-ib-report-details-previously-unknown-indian-sponsored-sidewinder-campaign/). 15.02.2023).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Суд присяжных в США вынес обвинительный вердикт человеку, который организовал преступную хакерскую схему, заработав 90 миллионов долларов за счет инсайдерской торговли, управляя базирующейся в Москве фирмой, предоставляющей ИТ-услуги, связанной с российским правительством.

После 10-дневного судебного разбирательства федеральный суд присяжных в Бостоне во вторник признал 42-летнего Владислава Клюшина виновным в получении несанкционированного доступа к компьютерам, а также в мошенничестве с использованием электронных средств связи и мошенничестве с ценными бумагами. Гражданину России, которому грозит более 50 лет тюрьмы и штраф, равный удвоенной сумме личной прибыли в размере 38 миллионов долларов, которую он получил от этой схемы, должен быть вынесен приговор в мае.

«В течение почти трех лет он и его сообщники неоднократно взламывали компьютерные сети США, чтобы получить завтрашние заголовки сегодня. Они использовали эту непубличную информацию для незаконной торговли акциями сотен публичных компаний», — заявила прокурор США Рэйчел С. Роллинз. округа Массачусетс.

Прокуроры заявили, что Клюшин лично заработал на этой схеме 38 миллионов долларов, в том числе 23 миллиона долларов на своих собственных сделках и более 13 миллионов долларов на сделках, которые он совершал для других, используя их деньги, в обмен на сохранение 60% полученной прибыли.

Связаться с адвокатом Клюшина, проживающим в Бостоне Максимом Немцевым, для комментариев не удалось. Но он сказал Associated Press, что прокуратура использовала «новые теории» в деле, которые до сих пор не проверены вышестоящими судами. Клюшин подаст апелляцию, сказал он.

Прокуроры заявили, что схема взлома действовала как минимум с января 2018 года по сентябрь 2020 года и включала более 2000 различных событий, связанных с получением прибыли.

Путь Клюшина в зал суда США начался в Швейцарии, где полиция арестовала его по распоряжению американских властей в марте 2021 года, когда он отдыхал с семьей. Как это обычно бывает при задержании гражданина России за

границей, Москва подала конкурирующий запрос об экстрадиции. Швейцарские власти приняли решение в пользу Вашингтона, экстрадировав Клюшина в декабре 2021 года. Во время его первой явки в федеральный суд Бостона судья отклонил его просьбу об освобождении под залог, заявив, что он представляет «существенный риск бегства».

В обвинительном заключении, опубликованном в январе 2022 года, пятерым россиянам, в том числе Клюшину, также известному как Клюшин, было предъявлено обвинение в совершении схемы, которая использовала хакерские атаки для кражи общедоступной информации, относящейся к сотням компаний, котирующихся на Нью-Йоркской фондовой бирже и Nasdaq.

Компании, чью информацию получили мужчины, включали Capstead Mortgage, Horizon Therapeutics, IBM, Microsoft, Roku, Snap, SS&C Technologies и Tesla, согласно информации, представленной в суде.

Четырем предполагаемым сообщникам Клюшина — Ивану Ермакову, Николаю Румянцеву, Михаилу Владимировичу Ирзаку и Игорю Сергеевичу Сладкову — также предъявлены обвинения, но все они остаются на свободе. Комиссия по ценным бумагам и биржам США подала отдельную жалобу на пятерых мужчин в декабре 2021 года.

Согласно информации, представленной на суде, взлом и кража финансовой информации, не являющейся общедоступной, осуществлялась московской фирмой по ИТ-услугам и мониторингу СМИ M-13, которую Клюшин основал и возглавлял. На своем сайте фирма заявила, что среди ее клиентов есть «администрация президента Российской Федерации, правительство Российской Федерации, федеральные министерства и ведомства, региональные органы государственной исполнительной власти, коммерческие компании и общественные организации».

Среди услуг, рекламируемых M-13, были тестирование на проникновение и «эмуляция полноценной целевой атаки (красная команда APT)».

Прокуратура заявила, что M-13 использовала свои возможности атаки и «вредоносную инфраструктуру» для кражи регистрационной информации для систем, используемых сотрудниками двух неназванных поставщиков услуг. Компании используют поставщиков для подачи в SEC ежеквартальных и годовых отчетов о доходах, которые содержат предварительную информацию о том, должна ли прибыль компании превысить или не оправдать рыночные ожидания. Подозреваемым было предъявлено обвинение в использовании этой информации для прогнозирования роста или падения курса акций компании, а также в совершении сделок, призванных извлечь выгоду из этой информации.

Прокуратура сообщила присяжным, что 97% сделок, совершенных Клюшиным и его сообщниками, коррелируют с информацией о доходах, которую обрабатывают две взломанные сервисные фирмы, которые обрабатывали документы SEC. «Свидетельские показания в суде показали, что вероятность того, что эта торговая модель произойдет при отсутствии связи между торговлей и личностью агента, подающего заявку, была меньше, чем один к триллиону», — заявило Министерство юстиции.

Схема была невероятно прибыльной, с доходностью 900%, когда рынок возвращал чуть более 25%. «Клюшин и его сообщники заработали около 100

миллионов долларов на торговле прибылью из примерно 9 миллионов долларов на инвестициях с использованием инсайдерской информации, даже несмотря на то, что они потеряли около 10 миллионов долларов на торговле без прибыли», — говорится в сообщении Министерства юстиции.

