**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

№ 1 (січень)

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.– №1 (січень) . – 229 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

Стан кібербезпеки в Україні 4
Кібервійна проти України 6
Міжнародне співробітництво у галузі кібербезпеки 24
Світові тенденції в галузі кібербезпеки 30
Сполучені Штати Америки та Канада 62
Країни ЄС та Великобританія 86
Австралія та Нова Зеландія 91
Російська Федерація та країни ЄАЕС 93
Інші країни 93
Кібервійни та протидія зовнішній кібернетичній агресії 94
Створення та функціонування кібервійськ 101
Кіберзахист критичної інфраструктури 104
Кіберзахист закладів охорони здоров'я 112
Захист персональних даних та соціальні мережі 114
Кібербезпека та хмарні технології 139
Кібербезпека Інтернету речей. Штучний інтелект 140
Кіберзлочинність та кібертероризм 148
Діяльність хакерів та хакерські угруповування 157
Вірусне та інше шкідливе програмне забезпечення 167
Фішингові атаки 192
Операції правоохоронних органів та судові справи проти кіберзлочинців 195
Технічні аспекти кібербезпеки 199
Виявлені вразливості технічних засобів та програмного забезпечення 199
Технічні та програмні рішення для протидії кібернетичним загрозам 211
Питання криптографії 224

«Антипіратська Ініціатива «Чисте небо», до складу якої входять найбільші гравці медіаринку України, підсумувала 2022 рік та розповіла про важливі кроки на шляху до формування культури споживання легального контенту і боротьби з піратським бізнесом. Через повномасштабну війну рф в Україні, активна діяльність ІЧН та певні проєкти ініціативи були призупинені. Разом з тим, зусиллями членів-учасників було зроблено чимало важливих справ, які розвивають медіаринок, допомагають в боротьбі на інформаційному фронті та наближають Перемогу.

«Попри виклики повномасштабного вторгенння рф в Україну, Ініціатива «Чисте небо» змогла переналаштувати роботу в нових реаліях, запустила чимало важливих ініціатив та продовжує активну боротьбу на інформаційному фронті. Наш фокус змістився і ресурсами компаній-учасниць Ініціативи ми докладаємо максимальних зусиль, аби, першочергово, протидіяти ворожій пропаганді, оперативно реагувати на загрози інформаційній безпеці України та впроваджувати необхідні зміни в медійному просторі. Віримо, що 2023 рік стане роком абсолютної Перемоги, а на ІЧН чекає ще більше важливих проєктів та позитивних змін», – прокоментував керівник ініціативи «Чисте небо» В'ячеслав Мієнко.

У 2023 році ІЧН ставить перед собою не менш амбітні завдання, які зміцнюватимуть процеси захисту інтелектуальної власності в Україні, активно протидіятимуть піратству та захищатимуть інфопростір України. Зокрема, будуть реалізовані законодавчі зміни, продовжуватиметься тісна співпраця з кіберполіцією та СБУ щодо протидії незаконному поширенню медіаконтенту, відбуватиметься подальше залучення органів прокуратури до активної боротьби з піратством у межах кримінальних проваджень тощо.

Про нові кримінальні провадження

У 2022 році було зареєстровано 19 нових кримінальних проваджень, ініційованих групою 1+1 media, за якими здійснюються слідчі дії та триває документування. Ще ряд поданих заяв перебуває на розгляді правоохоронців. До слова, у 2021 році кількість кримінальних проваджень, що стосуються порушень у сфері інтелектуальної власності, склала 11 випадків. Більшість нових кейсів стосуються порушників суміжних прав, які також забезпечують ретрансляцію заборонених в Україні телеканалів країни-агресора.

Знаковим кейсом минулого року стало відкриття кримінального провадження та проведення активних слідчих дій щодо CDN-хостингу (відеобалансеру) VOD-контенту. Також знову відкрито кримінальне провадження щодо фактів фінансування піратства.

З травня 2022 року відновлено повноцінне супроводження кримінальних проваджень на етапах досудового розслідування та участь у судових засіданнях.

Протягом 2022 року правоохоронцями проведені обшуки, в ході яких вилучено обладнання, техніка, засоби зв'язку у 14 кримінальних провадженнях. Загалом оголошено підозри 11 фігурантам кримінальних проваджень, до суду спрямовані два обвинувальні акти і одержано обвинувальний вирок суду по одній справі.

Про протидію ворожій пропаганді

Як вже зазначалося вище, учасники ІЧН протягом року ефективно співпрацювали з правоохоронними органами – Національною поліцією та СБУ – щодо припинення діяльності осіб чи компаній, які не лише порушують авторські та суміжні права, але й ведуть заборонену інформаційну діяльність, надаючи доступ глядачам до каналів країни-агресора.

Так, у лютому-березні 2022 року члени ІЧН разом з Міністерством культури та інформаційної політики України брали активну участь у формуванні переліків фізичних та юридичних осіб рф, причетних до медіаіндустрії країни-агресора. В результаті цього процесу були застосовані санкції, в тому числі й міжнародні, до ряду пропагандистів, які просувають проросійські наративи в інфополі. Серед таких осіб – олігархи Роман Абрамович та Герман Хан, генеральний директор «Першого каналу» Костянтин Ернст та інші.

Крім цього, з метою протидії масовій дезінформації з боку росії, протягом 2022 року члени ініціативи системно збирали інформацію, яка була використана при накладанні санкцій Європейського Союзу щодо заборони супутникового мовлення телеканалів рф та ретрансляції цих каналів європейськими кабельними операторами.

Законотворчість та GR

Учасники ІЧН долучились до прийняття ВРУ Закону України «Про медіа», який містить окремі положення, направлені на посилення боротьби з піратством в Україні.

До того ж триває робота по внесенню змін у законодавство про рекламу, які направлені на заборону розміщення реклами на піратських ресурсах (зокрема, включених в міжнародну базу даних WIPO ALERT). А частину необхідних для успішної боротьби з інтернет-піратством положень імплементовано у новій редакції Закону України «Про авторське право і суміжні права», що була прийнята ВРУ.

Додатково налагоджена робота з Комітетом гуманітарної політики ВР щодо доопрацювання урядового законопроєкту № 5970 «Про захист послуг, що надаються із застосуванням системи умовного доступу». Йдеться про імплементацію європейських норм щодо забезпечення заходів протидії застосуванню незаконних систем умовного доступу.

Співпраця з міжнародними партнерами

Командою Ініціативи «Чисте небо» підготовлено звернення Голові Національної ради з питань телебачення та радіомовлення – Представнику України в CDMSI (Керівному комітеті Ради Європи з питань медіа та інформаційного суспільства) щодо оновленого розділу про Україну в порівняльному дослідженні Ради Європи «Блокування, фільтрування та видалення незаконного контенту в мережі Інтернет».

Крім цього, до «Торгового представництва США» (USTR) подані коментарі щодо стану захисту авторського права і проблем правозастосування в Україні для щорічного «Спеціального звіту 301» (Comments and Notice of a Public Hearing Regarding the 2021 Special 301 Review).

Взаємодія з рекламним ринком (IAB Ukraine)

Восени 2022 року на запит рекламного ринку було відновлено формування блеклистів (списку сайтів, до яких є претензії правовласників, переліку провайдерів ТБ послуги, до яких є претензії правовласників blacklists.org.ua), та їх доведення до учасників ринку інтерактивної реклами.

За активного сприяння IAB Ukraine, проведено спільне обговорення з представниками гемблінгової індустрії («КОСМОЛОТ») щодо необхідності відмови від практики розміщення реклами на сайтах піратських онлайн-кінотеатрів та надані конкретні практичні рекомендації, як це зробити…» ***(Боротьба з піратством в Україні: підсумки 2022 року // Broadcast (http://broadcast.net.ua/ru/tech-articles/8350-borotba-z-piratstvom-v-ukraini-pidsumky-2022-roku). 23.01.2023).***

***

«Очільник Держспецзв'язку України Юрій Щиголь пропонує створити єдину глобальну організацію, яка б допомагала ділитися інформацією про загрози та готуватися до майбутніх кібератак. Він наголосив, що росія атакує інфраструктуру України та прагне створити максимальний хаос у світі.

На думку українських чиновників, створення «Кібер Організації Об'єднаних Націй» є одним з низки зусиль, які підтримає світова спільнота. Оскільки росія поєднує кібератаки з ракетними ударами, щоб завдати шкоди мирним громадянам у зимові місяці.

- Нам потрібна «Кібер ООН», нації, об'єднані в кіберпросторі, щоб захистити себе, ефективно захистити наш світ у майбутньому, кіберсвіт і наш реальний, звичайний світ. Що нам дійсно потрібно в цій ситуації, так це хаб або місце, де ми можемо обмінюватися інформацією, підтримувати один одного та взаємодіяти, - пояснив Юрій Щиголь.