Прокуратура заявила, что торговая деятельность мужчин была распределена между банками и брокерскими конторами на Кипре, в Дании, Португалии, России и США, и что группа «ввела в заблуждение брокерские фирмы относительно характера их торговой деятельности».

Одному из подозреваемых по этому делу, Ермакову, он же Ермаков, которого прокуратура называет другом Клюшина и содиректором М-13, а также российским военным, предъявлены другие обвинения во взломе, не связанные с этим делом.

В обвинительном заключении, выдвинутом против Ермакова, он обвиняется в сотрудничестве с хакерской группой ГРУ российской военной разведки, известной как Fancy Bear и APT28, для кражи информации из Национального комитета Демократической партии в рамках вмешательства России в выборы в США в 2016 году.

Ермакову также было предъявлено обвинение в том, что он был одним из предполагаемых агентов ГРУ, которых прокуратура описывает как причастных к «использованию хакерских атак для распространения личной информации сотен антидопинговых чиновников и спортсменов в попытке отвлечь внимание от спонсируемой государством российской политики». допинговая программа». ***(Mathew J. Schwartz. Russian Found Guilty of Insider Trading in Hacking Case // Information Security Media Group, Corp. (https://www.govinfosecurity.com/russian-found-guilty-insider-trading-in-hacking-case-a-21205). 15.02.2023).***

***

«Полиция конфисковала наркотики, огнестрельное оружие и 4 миллиона евро в ходе рейдов на пользователей и операторов Exclu

Многонациональная правоохранительная операция в Европе закрыла приложение для зашифрованного чата, предположительно пользующееся популярностью у организованной преступности, арестовав четыре десятка человек, включая владельцев и администраторов приложения.

Власти Германии заявляют, что расшифровали сообщения, которыми обменивались в приложении, и начали расследование в июне 2020 года. В операции участвовали полицейские из Нидерландов, Германии, Бельгии и Польши.

Власти говорят, что около 3000 пользователей зарегистрировались в Exclu, заплатив лицензионный сбор в размере 800 евро за шесть месяцев доступа. Приложение привлекло внимание немецких властей после рейда в 2019 году на бывший укрепленный военный бункер времен холодной войны в немецком городе Трабен-Трарбах, который затем использовался в качестве веб-хостинга организацией, называвшей себя Cyberbunker или CB3ROB. В Cyberbunker размещались темные веб-сайты и, по словам немецкой полиции, серверная часть Exclu…

Веб-сайт Exclu на момент публикации все еще находится в сети и рекламирует использование сквозного шифрования и возможность принимать платежи в биткойнах.

Рейд проводится на фоне возобновления опасений по поводу сквозного шифрования со стороны правительств, включая Европейскую комиссию, которая в мае предложила закон о борьбе с материалами о сексуальном насилии над детьми, которые, по мнению критиков, фактически запретят сквозное шифрование…» ***(Akshaya Asokan. European Police Shut Down Encrypted App Used by Criminals // Information Security Media Group, Corp. (https://www.govinfosecurity.com/european-police-shut-down-encrypted-app-used-by-criminals-a-21139). 07.02.2023).***

***

«Прокуратура США обнародовала обвинительный акт против высокопоставленной фигуры TrickBot

Российские операторы банковского трояна TrickBot, который позже превратился в программу-вымогатель, в четверг почувствовали трансатлантическое давление из-за санкций, введенных Соединенными Штатами и Великобританией, а также обвинительного заключения против высокопоставленного лица, раскрытого федеральной прокуратурой США в Нью-Джерси.

Впервые Министерство финансов США и Министерство финансов Великобритании совместно запретили финансовые операции с семью гражданами России, обвиняемыми в разработке и управлении вредоносным ПО TrickBot.

Прокуратура также обнародовала обвинительное заключение в отношении одного из подсанкционных лиц, Виталия Ковалева, по девяти пунктам обвинения в банковском мошенничестве или сговоре с целью совершения банковского мошенничества. Обвинения связаны с серией мошеннических транзакций, совершенных в банках США в 2009 и 2010 годах с целью перевода почти 1 миллиона долларов украденных средств, большая часть которых оказалась за границей. Ковалев является «старшей фигурой» в TrickBot, утверждает Минфин США, хотя предполагаемое мошенничество произошло до его участия в TrickBot.

Министерство финансов США заявляет, что члены группы TrickBot связаны с российскими спецслужбами и что ее деятельность «привела их в соответствие с целями российского государства и целями, ранее проводившимися российскими спецслужбами». В своем заявлении госсекретарь США Энтони Блинкен обвинил Кремль в укрывательстве таких групп, как Trickbot, назвав Россию «убежищем для киберпреступников».

Помимо Ковалева, который также ходит под ником Bentley в сети, под санкции попали Михаил Истрицкий, он же Тропа; Валентин Карягин, он же Глобус; Максим Михайлов, он же Багет; Дмитрий Плешевский, он же Изельдор; Валерий Седлецкий, он же Стрикс; и Иван Вахромеев, он же Гриб.

Санкции замораживают любые активы семи мужчин в финансовых учреждениях США или Великобритании, а также предупреждают мировую финансовую систему, чтобы избежать транзакций, которые могут быть связаны с ними. Любое иностранное финансовое учреждение, которое способствует

проведению крупной сделки или предоставляет значительные финансовые услуги любому из семи человек, само может быть подвергнуто санкциям.

«Налагая санкции на этих киберпреступников, мы посылаем им и другим лицам, причастным к программам-вымогателям, четкий сигнал о том, что они будут привлечены к ответственности», — заявил госсекретарь Великобритании по иностранным делам, делам Содружества и развитию Джеймс Клеверли.

Сочетание санкций со стороны США и. Британские регулирующие органы будут препятствовать конвертации украденных денег в твердую западную валюту для семи человек, сказал Дэйв Стетсон, бывший поверенный-советник в офисе главного юрисконсульта Управления по контролю за иностранными активами Министерства финансов. По его словам, европейские банки также, вероятно, откажутся обрабатывать транзакции, связанные с российскими мужчинами.

Трансатлантическая координация санкций против российских организаций заметно укрепилась после вторжения Москвы в Украину в феврале 2022 года. По словам Стетсона, в октябре прошлого года США и Великобритания пообещали более тесное партнерство, и сегодняшнее объявление принесло дивиденды.

Санкции также усложняют расчет для жертв, рассматривающих возможность оплаты требований хакеров-вымогателей о вымогательстве. Казначейство США оставляет за собой право применять санкции за нарушение на основании строгой ответственности, то есть ему не нужно доказывать умысел на совершение запрещенных операций. Федеральное руководство призывает компании координировать свои действия с властями при реагировании на запросы о программах-вымогателях, а это означает, что «OFAC может в какой-то форме утешить, что, основываясь на информации, доступной правительству США, объект санкций не участвует ни в каких транзакциях, — сказал Стетсон.

Он добавил, что в исключительных случаях OFAC «может дать определенную степень успокоения в связи с неиспользованием своих правоприменительных полномочий», когда есть связь.

Официальные лица США говорят, что TrickBot выбрал больницы и медицинские центры в качестве целей для атак программ-вымогателей в разгар новой пандемии коронавируса. Среди его жертв были три медицинских учреждения Миннесоты, которые были вынуждены отказать пациентам скорой помощи.

Исследователи безопасности впервые обнаружили TrickBot в 2016 году и отслеживали его эволюцию от варианта более раннего банковского троянца, получившего название Dyre или Dyreza, до вектора для программ-вымогателей Conti и Ryuk. В 2020 году газета Washington Post сообщила, что киберкомандование США предприняло операцию по разрушению ботнета TrickBot перед президентскими выборами в США, чтобы предотвратить потенциальные атаки программ-вымогателей на государственные или местные органы регистрации избирателей. Эксперты по кибербезопасности ожидали, что операция будет иметь лишь временный эффект…

Двое предполагаемых членов TrickBot уже предстали перед судами США. Южная Корея в конце 2021 года экстрадировала гражданина России Владимира Дунаева, обвинив его в разработке вредоносного ПО TrickBot путем надзора за

созданием функций внедрения в браузер, идентификации компьютеров и сбора данных. Его преследуют вместе с Аллой Витте, гражданкой Латвии, также арестованной в 2021 году и обвиненной прокуратурой в работе разработчиком TrickBot над контролем и развертыванием программ-вымогателей, получении вымогательских платежей и разработке программных инструментов для хранения украденных учетных данных. Судебное преследование Витте продолжается в Окружном суде США по Северному округу штата Огайо.

Как и в случае со многими типами вредоносных программ, операторы TrickBot усовершенствовали свой код, чтобы добавить дополнительные возможности и удовлетворить изменяющиеся требования преступников. Обновления включали использование его в качестве дроппера — инструмента для загрузки дополнительного программного обеспечения на зараженную конечную точку. Он также получил возможности веб-инъекций, что позволило ему подделывать законные банки и криптовалютные биржи.

В 2021 году TrickBot, по-видимому, начал первоначальные отношения доступа с группой программ-вымогателей Conti, предоставив ей исключительное право использовать все конечные точки, зараженные TrickBot, чтобы они могли быть заражены вредоносным ПО Conti для криптоблокировки, сообщила компания по анализу угроз Advanced Intelligence. «К концу 2021 года Conti фактически приобрела TrickBot, а несколько элитных разработчиков и менеджеров присоединились к cosa nostra программ-вымогателей», — говорится в сообщении. Позже операторы Conti выделили несколько групп, некоторые из которых продолжают использовать код, производный от TrickBot, прежде чем отказаться от торговой марки Conti в мае 2022 года.

Исследователи из Intel 471 в начале 2022 года с «высокой уверенностью» пришли к выводу, что операторы TrickBot перешли от работы над своим программным обеспечением к объединению усилий с операторами вредоносного ПО Emotet. Эти две группы уже сотрудничали ранее, когда вредоносное ПО TrickBot использовалось для возвращения Emotet после разрушительного уничтожения в 2021 году…» ***(David Perera. US and UK Sanction Members of Russian TrickBot Gang // Information Security Media Group, Corp. (https://www.govinfosecurity.com/us-uk-sanction-members-russian-trickbot-gang-a-21162). 09.02.2023).***

***

«Нідерландській поліції вдалося зламати сервіс зашифрованих повідомлень Exclu, який мав шалений попит у місцевого криміналітету. Про це пише медіа Vice. Кіберфахівці змогли проникнути на сервери компанії й відстежити все листування між різними злочинними синдикатами країни.