За його словами, після року постійних російських кібератак на українську критично важливу інфраструктуру, таку, як енергетичні системи та супутниковий зв'язок, існує потреба в «єдиному просторі, єдиному кіберпросторі», спільному для країн «цивілізованого світу». ***(Україна пропонує створити «Кібер ООН», щоб протистояти російським хакерським атакам // Маю право (https://mayupravo.com/news/view/ukrayina-proponue-stvoriti-kiber-oon-schob-protistoyati-rosiyiskim-hakerskim-atakam-a73476/). 17.01.2023).***

***

Кібервійна проти України

«В Україні зареєстрували та дослідили понад 1 500 кібератак від початку повномасштабного вторгнення росії. Більшість із них - з боку країни-агресора.

Про це повідомляє Державна служба спеціального зв'язку та захисту інформації.

Повідомляється, що у період від вересня по грудень 2022 року в Україні діяли такі російські та проросійські хакерські угрупування:

ARMAGEDDON/GAMAREDON/PRIMITIVE BEAR (ФСБ росії, активність відслідковується за ідентифікатором UAC-0010)

SANDWORM (Головне управління Генерального штабу Збройних сил росії (ГРУ), активність відслідковується за ідентифікатором UAC-0082)

APT28/FANCY BEAR (ГУ ГШ ЗС рф (ГРУ), активність відслідковується за ідентифікатором UAC-0028)

APT29/COZY BEAR (Служба зовнішньої розвідки України рф, активність відслідковується за ідентифікатором UAC-0029)

UNC1151/ GHOSTWRITER (Міністерство оборони білорусі, активність відслідковується за ідентифікатором UAC-0051)

XAKNET, KILLNET, Z-TEAM, CYBERARMYOFRUSSIA_REBORN (проросійські кібертерористи, активність відслідковується за ідентифікаторами UAC-0106, UAC-0108, UAC-0109, UAC-0107 відповідно)

Зазначається, що серед головних цілей хакерів - шпіонаж (отримання розвідувальних даних щодо логістики, озброєння, планів та операцій Сил безпеки та оборони), спроби виведення з ладу об'єктів критичної інформаційної інфраструктури, позбавлення доступу українців до держпослуг та сервісів, банківського обслуговування тощо.

Окрім того, метою хакерів є здійснення інформаційно-психологічні операції та дезінформаційні вкиди задля підриву довіри до спроможностей органів державлади, Сил безпеки та оборони, поширення панічних настроїв серед населення.

При цьому кіберзловмисникам не вдається досягти стратегічної мети і завдати істотної шкоди інфраструктурі України». ***(Стало відомо, скільки ворожих кібератак зареєстрували в Україні // ua.news (https://ua.news/ua/ukraine/stalo-izvestno-skolko-vrazheskih-kiberatak-zaregistrirovali-v-ukraine). 02.01.2023).***

***

«Українці продовжують боротися з країною-терористом на землі, у повітрі та у кіберпросторі. Як пише видання Speka, хакерам з України вдалось зламати всі 79 сервісів російської IT-компанії Yandex. 45 Гб даних Yandex опинились у відкритому доступі.

За словами хакерів, сервіси Yandex вдалось зламати ще у липні, втім лише зараз з`явилась нагода опублікувати отримані дані. Архів з кодами всіх проектів та сервісів компанії, внутрішньою документацією та ключами доступу до API розміщений на форумі dumpforums. Українці використовують цю платформу для публікації вилучених даних російських компаній — будь-яка інформація у боротьбі з росією має значення.

Серед опублікованих даних:

пошуковий двигун (фронтенд і бекенд);

бот індексації сторінок;

платформа web-аналітики Yandex Metrika;

картографічна система Yandex Maps;

голосовий помічник Аліса;

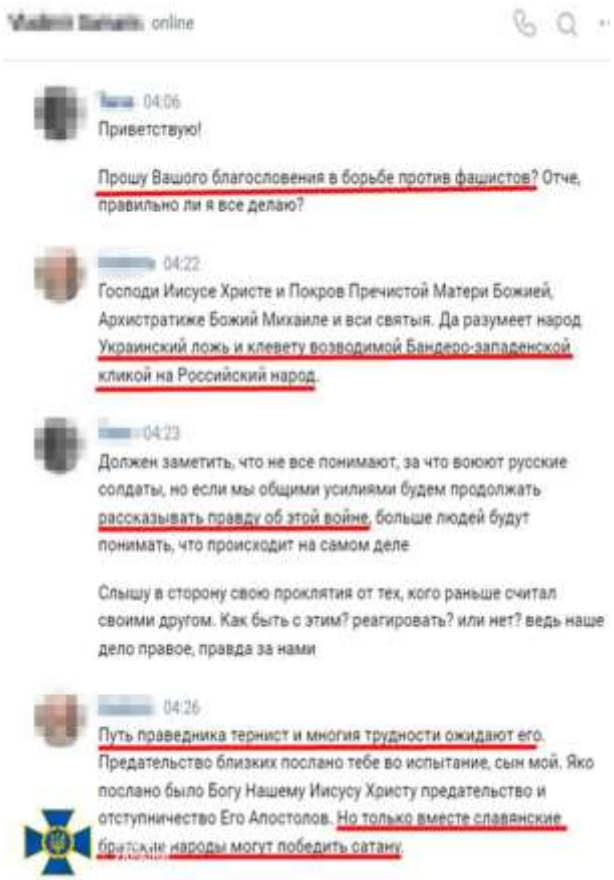
хмарна платформа Yandex Cloud;

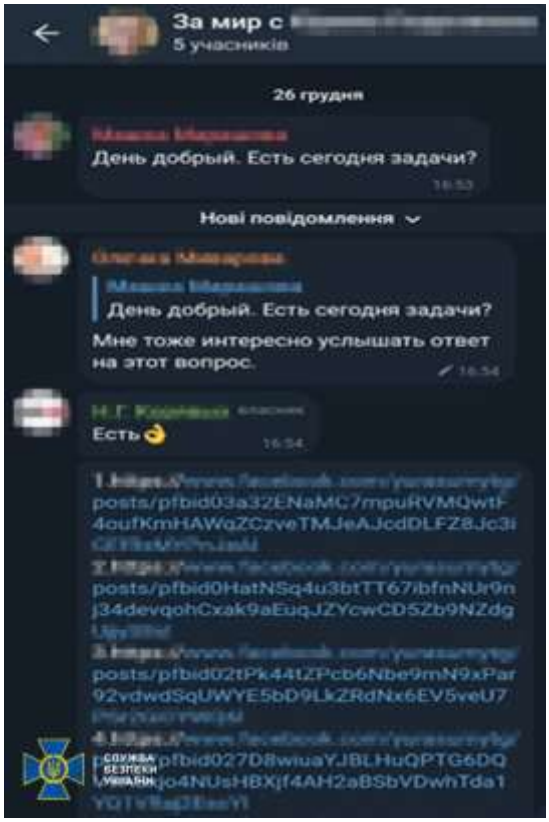
платіжна система Yandex Pay;
рекламна платформа Yandex Direct;
поштовий сервіс Yandex Mail;
інформаційна система служби підтримки;
Яндекс Таксі;
Yandex Phone;
сховище Yandex Disk;
мережа доставки контенту;
торговий майданчик Yandex Market;
бізнес-сервіси Yandex360.

Відтепер у вільному доступі лежить код, який показує як Yandex змінює пошукові алгоритми заради кремлівської пропаганди…». ***(Українські хакери зламали всі сервіси російського Yandex // No worries! (https://noworries.news/ukrayinski-hakery-zlamaly-vsi-servisy-rosijskogo-yandex-2/). 27.01.2023).***

***

«Зловмисники поширювали у соцмережах заклики на підтримку збройної агресії проти України та виправдовували воєнні злочини російських окупантів.





Встановлено, що як першоджерело інтернет-агенти використовували Телеграм-канал московського пропагандиста Юрія Подоляки – російського блогера, який нараховує більше ніж 2,7 млн підписників.

«Тролі» поширювали його публікації через репости або під виглядом «власних» публікацій у соцмережах.

За даними слідства, підривну діяльність на Київщині організували двоє місцевих жителів.

Комп'ютерне обладнання для проведення «інформударів» та комунікації з російськими кураторами встановили у власних помешканнях в столиці та Білій Церкві.

Для масового «покриття» інтернет-простору зловмисники намагалися залучити нових учасників пропагандистського «осередку» кремля.

Щоб збільшувати чисельність «аудиторії», використовували сотні бот-акаунтів, від імені яких поширювали і коментували дописи з російською пропагандою.