У результаті було заарештовано 49 осіб і проведено 79 обшуків на території Нідерландів, Бельгії, Німеччини та інших країн ЄС. Як стверджують правоохоронці, вони терпляче відстежували все листування впродовж шести місяців і збирали докази для майбутніх арештів. За деякими даними, більшість заарештованих були операторами нарколабораторій. У злочинців вилучили велику

кількість предметів розкоші, наркотиків, зброї та готівки — сумарний «чек» склав 4,3 мільйона євро.

Месенджер Exclu позиціював себе як приватне ПЗ для обміну повідомленнями, в якому застосовано передові засоби шифрування, а самі файли зберігаються тільки на пристроях користувача. За 900 євро на пів року клієнти могли абсолютно не переживати за свою безпеку.

До слова, нідерландські правоохоронці не вперше здійснюють гучні операції зі злому таємних зашифрованих сервісів. До цього поліція брала участь у зломах і відключеннях таких компаній як Ennetcom і Sky.

Часом месенджери з підвищеним рівнем конфіденційності піддаються не лише посиленому контролю з боку владних структур, але й стають мішенню хакерів. Нагадаємо — кіберзловмисники навчились читати видалені повідомлення в месенджері Signal. Дослідник Джон Джексон виявив у десктопній версії конфіденційного месенджера дві вразливості, завдяки яким хакери можуть отримувати доступ до видалених вкладень користувачів. Баги актуальні для версії Signal 6.2.0, яка працює на Windows, Linux і macOS». ***(Найбезпечніший месенджер у світі було зламано // No worries! (https://noworries.news/najbezpechnishyj-mesendzher-u-sviti-bulo-zlamano/). 08.02.2023).***

***

«9 февраля 2023 года Соединенные Штаты по согласованию с Соединенным Королевством внесли в список семь человек, которые являются частью базирующейся в России киберпреступной группировки Trickbot. Семь российских граждан, попавших под санкции, — Виталий Ковалев, Максим Михайлов, Валентин Карягин, Михаил Искрицкий, Дмитрий Плешевский, Иван Вахромеев и Валерий Седлецкий — по утверждениям Министерства финансов США являются членами базирующейся в России киберпреступной группировки Trickbot. Кроме того, их подозревают в том, что они стоят за атаками на критическую инфраструктуру, включая больницы как в США, так и в Великобритании во время пандемии Covid-19, и связаны с российскими спецслужбами.

Объявление о санкциях представляет собой самые первые санкции такого рода для Великобритании и является результатом совместного партнерства между Управлением по контролю за иностранными активами Министерства финансов США и Министерством иностранных дел, по делам Содружества и развития Великобритании; Национальный центр кибербезопасности, Национальное агентство по борьбе с преступностью; и Сокровищница Его Величества. Эта акция является последней попыткой западных стран подавить российские хакерские

операции, которые резко возросли в прошлом году в результате российско-украинского конфликта и обострения напряженности в отношениях с Западом.

Госсекретарь Энтони Блинкен выступил с поддерживающим заявлением, в котором говорится, что «Соединенные Штаты и Великобритания являются лидерами в глобальной борьбе с киберпреступностью и обязуются использовать все доступные инструменты для защиты от киберугроз». Он продолжил, заявив, что «поскольку незаконная война России против Украины продолжается, сотрудничество с нашими союзниками и партнерами как никогда важно для защиты нашей национальной безопасности». Заместитель министра финансов по борьбе с терроризмом и финансовой разведке Брайан Э. Нельсон повторил заявление Энтони Блинкена, заявив, что «киберпреступники, особенно базирующиеся в России, стремятся атаковать критически важную инфраструктуру, нацеливаются на американские предприятия и используют международную финансовую систему... Сегодня Соединенные Штаты предпринимают действия в партнерстве с Соединенным Королевством, поскольку международное сотрудничество имеет ключевое значение для борьбы с российской киберпреступностью».

Трикбот

Trickbot, впервые идентифицированный исследователями безопасности в 2016 году, представлял собой троянский вирус, который произошел от трояна Dyre. Dyre — это троян для онлайн-банкинга, управляемый физическими лицами из Москвы, Россия, который начал атаковать нероссийские компании и организации в середине 2014 года. Dyre и Trickbot были разработаны и управлялись группой киберпреступников для кражи финансовых данных. Троянские вирусы Trickbot заразили миллионы компьютеров-жертв по всему миру, включая компьютеры американских компаний и отдельных жертв. С тех пор он превратился в модульный набор вредоносных программ, который дает Trickbot Group возможность проводить различные незаконные кибер-действия, включая атаки программ-вымогателей. В разгар пандемии COVID-19 в 2020 году Trickbot атаковал больницы и медицинские центры, запустив волну атак программ-вымогателей на больницы в США, Великобритании и Ирландии. В ходе одной из этих атак группа Trickbot развернула программу-вымогатель против трех медицинских учреждений Миннесоты, нарушив работу их компьютерных сетей и телефонов и вызвав перенаправление машин скорой помощи. Члены Trickbot Group публично злорадствовали по поводу легкости нападения на медицинские учреждения и скорости, с которой группе выплачивались выкупы.

Обозначения новых санкций OFAC

Согласно заявлению OFAC Виталий Ковалев (он же онлайн-прозвище «Бентли» и «Бен»), Максим Михайлов (он же онлайн-прозвище «Багет»), Валентин Карягин (он же онлайн-прозвище «Глобус»), Михаил Искрицкий (он же онлайн-псевдоним «Тропа»), Дмитрий Плешевский (он же онлайн-псевдоним «Изельдор»), Иван Вахромеев (он же онлайн-псевдоним «Гриб») и Валерий Седлецкий (он же онлайн-псевдоним «Strix») из Trickbot Group предположительно связаны с российскими спецслужбами. Кроме того, их действия в качестве члена Trickbot

Group якобы были направлены против правительства США и американских компаний.

OFAC назначило каждого из этих лиц в соответствии с исполнительным указом (EO) 13694 с поправками, внесенными EO 13757, за оказание материальной помощи, спонсирование или предоставление материальной или технологической поддержки, товаров или услуг для или в поддержку описанной деятельности. в подразделе (a)(ii) раздела 1 EO 13694 с поправками…

Санкции Великобритании

Те же семь человек были включены в список в Великобритании в соответствии с Положением о кибербезопасности (санкциях) (выход из ЕС) 2020 года на основании участия, финансовой или технической помощи или иного содействия кибердеятельности, которая:

подрывает или намеревается подорвать целостность, процветание или безопасность Великобритании или другой страны;

прямо или косвенно причиняет или намеревается причинить экономический ущерб или нанести ущерб коммерческим интересам тех, кого затрагивает деятельность;

подрывает или намеревается подорвать независимость или эффективное функционирование международной организации или неправительственной организации или форума, полномочия или цели которых связаны с управлением международным спортом или Интернетом; или иным образом затрагивает значительное число лиц неизбирательным образом.

В соответствии с этими санкциями запрещено предоставлять средства физическим лицам, например, для оплаты программ-вымогателей, в том числе в криптоактивах. Каждому человеку также запрещен въезд в Великобританию в соответствии с запретом на поездки…» ***(Jonathan Cross, Christopher Boyd, Brittany Crosby-Banyai, Aba Edwards-Idun, Kelly Adams, Chris Arima. The United States and United Kingdom Issue Historic Joint Cyber Sanctions // Herbert Smith Freehills (https://hsfnotes.com/sanctions/2023/02/15/the-united-states-and-united-kingdom-issue-historic-joint-cyber-sanctions/#page=1). 15.02.2023).***

***

Технічні аспекти кібербезпеки

«Google випустила першу версію Android 14 для розробників. Тепер додатки повинні вказувати, яким чином вони мають намір використовувати певні функції пристрою, обмін даними буде обмежений, а додаткові файли, що завантажуються додатками, будуть мати права тільки для читання (read-only).

Розробники розповіли, що завдяки використанню механізму Runtime receivers, орієнтовані на Android 14 додатки, повинні будуть заявляти про те, що їм потрібно отримати інформацію від інших додатків. В іншому випадку вони будуть обмежені лише системними broadcast'ами.

Щоб додатково ускладнити перехоплення конфіденційної інформації, під час обміну даними між додатками буде обмежено надсилання «намірів» (intents), які не

мають конкретного одержувача. Фактично це означає, що хакер більше не зможе перехоплювати «наміри», відправлені іншими додатками, і читати їхній вміст.

Ще однією важливою захисною функцією в Android 14 стане більш безпечне завантаження динамічного коду, яке обмежить будь-які файли, що завантажуються додатком, режимом read-only. За задумом розробників, це має запобігти деяким сценаріям впровадження коду за допомогою маніпуляцій виконуваними файлами». ***(Розробники Android 14 винайшли спосіб перемогти віруси // No worries! (https://noworries.news/rozrobnyky-android-14-vynajshly-sposib-peremogty-virusy/). 13.02.2023).***

***

«…Сегментация сети является важным компонентом кибербезопасности. Он включает в себя разделение сети на более мелкие и более безопасные сегменты, которые могут помочь защититься от кибератак. Внедряя сегментацию сети, предприятия могут уменьшить поверхность атаки и ограничить потенциальный ущерб, который может быть вызван успешной атакой.

Одним из основных преимуществ сегментации сети является то, что она помогает ограничить распространение вредоносных программ. Разделение сети на более мелкие сегменты затрудняет распространение вредоносных программ из одного сегмента в другой. Это означает, что если вредоносному ПО удастся проникнуть в один сегмент сети, вероятность его распространения на другие части сети будет меньше, что снизит общее воздействие атаки.

Сегментация сети также помогает защитить конфиденциальные данные. Изолируя конфиденциальные данные в отдельном сегменте сети, предприятия могут гарантировать, что они недоступны для неавторизованных пользователей. Это может быть особенно важно для компаний, которые работают с конфиденциальной информацией, такой как личные данные, финансовая информация или интеллектуальная собственность.

Еще одно преимущество сегментации сети заключается в том, что она позволяет более эффективно отслеживать и обнаруживать кибератаки. Разделив сеть на более мелкие сегменты, компаниям будет проще определить источник атаки и принять соответствующие меры для его сдерживания. Это может помочь уменьшить общее воздействие атаки и свести к минимуму ущерб.