Під час обшуків за місцями проживання зловмисників правоохоронці виявили мобільні телефони і комп'ютери із доказами злочинних дій.

На підставі зібраних доказів слідчі СБУ повідомили двом фігурантам з Києва про підозру за ч. 2 ст. 436-2 Кримінального кодексу України (виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників).

Судом зловмисникам обрано міру запобіжного заходу для запобігання ухилення їх від кримінальної відповідальності.

Триває розслідування для притягнення всіх винних до відповідальності.

Слідчо-оперативні дії проводили співробітники СБУ м. Києва та Київської області за процесуального керівництва Київської міської прокуратури». ***(Кіберфахівці СБУ нейтралізували прокремлівську «фабрику тролів» у Києві //***

Магнолія-ТВ (https://magnolia-tv.com/news/84333-kiberfakhivtsi-sbu-neytralizuvaly-prokremlivsku-fabryku-troliv-u-kyyevi-foto?prov=ukrnet). 10.01.2023).

***

«Російські пропагандистські ЗМІ пишуть, ніби заступник голови Держслужби спецзв'язку та захисту інформації України Віктор Жора заявив про ефективність ворожих кібератак у матеріалі Politico. Однак про це у публікації авторитетного західного медіа не йдеться.

Про це повідомляє Центр стратегічних комунікацій та інформаційної безпеки.

Російські пропагандистські ЗМІ пишуть, ніби заступник голови Держслужби спецзв'язку та захисту інформації України Віктор Жора заявив про ефективність ворожих кібератак у матеріалі Politico. Однак про це у публікації авторитетного західного медіа не йдеться.

Про це повідомляє Центр стратегічних комунікацій та інформаційної безпеки.

У чому полягає маніпуляція росіян

Як зазначили журналісти фактчекінгового проєкту StopFake, в оригінальній статті "Київ стверджує, що російські кібератаки є воєнними злочинами", на яку посилаються фейкомети, йдеться про те, що українські фахівці збирають докази російських кібератак і передають цю інформацію до Міжнародного кримінального суду в Гаазі.

Віктор Жора, який керує операціями з кібербезпеки в українській службі безпеки зв'язку, навів як приклад атаки рф на ДТЕК у липні минулого року.

«Їхня ТЕЦ була обстріляна, і одночасно була атакована їхня корпоративна мережа. Це спрямована та спланована діяльність росіян, яку вони вели як у звичайній сфері, так і в кіберпросторі», — йдеться у статті.

Втім, у матеріалі Politico не йдеться про те, що ці атаки були ефективними та успішними.

У Центрі нагадали, що наприкінці 2022 року СБУ заявила про нейтралізацію сотень ворожих кібератак на об'єкти енергетики України, з яких близько 30 могли стати надкритичними…». ***(Надія Клочко. Чи є ефективними кібератаки рф: аналітики викрили чергову маніпуляцію роспропаганди // Новини.LIVE (https://it.novyny.live/chi-ie-efektivnimi-kiberataki-rf-analitiki-vikrili-chergovu-manipuliatsiiu-rospropagandi-71931.html). 10.01.2023).***

***

«Украина связала кибератаку, которая задержала брифинг национального агентства по защите информации для прессы во вторник, с российскими хакерами Sandworm. По словам следователей, группа, обвиняемая в использовании вредоносного ПО Wiper для нарушения работы украинского национального медиацентра, имеет тесные связи с российским ГРУ.

В атаке использовались пять типов вредоносного ПО, связанных с российскими хакерами: CaddyWiper, ZeroWipe, SDelete, AwfulShred и BidSwipe, как утверждают следователи Украинской группы реагирования на компьютерные

чрезвычайные ситуации в рамках расследования совместно с Государственной службой специальной связи и защиты информации.

Укринформ, национальное информационное агентство и медиацентр страны, начал испытывать проблемы с подключением к Интернету во время пресс-брифинга, который на прошлой неделе провел глава Государственной службы специальной связи и защиты информации Украины Юрий Щеголь.

По словам экспертов CERT-UA, злоумышленники предприняли безуспешные попытки нарушить нормальную работу рабочих станций пользователей, используя деструктивные вредоносные программы CaddyWiper и ZeroWipe, а также легитимную утилиту SDelete.

«При этом объект групповой политики использовался для централизованного распространения вредоносного ПО. Он позволял создавать соответствующие запланированные задачи», — говорится в сообщении CERT-UA.

Прерванный брифинг для прессы

Щиголь собирался подробно обсудить гибридную войну России, ее цель уничтожить информационную инфраструктуру страны, а также широкое использование Москвой кибератак в качестве прелюдии к ракетным атакам на критически важную инфраструктуру Украины (см.: Украина: русские стремятся уничтожить информационную инфраструктуру).

Из-за этого все онлайн-трансляции были прерваны на 15 минут, но команда SSSCIP смогла оперативно восстановить связь, после чего медиацентр продолжил работу в штатном режиме.

В опубликованном через несколько часов заявлении медиа-центр приписал кибератаку России. Щиголь на возобновлении пресс-брифинга прокомментировал, что «все, что смогли сделать российские хакеры, — это отсрочить начало нашего брифинга на 15 минут. Точно так же своими действиями они оттягивают конец своей страны. Это обязательно произойдет в ближайшее будущее."

Русскоязычный Telegram-канал CyberArmyofRussia_Reborn взял на себя ответственность за атаку в полдень во вторник, всего через несколько минут после того, как впервые возникли технические проблемы. CERT-UA сообщает, что Telegram-канал неоднократно публиковал деструктивную деятельность группы Sandworm в дополнение к типичным сообщениям о DDoS-атаках и порче веб-сайтов.

CERT-UA сообщает, что кибератака была предотвращена за счет оперативной локализации угрозы.

Агентство также подчеркивает, что кибератака имела лишь частичный успех, особенно в отношении ограниченного числа пострадавших систем хранения данных.

Хакеры из песчаных червей

Традиционно известно, что хакеры Sandworm используют несколько семейств вредоносных программ, таких как ORCSHRED, SOLOSHRED, AWFULSHRED, и самое популярное из них — Industroyer — для нападения на жертв.

Известно, что в декабре 2016 года эта группировка атаковала энергосистему Украины с помощью вредоносного ПО Industroyer, а в апреле 2022 года собиралась

повторить историю с усовершенствованным вариантом Industroyer2, но была вовремя остановлена перед казнью.

В ходе анализа этой атаки фирма по кибербезопасности ESET также обнаружила развертывание вредоносного ПО Caddywiper, которое, как следует из названия, является средством очистки данных. ESET заявила, что группа активно использовала это вредоносное ПО для атак на компьютеры, работающие под управлением операционной системы Windows.

В нем также говорится, что существует две версии вредоносного ПО: первая для замедления попыток восстановить контроль над консолями промышленной системы управления, а вторая — для развертывания через объект групповой политики, указывающий на то, что злоумышленники ранее контролировали сеть цели, считают исследователи ESET. сказал.

В первоначальном анализе последней кибератаки на медиацентр, проведенном CERT-UA, говорится, что злоумышленники использовали схожую тактику: «Вредоносная программа CaddyWiper была запущена централизованно, чтобы нарушить целостность и доступность информации с помощью GPO». Этот и другие методы и процедуры помогли CERT-UA приписать кибератаку UAC-0082 или группе Sandworm.

CERT-UA не ответил на запрос информационной безопасности Media Group о дополнительных подробностях о том, как долго группа Sandworm имела предварительный доступ к сети Media Center, чтобы рассчитать время атаки во время пресс-конференции». ***(Mihir Bagwe. Ukraine Links Media Center Attack to Russian Intelligence // Information Security Media Group, Corp. (https://www.govinfosecurity.com/ukraine-links-media-center-attack-to-russian-intelligence-a-21043). 28.01.2023).***

***

«Всплеск фишинговых атак на критические секторы Украины в конце 2022 года произошел, когда эксперты отслеживали «снижение темпа» в конфликте

Попытки нарушить украинское киберпространство, по-видимому, участились в конце 2022 года, говорят независимые наблюдатели за сетями страны, поскольку Россия продолжает настаивать на своем вторжении.

Фишинговые атаки и кампании вредоносного ПО, нацеленные на Украину, резко возросли в ноябре, а затем сократились к концу года, сообщает охранная фирма Trellix. То же самое произошло и с предупреждениями о безопасности конечных точек в регионе, связанными с «потенциально нежелательными программами».

Всплеск атак аналогичен выводам других наблюдателей за кибератаками. Базирующаяся в Женеве некоммерческая группа CyberPeace Institute сообщает, что с января 2022 года было совершено 918 кибератак и операций, связанных с конфликтом.

В ноябре институт зафиксировал внезапный рост онлайн-атак, связанных с войной в России, по сравнению с предыдущим месяцем. Единственным

исключением стала Российская Федерация, где количество атак на нее уменьшилось.

Эксперты говорят, что на протяжении всей войны правительство Украины, энергетика, транспорт, финансовые услуги и другие критически важные секторы инфраструктуры остаются в числе главных целей онлайн-атак. «От вредоносной электронной почты и URL-адресов до использования вредоносных программ, поддерживаемых государством, киберактивность продолжает сопровождать кинетическую военную активность и социальное недовольство», — говорят исследователи Trellix.

Неясно, что может объяснить рост или снижение в последние месяцы 2022 года, особенно в то время, когда глава разведки США заявил, что частота атак замедлилась.

«Мы уже наблюдаем своего рода замедление темпов конфликта, — сказала директор национальной разведки Аврил Хейнс участникам Рейгановского форума национальной обороны 3 декабря, — и мы ожидаем, что это, вероятно, будет тем, что мы увидим в ближайшем будущем. месяцы».

Trellix сообщает, что в ноябре и декабре прошлого года наблюдаемый объем фишинговых атак на Украину вырос в двадцать раз, и большинство атак были нацелены на адреса электронной почты, зарегистрированные в.uaдомене верхнего уровня, который используется государственными и военными ведомствами. Хотя отправителя часто подделывали, «подавляющее большинство» этих атак, по-видимому, связано со спонсируемой государством российской группой «Гамаредон», названной так потому, что в ранних атаках этой группы содержались сообщения с орфографическими ошибками в слове «армагеддон».

Рост числа потенциально нежелательных программ связан с попытками заразить системы вредоносными программами, которые выглядят как программы для пиратства продуктов Adobe. Trellix заявляет, что все эти атаки прослеживаются «к одной программе активации программного обеспечения, направленной на активацию Adobe», и говорит, что, хотя использование «пиратских активаторов лицензий» остается широко распространенным, огромное количество из них являются подделками, предназначенными исключительно для заражения системы вредоносным ПО.

С тактической точки зрения попытки фишинга также не выглядели продвинутыми. Многие из них полагались на широко распространенную тактику, такую как использование электронных таблиц Microsoft Excel с поддержкой макросов, документов Microsoft Word и файлов ярлыков LNK Windows.

Примеры фишинговых электронных писем, обнаруженных Trellix, включают сообщения, якобы отправленные Министерством иностранных дел Эстонии, с раскрытием контактных данных, но перенаправляющие на вредоносный файл, размещенный на Google Диске; HTML-уведомление о доставке, которое перенаправляет на фишинговую страницу; и запрос от украинских военных проверить почтовый ящик, который содержит ссылку на вредоносный веб-сайт.

Атаки Андромеды

Помимо фишинговых кампаний группы Gamaredon, Trellix сообщает, что в последние месяцы она также столкнулась с рядом атак с использованием H-Worm,

также известного как Houdini RAT, троянца удаленного доступа, в том числе в «целевых атаках на международную энергетическую отрасль»; Вредоносное ПО для кражи информации Formbook; программное обеспечение удаленного управления Remcos; и вредоносное ПО Andromeda.

Атаки Андромеды были необычными. Впервые появившаяся в 2011 году, Andromeda представляет собой коммерчески доступное готовое вредоносное ПО, которое продолжает обновляться. Но группа реагирования на инциденты Google Mandiant сообщила 5 января, что она видела версию Andromeda 2013 года, которую, как она подозревает, использует российская государственная хакерская группа Turla, также отслеживаемая как Venomous Bear и Krypton.

В сентябре Mandiant обнаружил предполагаемую операцию Turla Team по распространению разведывательной утилиты KopiLuwak и бэкдора QuietCanary среди жертв вредоносного ПО Andromeda в Украине. Операторы вредоносных программ перерегистрировали как минимум три домена управления и контроля Andromeda с истекшим сроком действия и начали профилировать жертв для выборочного развертывания KopiLuwak и QuietCanary.

Mandiant говорит, что заражение началось в декабре 2021 года, когда жертва подключила зараженное USB-устройство к системе Windows, а затем щелкнула ссылку на вредоносный файл, замаскированный под папку.

Непонятно, почему злоумышленники в 2022 году хотели использовать вредоносное ПО эпохи 2013 года, привязанное к доменам, которые они были вынуждены сначала перерегистрировать. С другой стороны, «более старые вредоносные программы и инфраструктура с большей вероятностью будут упущены из виду защитниками, сортирующими широкий спектр предупреждений», — говорят исследователи Mandiant.

Эта запоздало замеченная атака действительно удалась, в результате чего злоумышленники украли данные». ***(Mathew J. Schwartz. Ukraine's Critical Sectors Targeted in Phishing Attack Surge // Information Security Media Group, Corp. (https://www.govinfosecurity.com/ukraines-critical-sectors-targeted-in-phishing-attack-surge-a-21024). 26.01.2023).***

***

«…Главное агентство по защите информации Украины заявляет, что российские кибератаки сосредоточены на разрушении критической информационной инфраструктуры, шпионаже и дезинформации.

Для уничтожения информационных систем российские хакеры, спонсируемые государством, широко использовали вредоносные программы datastealer и data wiper, заявил во вторник на пресс-конференции глава Государственной службы специальной связи и защиты информации Украины Юрий Щеголь. «Такие атаки составляют более четверти от их общего количества и могут быть частью более сложных и мощных операций», — говорит он.

По словам Щеголя, наиболее атакуемыми секторами являются энергетика, безопасность и оборона, телекоммуникации, технологии и развитие, финансы и логистика.

SSSCIP позиционирует Систему безопасного доступа в Интернет для противодействия этой агрессии и обеспечения кибербезопасности органов государственной власти Украины. Щиголь сказал, что система, которая блокирует большинство кибератак, в настоящее время используется почти 200 государственными органами, в том числе из сектора национальной безопасности и обороны.

Система, которой управляют специалисты SSSCIP, «является одним из наших надежных щитов, который обеспечивает киберустойчивость государства, останавливает и блокирует попытки вторжений, DDoS, заражение и распространение шпионских программ и т. д.», — говорит Щеголь.

Украина ежедневно сталкивается с тысячами кибератак, и власти заявляют, что ежедневно им удается отразить до 40 мощных DDoS-атак высокого уровня. В декабре прошлого года они заблокировали 395 таких атак.

Агентство сообщает, что в 2022 году оно задокументировало семь новых типов вирусов или других вредоносных программ. SSSCIP не сразу ответил на запрос Information Security Media Group о предоставлении дополнительной информации об этих недавно выявленных вариантах вредоносных программ.

Доставка вредоносных программ часто осуществляется с помощью фишинговых писем, содержащих срочные формулировки, чтобы вызвать немедленный ответ. Государственные служащие являются предпочтительными целями.

За фишингом следует эксплуатация уязвимостей в качестве начального вектора доступа. Агентство сообщает, что в декабре было зафиксировано около 170 000 попыток эксплуатации программных уязвимостей, но они были обнаружены и заблокированы.

Щиголь также объяснил успех киберустойчивости Украины поддержкой со стороны международного сообщества и компаний частного сектора, включая Microsoft и Amazon, которые помогли Украине приобрести необходимые технологические достижения для киберзащиты. В первую очередь глава ГСИН приписал успех украинским специалистам по кибербезопасности, 90% которых работают в госсекторе.

Щеголь также процитировал недавно опубликованный отчет Украинской группы реагирования на компьютерные инциденты, в котором задокументировано более 2100 киберинцидентов в 2022 году. Около четверти атак были направлены на правительство и местные органы власти. Но, ссылаясь на тот же отчет, Щеголь сказал, что ежегодная статистика показывает, что российские атаки на военные и гражданские цели в киберпространстве связаны.

Россияне также использовали кибератаки как прелюдию к ракетным ударам. «Кибератаки стали полноценным компонентом войны, а также кинетических действий», — говорится в сообщении SSSCIP.

Эта координация была подтверждена новым исследованием «Кибер, артиллерия, пропаганда: общий обзор масштабов российской военной агрессии», проведенным ГСИНБ и экспертами Совета экономической безопасности Украины, главнокомандующим Вооруженных Сил. Украины и эксперты агентства TRUMAN.

В отчете показана хронология всех крупных кибератак, направленных на различные объекты критической инфраструктуры в Украине, и их связь с обычным полномасштабным вторжением в Россию посредством скоординированных ракетных ударов по учреждениям, которые помогают Украине.

Одним из немногих примеров, упомянутых в отчете, является то, как Россия проводила DDoS-атаки на несколько банковских сайтов и сайт Минобороны не один, а два раза, причем последняя атака произошла всего за день до физического вторжения 23 февраля 2022 г. (см. : Кибератака поразила украинское правительство, банковские сайты).