Сегментация сети также может помочь предприятиям соблюдать нормативные требования. Например, некоторые отрасли обязаны соблюдать такие правила, как Закон о переносимости и подотчетности медицинского страхования (HIPAA) или Стандарт безопасности данных индустрии платежных карт (PCI-DSS). Сегментация сети может помочь предприятиям соблюдать эти правила, обеспечивая безопасное хранение и передачу конфиденциальной информации.

Внедрение сегментации сети может быть сложным процессом, и важно работать с экспертом по кибербезопасности, чтобы убедиться, что все сделано правильно. Предприятиям необходимо оценить свою сетевую архитектуру и определить критические активы, которые необходимо защитить. Они также должны учитывать различные типы трафика, который будет проходить через сеть, и способы его эффективной сегментации.

В заключение, сегментация сети является ключевым компонентом кибербезопасности. Разделив сеть на более мелкие и более безопасные сегменты, предприятия могут уменьшить поверхность атаки и ограничить потенциальный ущерб, который может быть вызван успешной атакой. Сегментация сети также помогает защитить конфиденциальные данные, улучшить мониторинг и обнаружение кибератак и обеспечить соблюдение нормативных требований. Компании должны работать с экспертом по кибербезопасности, чтобы эффективно реализовать сегментацию сети…» ***(Ismail Tasdelen. The Importance of Network Segmentation for Cybersecurity // Medium (https://systemweakness.com/the-importance-of-network-segmentation-for-cybersecurity-8c4492f07e05). 01.02.2023).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Напоминание: реальные атаки часто фокусируются на небольшом подмножестве известных уязвимостей

В последнее время преступники отдают предпочтение двум типам атак: использованию протокола удаленного рабочего стола и проникновению в облачные базы данных.

Так предупреждает киберстраховщик Coalition, основываясь на доказательствах, собранных с помощью годовых данных по андеррайтингу и претензиям, сканировании миллиардов IP-адресов и глобальной сети приманок, которыми она управляет.

Эксперты по безопасности давно предупреждают, что преступники, особенно брокеры начального доступа и группы вымогателей, склонны использовать RDP.

Несмотря на неоднократные предупреждения о том, что организациям, использующим RDP, необходимо заблокировать его, Coalition сообщает, что основная активность злоумышленников по сканированию по-прежнему заключается в поиске открытого или плохо защищенного доступа к RDP.

Плохо защищенные хранилища больших данных также остаются главной целью вымогателей. «Базы данных Elasticsearch и MongoDB имеют высокий уровень компрометации, и сигналы показывают, что большое их количество было захвачено атаками программ-вымогателей», — сообщает Coalition.

В более широком плане Тиаго Энрикес, вице-президент по исследованиям Coalition, говорит, что результаты напоминают о том, что, несмотря на то, что ежемесячно обнаруживаются тысячи новых уязвимостей, злоумышленники, скорее всего, нацелятся лишь на небольшой набор из них. Опять же, когда злоумышленники находят что-то, что работает, они часто предпочитают тратить свое время на то, чтобы заставить это работать, а не придумывать совершенно новую тактику. Это касается как преступников, так и нападающих на национальные государства, и, конечно, иногда один подрабатывает другим.

В прошлом году разведывательный альянс Five Eyes, в состав которого входят Австралия, Канада, Новая Зеландия, Великобритания и США, выпустил совместный бюллетень с подробным описанием 15 наиболее часто используемых уязвимостей, которые они видели в реальных атаках за предыдущий год. Сообщение для организаций: сначала исправьте эти недостатки, если вы еще этого не сделали, поскольку они, скорее всего, станут мишенью для злоумышленников.

Это полезная информация, но, конечно же, это всего лишь один из источников информации, и каждой организации необходимо обращаться к нескольким источникам, чтобы определить, какие системы следует устанавливать в первую очередь. Как сообщает Национальный центр кибербезопасности Великобритании: «Внесение исправлений остается наиболее важной вещью, которую вы можете сделать для защиты своей технологии, и именно поэтому применение исправлений часто описывается как «выполнение основ».

Но дисциплина устранения ошибок, более известная как управление уязвимостями, сталкивается с многочисленными препятствиями.

Отчасти это потому, что есть так много свежих ошибок, которые нужно исправлять. В прошлом году в Национальной базе данных уязвимостей США, которую ведет Национальный институт стандартов и технологий, было зарегистрировано 25 059 новых распространенных уязвимостей и экспозиций, или CVE.

По данным CVE Details, около 10% всех уязвимостей представляют собой критический риск, получив девять или более баллов по 10-балльной общей системе оценки уязвимостей.

Основываясь на тенденциях CVE за последнее десятилетие, Coalition прогнозирует, что в этом году ежемесячно будет появляться около 2000 новых CVE, «в том числе 270 уязвимостей с высокой степенью серьезности и 155 уязвимостей критического уровня». Это будет на 13% больше, чем ежемесячные объемы, наблюдаемые в 2022 году.

Это множество ошибок, которые ИТ-команды должны расставить по приоритетам, а затем протестировать и внедрить в производственные системы.