В докладе рекомендуется пересмотреть юридическое определение агрессии, содержащееся в резолюции 3314 Генеральной Ассамблеи ООН 1974 года. В настоящее время резолюция гласит: «применение любого оружия государством против территории другого государства», но не дает четкого указания на то, является ли «любое оружие» включает оружие кибервойны.

Еще одна рекомендация, которую дает отчет, — объявить кибератаки военными преступлениями. «Международное гуманитарное право должно установить более строгие рамки для нетрадиционных нападений», — говорится в нем.

В SSSCIP говорят, что война нанесла значительный ущерб инфраструктуре информационно-коммуникационных технологий более чем в 10 из 24 областей Украины. И хотя усилия предпринимаются, для полного восстановления телекоммуникационного сектора, который в прошлом году стал жертвой наиболее целенаправленных кибер- и физических атак, потребуется 1,79 млрд долларов, говорится в сообщении». ***(Mihir Bagwe. Ukraine: Russians Aim to Destroy Information Infrastructure // Information Security Media Group, Corp. (https://www.govinfosecurity.com/ukraine-russians-aim-to-destroy-information-infrastructure-a-20964). 18.01.2023).***

***

«Сайт Legacy of War Foundation, за допомогою якого британський художник Бенксі проводив розпродаж 50 своїх робіт на допомогу Україні, зазнав хакерських атак із РФ. Приблизно 3500 із них мали російські IP-адреси. Про це повідомляється на сайті благодійної організації.

«Зараз ми відбираємо зареєстровані заявки та незабаром повідомимо про успішних покупців. Сайт отримав понад мільйон заявок (і 3500 ворожих атак із російських IP-адрес), тому цього разу будемо вдячні за ваше терпіння», — йдеться в публікації.

У грудні 2022 року Бенксі виставив на продаж 50 своїх малюнків, кошти від продажу яких збирався передати на допомогу Україні.

Legacy of War Foundation — міжнародна благодійна організація, що підтримує громадян, які постраждали під час конфліктів. Головний офіс організації розташований у Великій Британії…» ***(Сайт Бенксі з малюнками на допомогу Україні атакували з Росії 3500 разів // ФОКУС (https://focus.ua/uk/digital/544688-sayt-benksi-s-risunkami-v-pomoshch-ukraine-atakovali-iz-rossii-3500-raz). 10.01.2023).***

***

«Перша світова кібервійна – саме так можна назвати те, що нині відбувалося і відбувається в цифровому просторі. Вперше Росія атакувала Україну ще 2014 року, і відтоді бій не вщухав ні на хвилину, а торік інтенсивність атак збільшилася утричі. Тут теж є своя важка артилерія і свої системи захисту та прориву, йдеться в ТСН.

Вісім років тому ляп російського телебачення про те, що нібито Дмитро Ярош став президентом України, спричинив фурор. Саме ці події експерти вважають початком російсько-української кібервійни. Насправді табло з нібито перемогою Яроша мало з'явитися на центральній плазмі ЦВК, якби російська кібератака вдалася. «Формально відбулося проникнення в Мережу, але воно було швидко виявлено, локалізовано і мінімізовані наслідки. Вистояла. До цього готувалися ретельно, були залучені професійні компанії, які перед виборами просто ночували там на місці», – розповідає експерт з кібербезпеки Костянтин Корсун.

Наступна потужна кібератака Росії на Україну наполохала увесь світ – вивчати її з'їхалися спеціалісти найвищого рівня. Російським хакерам вдалося підключитися до комп'ютера «Прикарпаттяобленерго» і знеструмити цілу область. «Близько 200 тисяч мешканців області залишилися на 6 годин без світла. Це дуже серйозний інцидент», – зазначає експерт.

Так українці дізналися значення слова «фішинг», адже саме випадковий лист створив блекаут на Прикарпатті. «Цей самий комп'ютер був під'єднаний до Інтернету. Туди просто надіслали листа електронного з макросом, і ідіот, який сидів за цим комп'ютером, просто відкрив цього листа», – каже експерт з кібербезпеки Микита Книш.

Наступна кібератака, яка вийшла офлайн, сталася 2017 року, вірус NotPetya частково паралізував країну – банкомати, каси, робочі комп'ютери і навіть аеропорт Бориспіль, неушкодженим, здається, лишилося тільки те, що не було підключене до Інтернету.

Вірус зачепив і Європу – загалом втрати оцінять у понад 10 млрд доларів. Відтоді кращі спеціалісти з кіберзахисту стали частими гостями в Україні. «Вони збирають зразки російських, китайських, американських, сирійських, ізраїльських та будь-яких вірусів для того, щоб краще тренувати системи безпеки. Бо Україна – то полігон із кібербезпеки, полігон із випробовування кіберзброї», – кажуть експерти.

В січні 2022 року – за місяць до вторгнення – російські хакери зламали наші бази даних, особиста інформація українців опинилася в загальному доступі. «Нас рознесли в нуль, хлопці та дівчата, вітчизняної кібербезпеки як не існувало», – переконує Микита.

«Після цієї атаки були зроблені організаційні висновки і ці дірки, які там були, я думаю, давно вже залатані, тому що після 13 січня ми вже не бачимо великих витоків інформації», – твердить радник міністра інфраструктури Євген Поремчук.

Першого достойного кіберляпаса від України РФ отримала в березні 2022 року. Росавіацію змусили згадати, як діди воювали. «Внаслідок атаки вони змушені

були перейти на паперовий документообіг. Опуститися в минуле століття», – нагадує Костянтин.

На День перемоги хакери зупинили найбільший російський відеохостинг – RuTube. «Знищили все просто, випалили напалмом настільки, що росіяни понад місяць не могли відновитися. А те, що вони називали відновленням, було дуже частковим відновленням», – переконують експерти.

«Ми зрівняли шанси, ми злили усі бази даних «Яндексу», «Яндекс-їжа», банків Росії, кредитних карток. Зараз ми тільки зрівняли ситуацію і зрівняли це фахівці з приватного сектору, активісти», – додає Микита.

КІБЕРВІЙНА ТРИВАЄ ЩОХВИЛИНИ: ЇЇ ПЕРЕМОГИ ТА ПОРАЗКИ МОЖУТЬ СТАТИ ВИРІШАЛЬНИМИ І НА РЕАЛЬНОМУ ПОЛІ БОЇ

Наступні цілі своєї атаки Росія нахабно анонсує на весь світ. «Це будуть непрямі атаки на енергогенерувальні компанії, як ГЕС, ТЕС. Атаки через постачальників, кожне підприємство – велике чи мале – має постачальників, через яких вони співпрацюють», – розповідає Костянтин.

В українських хакерів теж є свої творчі плани на майбутнє. «Ми будемо робити тактику тисячі дрібних порізів, будемо розривати ланцюжок поставки. Зараз ми займаємося блокуванням карток волонтерів, які збирають гроші в Росії. Ми блокуємо картки росіян, які на передовій, щоб дружина не могла знімати гроші. Вони тут воюють за гроші, не за ідею. Ми будемо критичні об’єкти інфраструктури намагатися вивести з ладу, навіть газове обладнання, і це логічно», – кажуть вони.

Ця невидима війна триває щохвилини. Її бої не нанесеш на мапу, і не всі й помітять вдалий наступ чи контрнаступ, але перемоги та поразки можуть стати вирішальними і на реальному полі бою». ***(Перша світова кібервійна. ЇЇ перемоги і поразки такі ж вирішальні, як на полі бою. Як Україна дає собі раду // Inshe.tv (https://inshe.tv/suspilstvo/2023-01-10/732853/). 10.01.2023).***

***

«Сьогодні війна йде не тільки в українських містах та селах. Повномасштабне вторгнення росії в нашу країну супроводжується активним поширенням від ворожих хакерів дезінформації, пропаганди, проведенням інформаційно-психологічних операцій, кібератаками на об’єкти критичної інфраструктури нашої країни.

Скільки кібератак на Україну здійснила росія

З початку 2022 року Служба безпеки України нейтралізувала понад 4,5 тис. кібератак на Україну. Якщо у 2020 році було зафіксовано майже 800 кібератак, у 2021 – 1400, то вже минулого року їхня кількість зросла у понад три рази.

Приєднуйтесь до нас в соцмережах!

Урядова команда реагування на комп’ютерні надзвичайні події CERT-UA, яка діє при Держспецзв’язку, зареєструвала та дослідила протягом 2022 року 2,1 тис. кіберінцидентів та кібератак. А від початку повномасштабного воєнного вторгнення росії в Україну – понад 1,5 тис.

Найчастіше ворожі хакери атакують державний сектор: на нього припадає близько чверті всіх досліджених випадків.

Серед головних цілей ворожих хакерів наводять такі:

шпіонаж (отримання розвідданих щодо логістики, озброєння, планів та операцій Сил безпеки та оборони);

спроби виведення з ладу об’єктів критичної інформаційної інфраструктури;

позбавлення доступу громадян до державних послуг та сервісів, банківського обслуговування тощо.

А також – інформаційно-психологічні операції та дезінформаційні вкиди з метою підриву довіри до органів державної влади, Сил безпеки та оборони, поширення панічних настроїв серед населення.

Під особливою увагою російських хакерів залишається енергетичний сектор. Кібератаки на підприємства енергетики відрізняються складністю проведення та підготовлення, їх важче виявляти. Також під постійним прицілом – компанії, що є постачальниками послуг, апаратного та програмного забезпечення для енергокомпаній.

Український кіберзахист: як Україна захищається від кібератак

Сьогодні Security Operation Center МОУ в режимі 24/7 проводить моніторинг подій безпеки на всіх рівнях — від інфраструктурного до аплікаційного. Також на щоденній основі аналізується кіберпростір і опрацьовуються гіпотези щодо актуальних тактик та технік, притаманних спецслужбам ворога.

«Поки ворожим хакерам не вдалося досягнути якихось стратегічних цілей. Але попри нашу достатньо ефективну діяльність щодо попередження кібератак, ворог продовжує шукати можливості та використовувати їх для того, щоб отримати доступ до інформаційно-комунікаційних мереж об’єктів критичної інфраструктури. Більше того, із великою ймовірністю агресія у кіберпросторі з боку росії буде тривати навіть після нашої перемоги», – зауважує заступник голови Держспецзв’язку Віктор Жора.

До кіберзахисту українських інформаційних систем долучились найкращі вітчизняні та світові фахівці. Нам допомагають уряди та комерційні компанії більшості демократичних країн світу.

Держава також активно набирає кіберволонтерів і, наприклад, за допомогою смс розсилки запрошує до кібервійська України.

Втім Костянтин Корсун, автор цифрового контенту у Facebook, зазначає:

«Немає в Україні взагалі жодного кібервійська. Не існує в природі. Саме як «війська», а не волонтерсько-партизанських айті-угруповань, які можуть називати себе як завгодно. І за участь у яких після нашої перемоги не виключені проблеми юридичного характеру. Якби у кіберполіції знали хоча б основи кібергігієни – нізащо б не відправляли масових смс із запрошенням до «кібервійська» у рашистському Телеграмі. Це просто табу для більш-менш освіченого кібербезпечника».

За свого боку, Володимир Кондрашов, речник у Державній службі спеціального зв'язку та захисту інформації України, підкреслює, що використання того чи іншого месенджера визначається завданнями комунікації кожного користувача, наявним функціоналом, необхідним ступенем захисту:

«Потрібно мати розуміння, що не буває абсолютно безпечних чи захищених систем. Як і раніше, ми рекомендуємо використовувати перевірені месенджери з відкритим кодом».

Які російські та проросійські хакери атакують Україну

За інформацією Державної служби спеціального зв'язку та захисту інформації України, у період від вересня по грудень 2022 року в Україні діяли такі російські та проросійські хакерські угрупування:

ARMAGEDDON/GAMAREDON/PRIMITIVE BEAR (ФСБ рф, активність відслідковується за ідентифікатором UAC-0010).

SANDWORM (ГУ ГШ ЗС рф (ГРУ), активність відслідковується за ідентифікатором UAC-0082).

APT28/FANCY BEAR (ГУ ГШ ЗС рф (ГРУ), активність відслідковується за ідентифікатором UAC-0028).

APT29/COZY BEAR (СЗР рф, активність відслідковується за ідентифікатором UAC-0029).

UNC1151/ GHOSTWRITER (Міністерство оборони рб, активність відслідковується за ідентифікатором UAC-0051).

XAKNET, KILLNET, Z-TEAM, CYBERARMYOFRUSSIA_REBORN (проросійські кібертерористи, активність відслідковується за ідентифікаторами UAC-0106, UAC-0108, UAC-0109, UAC-0107 відповідно).

Від початку 2022 року росія запустила щонайменше декілька сімейств шкідливого програмного забезпечення в Україні:

WhisperGate/WhisperKill;

CaddyWiper;

Hermetic Wiper;

Industroyer2;

DoubleZero

та інші.

Види кібератак у 2022 році:

сканування (збір інформації про системи або мережі);

спроби експлуатації вразливості (спроби вторгнення з використанням вразливості у системі, компоненті чи мережі);

шкідливе підключення (спроби з'єднання від/до IP/URL — адреси, пов'язаної з відомим ШПЗ, наприклад С2С або ресурсом розповсюдження компонентів, пов'язаних із активністю певної бот-мережі);

спроби авторизації або входу в систему (спроба входу до служб або механізмів доступу, невдала спроба підбору автентифікаційних даних чи використання раніше скомпроментованих (вже неактуальних даних);

атаки на відмови в обслуговуванні Dos/Doss (вплив на нормальне функціонування системи чи сервісу, що досягається направленням з одного чи багатьох джерел до цільового ресурсу запитів для перенасичення пропускної здатності чи системних ресурсів).

Приклади кібератак: маскування під ДСНС та Генштаб

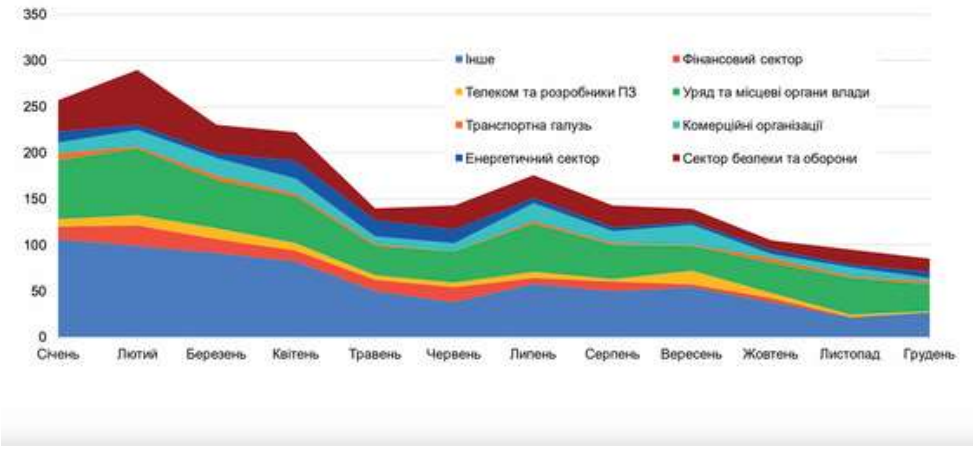
Фахівці CERT-UA 21 жовтня виявили факт розповсюдження електронних листів, начебто від імені пресслужби Генштабу ЗСУ. У повідомленнях містилося посилання на завантаження «наказу», перейшовши за яким, жертва потрапляла на сторінку із повідомленням про необхідність оновлення програмного забезпечення

(PDF Reader). Натискання на кнопку «Завантаження» призводило до завантаження шкідливої програми RomCom.11.

Ще російські хакери маскувалися під ДСНС, розсилаючи листи з темою «Як розпізнати дрон-камікадзе». Таким чином вони намагались розповсюджувати шкідливу програму DolphinCape, серед функції якої — збір інформації, запуск EXE/DLL файлів, відображення списку файлів та їх вивантаження, а також створення та ексфільтрація знімків екрана.

У кіберпросторі росія атакує Україну з такою ж інтенсивністю, як б'є по нас ракетами. Віртуальні атаки противника найчастіше спрямовані на цивільну інфраструктуру енергетику, зв'язок, бази даних та реєстри, урядові сайти. Вони мають на меті створити паніку та гуманітарну кризу в Україні, підірвати оборонну спроможність ЗСУ. Російські хакери мають великий досвід соціальної інженерії, точні дані щодо «гарячих» тем в країні та майстерно все це використовують для дезінформації усього світу.

У нас вже є потужна армія кіберволонтерів, професійні спеціалісти кібербезпеки державного сектору та високий рівень державно-приватного партнерства завдяки підтримці від бізнесу. Разом з тим, необхідно якнайшвидше ухвалити закон про створення та функціонування у системі Міноборони кібервійськ, який має стати підґрунтям у сфері кібероборони, залучення до цієї діяльності кіберволонтерів та створення кіберрезерву.