Чтобы решить эту проблему программно, исследовательская фирма Gartner рекомендует компаниям внедрить программу непрерывного управления подверженностью угрозам, также известную как CTEM, которая рассматривает как активы внутри организации, так и информацию об уязвимостях, сверяясь с регионом организации, отраслью и активами.

При правильном подходе у организаций будет надежная система, позволяющая узнать, какие уязвимости нужно исправить или иным образом смягчить в первую очередь, чтобы наилучшим образом свести к минимуму их воздействие.

Поддержание быстрой частоты установки исправлений может иметь огромные преимущества с точки зрения снижения риска. Основываясь на обзоре новых уязвимостей, обнаруженных в прошлом году, Coalition выяснила, что если недавно обнаруженная уязвимость была использована, то в большинстве случаев это происходило менее чем через 30 дней после того, как подробности о ней стали достоянием общественности. Если уязвимость не была использована в течение 90

дней после того, как она стала достоянием общественности, скорее всего, она не стала целью.

Таким образом, вместо того, чтобы беспокоиться о большом и постоянно растущем числе новых CVE, организациям следует сосредоточиться на том, что с ними делать. «Когда растущее число уязвимостей становится непреодолимым, организациям необходимо сосредоточиться на небольшом количестве уязвимостей, которые фактически эксплуатируются в дикой природе», — говорит Энрикес из Coalition». ***(Mathew J. Schwartz. Cyber Insurer Sees Remote Access, Cloud Databases Under Fire // Information Security Media Group, Corp. (https://www.govinfosecurity.com/blogs/cyber-insurer-sees-remote-access-cloud-databases-under-fire-p-3369). 03.02.2023).***

***

«Кіберспеціалісти IT-компанії Unciphered знайшли спосіб зламати апаратний криптогаманець OneKey за одну секунду. Як розповіли експерти на своєму YouTube-каналі, OneKey виявився вразливим для перехоплення мнемонічної фрази в незашифрованому вигляді.

Гаманець зовсім не шифрує дані, що передаються із зашифрованої частини на центральний процесор. Вторгнувшись на апаратному рівні в роботу гаманця, аналітики змогли обдурити пристрій, змусивши його повернутись до заводських налаштувань. Внаслідок такого «обнулення», експерти змогли за секунду перехопити сід-фразу гаманця — саме завдяки їй зловмисник може безперешкодно переказувати криптовалюту на будь-яку адресу.

За словами спеціалістів Unciphered, виявлений експлойт є надзвичайно критичним для безпеки гаманців OneKey. Ймовірно, представники OneKey так не вважають, оскільки заплатили експертам Unciphered всього $ 10 000, що вважається малою сумою за виявлену вразливість такого масштабу. Втім, засновник OneKey Іші Ванг запевнив криптоспільноту, що розробники вже підготували оновлення, яке вирішить проблему…» ***(Спеціалісти з кібербезпеки розкрили схему, як зламати криптовалютний гаманець за одну секунду // No worries! (https://noworries.news/speczialisty-z-kiberbezpeky-rozkryly-shemu-yak-zlamaty-kryptovalyutnyj-gamanecz-za-odnu-sekundu/). 10.02.2023).***

***

«На смартфонах iPhone виявлені вразливості, які дають хакеру можливість повністю відформатувати накопичувач будь-якого пристрою, а перед цим отримати доступ до фотографій, повідомлень, мікрофону та камери жертви. Про це повідомляє Dark Reading.

Зазначається, що компанія Apple самостійно внесла експлойти до бази даних під двома номерами: CVE-2023-23530 та CVE-2023-23531. Дослідник компанії Trellix Остін Еммітт зазначив, що нові вразливості «дозволяють обійти підпис коду для виконання довільного скрипту», тобто дадуть можливість зловмисникові проводити самостійні дії на гаджеті жертви.

Збій виникає через систему NSPredicate, спочатку створену для того, щоб розробники додатків могли фільтрувати списки об’єктів на пристрої. «Однак

можливість динамічно генерувати та запускати код на iOS весь цей час була офіційною функцією», – констатував Еммітт.

Дослідник запевнив, що використовувати вразливість можна тільки якщо зловмисник вже має доступ до пристрою. Отримання доступу може бути реалізовано через фішинг чи інші методи соціальної інженерії, пояснив Еммітт». ***(Андрій Неволін. Хакери знайшли спосіб віддалено видаляти всі дані на iPhone // T4 (https://t4.com.ua/tech/hakery-znajshly-sposib-viddaleno-vydalyaty-vsi-dani-na-iphone/). 26.02.2023).***

***

«Cisco подтвердила, что исправила серьезную уязвимость, которая влияла на среду размещения приложений IOx.

Cisco IOx — это среда приложений, позволяющая последовательно развертывать приложения, независимые от сетевой инфраструктуры и инструментов Docker для разработки. Он используется широким кругом предприятий, от производства до энергетики и государственного сектора.

Уязвимость, отслеживаемая как CVE-2023-20076, позволяла злоумышленникам сохраняться в операционной системе, получая таким образом возможность удаленного выполнения команд.

«Злоумышленник может воспользоваться этой уязвимостью, развернув и активировав приложение в среде размещения приложений Cisco IOx с помощью созданного файла полезной нагрузки активации», — говорится в сообщении Cisco (открывается в новой вкладке) в своих рекомендациях по безопасности.

Затронуты пользователи, работающие под управлением IOS XE без встроенной поддержки Docker, а также пользователи, использующие промышленные маршрутизаторы ISR серии 800, вычислительные модули CGR1000, промышленные вычислительные шлюзы IC3000, промышленные маршрутизаторы WPAN IR510 и конечные точки точек доступа Cisco Catalyst (COS-AP) (открывается в новая вкладка).

Компания добавила, что коммутаторы Catalyst серии 9000, программное обеспечение IOS XR и NX-OS, а также продукты Meraki не затронуты этой уязвимостью.

Предупреждение об этой уязвимости заключается в том, что субъекты угрозы уже должны быть аутентифицированы как администратор уязвимых систем.

Тем не менее, исследователи из Trellix, которые первыми обнаружили уязвимость, заявили, что мошенники могут легко связать эту уязвимость с другими в своих вредоносных кампаниях. Аутентификацию можно получить с помощью учетных данных для входа по умолчанию (многие пользователи никогда их не меняют), а также с помощью фишинга и социальной инженерии.

После аутентификации CVE-2023-20076 можно использовать для «неограниченного доступа, что позволяет вредоносному коду скрываться в системе и сохраняться при перезагрузках и обновлениях прошивки».

«Обход этой меры безопасности означает, что если злоумышленник воспользуется этой уязвимостью, вредоносный пакет будет продолжать работать до

тех пор, пока устройство не будет сброшено до заводских настроек или пока оно не будет удалено вручную».

Хорошей новостью является то, что до сих пор нет доказательств того, что уязвимость используется в дикой природе, но тем не менее, если вы используете это решение, убедитесь, что оно обновлено до последней версии». ***(Sead Fadilpašić. Cisco fixes security flaw that could have allowed sneaky hacking // Future US, Inc (https://www.techradar.com/news/cisco-fixes-security-flaw-that-could-have-allowed-sneaky-hacking). 03.02.2023).***

***

«Корпорация Intel устранила несколько уязвимостей, обнаруженных в своих расширениях Software Guard Extensions (SGX), и теперь призывает пользователей как можно скорее установить исправление.

Недостатки затрагивают «широкий спектр продуктов Intel», включая процессоры Xeon, сетевые адаптеры и программное обеспечение. Всего в Intel Security Center была добавлена 31 рекомендация, в том числе пять CVE.

Из этих пяти две представляют собой уязвимости повышения привилегий, которые могут позволить злоумышленникам повысить привилегии своих учетных записей на целевых конечных точках (откроется в новой вкладке) и использовать их для кражи конфиденциальных данных. Ирония здесь ощутима, намекает издание, потому что SGX — это функция, «которая должна обеспечивать безопасную обработку конфиденциальных данных внутри зашифрованных областей памяти, известных как анклавы».

Третий недостаток, отслеживаемый как CVE-2022-38090, представляет собой уязвимость со средним рейтингом, затрагивающую, в частности, процессоры 3-го поколения Xeon Scalable. Согласно Intel, «неправильная изоляция общих ресурсов в некоторых процессорах Intel при использовании Intel Software Guard Extensions может позволить привилегированному пользователю потенциально включить раскрытие информации через локальный доступ».

По словам Intel, лучший способ действий — обновить прошивку вашего устройства.

Четвертая уязвимость, отслеживаемая как CVE-2022-33196, представляет собой уязвимость высокой степени серьезности, которая также затрагивает процессоры Xeon Scalable 3-го поколения, а также процессоры Xeon D. Компания добавила, что исправления в виде обновлений BIOS и микрокода уже в пути.

Пятая уязвимость касается комплекта разработки программного обеспечения (SDK) SGX. По словам Intel, несмотря на низкий уровень серьезности, мошенники могут использовать его для кражи конфиденциальных данных. Обновление тоже на подходе.

SGX, которому уже восьмой год, «изобилует уязвимостями», говорится в публикации, добавляя, что этот инструмент устарел в ориентированных на клиента чипах процессоров Core 11-го и 12-го поколения». ***(Sead Fadilpašić. Intel is patching a load of serious software security holes // Future US, Inc. (https://www.techradar.com/news/intel-is-patching-a-load-of-serious-software-security-holes). 16.02.2023).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Группа Т1 представила систему видеоконференцсвязи Dion с постквантовой защитой данных. Сервис стал первой российской ВКС-системой, которая на программном уровне противостоит кибератакам с применением квантовых компьютеров. Об этом RB.RU рассказали разработчики.

Поставщиком решения выступил разработчик комплексных продуктов кибербезопасности на основе постквантовых алгоритмов — компания QApp.

В компании заявили, что постквантовое шифрование — многообещающее направление в сфере кибербезопасности, продукты которого активно используют во многих странах для защиты государственной и коммерческой тайны, персональных и финансовых данных.

Во время пилотного проекта компании добавили в Dion постквантовый VPN. Это позволило в тестовом режиме защитить видеоканал передачи данных от атак с использованием как классических, так и квантовых компьютеров.

Участникам конференции также удалось обеспечить защищенный обмен данными без использования дополнительного оборудования на расстоянии 1,8 тыс. км». ***(Карина Пардаева. В России впервые протестировали постквантовую защиту для видеоконференцсвязи // rb.ru (https://rb.ru/news/t1-dion/). 16.02.2023).***

****