Кібератаки на Україну у 2022 році. Дані Державної служби спецзв`язку та захисту інформації України». ***(Наталія Толуб. Кібервійна рф проти України: як працюють російські хакери та воюють українські кібервійська // thepage (https://thepage.ua/ua/politics/kibervijna-rf-proti-ukrayini-yak-voyuyut-ukrayinski-kibervijska). 10.01.2023).***

***

«Група «Технарі» з Одеси представили програму для смартфонів під назвою «Цифрова бавовна» для автоматичних DDoS-атак російських сайтів. Один із розробників і співзасновник ресурсу IT WAR UA Андрій Кривошеєв розповів подробиці виданню DOU.

Додаток для Android «Цифровий бавовна» змушує смартфон тривалий час відправляти запити російським сайтам із метою перевантажити їх та вивести з ладу. Чим більше пристроїв одночасно задіють програму, тим більший удар. Програма автоматично формує пакет цілей, після чого спрямовує атаки з 2, 5, 10 або 50 тисяч телефонів. Якщо сайт відновлюється, система робить паузу, обнуляє списки атак і відновлює кібердари.

За словами Андрія Кривошеєва, основними цілями «Технарі» зробили банківську та фінансову інфраструктуру, а також державні органи РФ. Такими ресурсами росіяни користуються щодня, тому збої завдають їм безліч незручностей. Через кібератаки громадяни Росії не зможуть скористатися онлайн-банкінгом, сплатити комунальні послуги, звернутися в техпідтримку тощо.

Зараз «Цифрову бавовну» вже використовують кілька тисяч людей, і додаток щодня нагадує, що його варто запустити, крім цього, від користувачів нічого не потрібно. Як запевняє Кривошеєв, команда подбала про надійний захист користувачів. Атаки проводяться через 100 тисяч проксі, розрахованих на 500 тисяч осіб, тому росіяни не зможуть дізнатися IP-адреси українців, які використовують програму. Підставні адреси постійно змінюються, що ще більше ускладнює завдання.

«Ми не тягнемо трафік із користувачів постійно, а беремо його тільки в моменти атак, після чого виробляємо умовні DDoS-пульсації проти ворога. Жодних персональних даних від вас додаток не збиратиме і вимагатиме», — обіцяє Кривошеєв. — «Єдине, що знадобиться — згода на роботу програми у фоновому режимі та згода на показ пуш-повідомлень».

За допомогою програми команда прагне повністю ламати російські сайти. З початку повномасштабної війни «ІТ-армія України» почала зламувати критично важливу онлайн-інфраструктуру Росії, спочатку атаки тривали максимум кілька днів, після чого хактивісти змінювали цілі, зараз вони можуть атакувати систему тижнями.

«Ми хочемо масштабувати процес так, щоб у всіх потрібних нам російських ресурсів не було шансів на відновлення або вони були мінімальними», — поділився планами розробник. — «Коли ми зберемо критичну масу, майже 100 тисяч користувачів, то програма стане реальною зброєю».

Ідея «Бавовни» виникла у команди ще на початку вторгнення, але роботу вона розпочала лише у жовтні. Приблизно за місяць програмісти написали код, потім ще місяць тестували програму, щоб запобігти збоям і перевантаженням, до розробки залучили досвідчених фахівців рівня Senior. З новим оновленням розробники планують додати 50 тисяч проксі для додаткового захисту та рейтинг користувачів, щоб нагороджувати найактивніших.

Група «Технарі» також розробила додаток «єППО», який допомагає збивати іранські дрони над Україною. Будь-який користувач може допомогти ЗСУ, вказавши напрямок польоту ракети або безпілотника натисканням однієї кнопки. Щоправда, для цього необхідно авторизуватись через «Дію». ***(«Цифрова бавовна». В Україні створили програму для кібератак на російські сайти // Internetua (https://internetua.com/-cifrova-bavovna-v-ukrayini-stvorili-programu-dlya-kiberatak-na-rosiiski-saiti). 13.01.2023).***

***

«Україна зуміла здійснити «справжню революцію», просунувшись на вищий щабель у своїй кіберобороні, потерпаючи від кібератак високого рівня.

Про це сказав глава Командування кіберзахисту Франції (COMCYBER) генерал Еймерік Боннемізон під час пресконференції у четвер, пише «Європейська правда».

Кібератаки, зокрема російського походження, завдають шкоди Україні та її критичній інфраструктурі щонайменше з 2014 року, сказав Боннемізон. Україна ж у відповідь посилила свої можливості кіберзахисту, що дозволило їй здійснити «справжню революцію, вийшовши на новий рівень у її комп'ютерній оборонній боротьбі», додав він.

У грудні минулого року під час закритих слухань у Національній асамблеї, зміст яких було оприлюднено у четвер, генерал Боннемізон пояснив, що Україна працювала над своїми вразливими місцями разом із західними кібердержавами, в першу чергу, зі Сполученими Штатами.

Він назвав цю підтримку «вирішальною» і «наближенням українських стандартів і процедур до західних моделей». Це дає можливість швидко обмінюватися ознаками атаки та першими технічними засобами захисту від неї, пояснив він.

У четвер генерал високо оцінив стійкість та ефективність українського кіберзахисту, додавши, що він задоволений тим, що російські кібератаки були «набагато менш впливовими та ефективними, ніж очікувалося».

За його словами, Україна могла бути «поставлена на коліна», але цього не сталося, а зовсім навпаки: Україна зараз має оборонну перевагу, яка, за словами генерала, «є справжньою зміною парадигми», що дозволяє українській державі стримувати, реорганізовувати й «використовувати інші системи для відновлення, і все це зі значним творчим підходом та інноваціями» у сфері кіберзахисту». ***(Валерія Драгомирова. Україна здійснила «революцію кіберзахисту» на тлі атак РФ, – французький генерал // Українські Новини (https://ukranews.com/ua/news/908364-ukrayina-zdijsnyla-revolyutsiyu-kiberzahystu-na-tli-atak-rf-frantsuzkyj-general). 13.01.2023).***

***

«Официальные лица Эстонии предоставили свежие подробности о том, как они помогают специалистам по кибербезопасности в осажденной Украине и координируют свои действия с более влиятельными союзниками в Европе и США.

Украина удивила мир своей способностью отражать крупные кибератаки со стороны России. И одна маленькая страна — Эстония — сыграла огромную роль, помогая им в этом.

Страна с населением чуть более 1 миллиона человек, которая годами отражала кибератаки внутри своих границ из России, в настоящее время возглавляет многие усилия по предоставлению информации о киберугрозах, финансированию и важным международным связям для защиты Украины от российских хакеров.

В интервью в Таллинне официальные лица Эстонии предоставили свежие подробности о том, как они помогают специалистам по кибербезопасности в осажденной Украине и координируют свои действия с более влиятельными союзниками в Европе и США в глобальных усилиях по защите от цифровых атак России». ***(How Estonia Is Helping Ukraine Take on Russian Cyber Threats // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/how-estonia-is-helping-ukraine-take-on-russian-cyber-threats/). 02.01.2023).***

***

«Секретар РНБО Олексій Данилов підписав Технічну угоду про приєднання України до Об'єднаного центру передових технологій кібероборони НАТО (CCDCOE). Це серйозно підвищить здатність нашої країни протистояти різним загрозам в інтернеті, зокрема з боку російських спецслужб.

Сьогодні кіберагресія кремлівського режиму завдає відчутної шкоди не лише українським організаціям, а й великим закордонним компаніям, а також демократичним інституціям. Нагадаємо, заявку на членство України в CCDCOE було подано ще в серпні 2021 року за участю Держспецзв'язку. 4 березня 2022 року її схвалили члени правління організації.

Глава Держспецзв'язку Юрій Щеголь заявив, що під час воєнних дій українські експерти з безпеки активно співпрацювали з Центром передових технологій з кібероборони НАТО. Також група делегатів з України вперше взяла участь у засіданні CCDCOE». ***(Україна розпочала процес приєднання до Центру передових технологій з кібероборони НАТО // PaySpace Magazine (https://psm7.com/uk/security/ukraina-nachala-process-prisoedineniya-k-centru-peredovyx-texnologij-po-kiberoborone-nato.html). 21.01.2023).***

***

«Учитывая важность киберпространства и информационного пространства, Встреча министров цифровых технологий АСЕАН (ADGMIN)

запустила Стратегию сотрудничества АСЕАН в области кибербезопасности (2021–2025 гг.). Для реализации этой стратегии в 2022 году были запущены некоторые инициативы. Например, в январе 2022 года Совещание старших должностных лиц АСЕАН по вопросам образования (SOM-ED) запустило «Программу подготовки инструкторов для противодействия дезинформации и повышения медиаграмотности». развивать медиаграмотность и критическое мышление в качестве защиты от дезинформации.

В июне 2022 года 16-е совещание министров обороны АСЕАН (ADMM) приняло круг ведения Центра передового опыта ADMM по кибербезопасности и информации (ACICE). Условия определяют четыре основных рабочих направления, а именно: (i) создание базы данных о кибервредоносных программах и информационных угрозах, (ii) повышение осведомленности и знаний, например, посредством аналитических центров и академических обменов, (iii) содействие взаимодействию, например, посредством диалогов и упражнений и (iv) поддержка деятельности Сети киберзащиты АСЕАН (ACDN).

В октябре 2022 года была создана Региональная группа реагирования на компьютерные инциденты АСЕАН (CERT) для повышения оперативной готовности региона и углубления сотрудничества и обмена информацией между национальными CERT, академическими кругами и промышленностью. Признавая важность трансграничных информационных инфраструктур, в сферу функций CERT входят банковский, авиационный и морской секторы.

Подводя итоги года, можно сказать, что в заявлении председателя по итогам саммита АСЕАН в ноябре 2022 года были отмечены существующие усилия, в том числе деятельность рабочих групп экспертов ADMM-Plus (EWG) и региональной CERT АСЕАН, которые способствовали укреплению региональной кибербезопасности. Заявление также поддерживает усиленную синергию между механизмами АСЕАН для поддержания безопасности и региональной архитектуры, ориентированной на АСЕАН.

Важность синергии

В двух конкретных областях — российско-украинской войне и морской безопасности, — где злонамеренные кибер- и информационные операции могут проводиться совместно для достижения стратегического или тактического преимущества, контрмеры АСЕАН выиграют от синергии, возникающей в результате сотрудничества.

Основываясь на текущих тенденциях, прогноз компании по кибербезопасности Mandiant на 2023 год предсказывает продолжение злонамеренных операций в форме кражи цифровых учетных данных, атак типа «программа-вымогатель как услуга», кибершпионажа и информационных операций, в том числе со стороны хактивистских фронтов и переданы на аутсорсинг субъектам «взлома по найму» для целевых государственных и стратегических организаций частного сектора. Более того, эти операции повлияют на информационные системы и проникнут в платформы социальных сетей, как и предсказывает компания Norton, занимающаяся кибербезопасностью.

Такие операции могут иметь ограниченное ощутимое влияние во время войны. Но они могут быть мощными инструментами в континууме между миром и

войной, также известном как серая зона, где геополитическая борьба между крупными державами становится все более интенсивной. Для АСЕАН ситуация в серой зоне из-за динамики действия-реакции, вызванной операциями влияния Китая, сохранится. Как заявил бывший министр иностранных дел Индонезии доктор Марти Наталегава, регион снова окружен дугой нестабильности. Следовательно, АСЕАН нуждается в дальновидном подходе к поддержанию безопасности.

Дальновидный подход может сделать обмен анализом угроз и опытом более значимым и может быть направлен на выявление возможностей синергии между различными механизмами и инициативами АСЕАН. Например, чтобы извлечь уроки из кибер- и информационных операций в российско-украинской войне, оборонным ведомствам следует проанализировать, как субъекты угроз могут извлечь уроки из российско-украинского опыта, чтобы улучшить свою игру. Подобно тому, как субъекты угроз могут зависеть от синергии кибер- и информационных операций для воздействия на свою целевую аудиторию, защита от таких угроз требует синергии превентивных и контрмер. Это стремление учиться у настоящего, чтобы подготовиться к будущему, является ролью, которая лучше всего подходит для центров, связанных с АСЕАН, особенно в рамках ACICE.

Потенциальные области синергии

Существующие и вероятные сценарии угроз и их результаты можно разделить на тематические области, имеющие отношение к исследованиям АСЕАН. Они могут служить основой для понимания того, как различные кибер- и информационные угрозы пересекаются, и как должна быть синергия между различными инициативами АСЕАН в области кибер- и информационной безопасности для устранения этих угроз. Для начала АСЕАН может сосредоточиться на двух тематических областях, основанных на ключевых событиях в области безопасности в 2022 году.

Во-первых, АСЕАН могла бы обратиться к событиям в российско-украинской войне, чтобы оценить текущие предположения, лежащие в основе кибер- и информационных операций. Со стороны агрессора, как субъекты угрозы могут лучше интегрировать кибер- и информационные операции с кинетическими операциями в серой зоне и на войне для достижения большего стратегического воздействия? Они могли бы принять более основанный на разведке подход к кибер- и информационным операциям, в частности, участвовать в кибер-вторжениях для сбора разведданных перед запуском враждебных кинетических операций. Но для правдоподобного отрицания субъекты угрозы могут осуществлять такие вторжения через киберпреступников, которые не связаны нормами ответственного поведения государства.

Со стороны защитников, как АСЕАН может помочь смягчить такие злонамеренные операции, которые дестабилизируют национальное киберпространство стран АСЕАН, оказывая косвенное влияние на региональную безопасность? В этом контексте АСЕАН также необходимо будет предусмотреть непредвиденный случай, когда технологические корпорации частного сектора по какой-то причине могут рассчитать, что они имеют меньше коммерческих и

политических интересов в защите цифровых инфраструктур региона, если в Индо-Тихоокеанском регионе разразится война, чем они. иметь в защите от угроз, связанных с российско-украинской войной.

Для изучения этих вопросов Рабочая группа экспертов ADMM-Plus (EWG) по кибербезопасности могла бы возглавить проведение семинаров при поддержке ACICE. Учитывая взаимосвязанность гражданского, делового и военного секторов в кибер-информационном пространстве, в семинарах должны участвовать представители невоенных механизмов АСЕАН, таких как ADGMIN и SOM-ED. Их роль будет иметь важное значение для планов по привлечению частного сектора и защите гражданского населения от психологического воздействия киберугроз и информационных угроз.

Во-вторых, АСЕАН могла бы оценить волну киберугроз, затрагивающих морской сектор. Этот сектор, один из столпов глобальных цепочек поставок, быстро переходит на цифровые технологии, что делает его более уязвимым для кибератак. Такие атаки могут служить целям военного и коммерческого шпионажа. Но они будут более разрушительными, если прервут работу навигации и других бортовых систем, что приведет к авариям и сбоям в бизнес-операциях. Например, базирующийся в Великобритании Центр судоходства НАТО выпустил предупреждение о рисках для гражданского судоходства, которые могут быть вызваны кибератаками на системы навигации и связи судов.

Точно так же кибератаки, затрагивающие суда на оживленных морских коммуникациях, таких как Малаккский и Сингапурский проливы (SOMS), могут быть разрушительными и принудительными. Следовательно, инициативы АСЕАН в области кибербезопасности и информационной безопасности должны уделять больше внимания морскому сектору, в первую очередь потому, что большинство стран АСЕАН зависят от морской связи. Учитывая угол морской безопасности, может быть синергия между этими инициативами АСЕАН и другими региональными / субрегиональными усилиями, такими как Центр обмена информацией ReCAAP (ISC) и четырехсторонний патруль Малаккского пролива (MSP).

В частности, ЭРГ ADMM-Plus по кибербезопасности и безопасности на море могли бы организовать совместные семинары, чтобы лучше понять взаимодействие между обеими областями безопасности и предвидеть проблемы, которые могут возникнуть в результате кибератак на суда вдоль SOMS. В этих семинарах должны участвовать представители ReCAAP ISC и MSP. Их роль будет иметь важное значение для организации обмена наземной информацией и выявления аномалий, которые могут свидетельствовать о морских инцидентах, связанных с киберпространством, а также для привлечения судоходной отрасли и разработки скоординированных планов реагирования на инциденты.

Заключение

Кибер- и информационные угрозы, с которыми АСЕАН может столкнуться в ситуации, формируемой развивающимися субъектами угроз и острой геополитической конкуренцией, весьма разнообразны. АСЕАН должна опираться на существующие усилия в этом пространстве. Но чтобы идти в ногу с угрозами, он должен применять дальновидный подход и искать синергию между различными

механизмами и инициативами АСЕАН. На фоне появления новых мини-партнеров и обязательств (например, Quad), которые продвигаются крупными державами и все больше сосредоточены на технологиях 5G и кибербезопасности, такое дальновидное мышление и синергетические действия могут добавить больше структуры и содержания региональной безопасности, ориентированной на АСЕАН. Архитектура». ***(Muhammad Faizal bin Abdul Rahman. Advancing Cyber And Information Security Cooperation In ASEAN – Analysis // Eurasia Review (https://www.eurasiareview.com/04012023-advancing-cyber-and-information-security-cooperation-in-asean-analysis/). 04.01.2023).***

***

«Тайвань планирует сотрудничать с Литвой в области кибербезопасности, заявила министр по цифровым вопросам Тайваня Одри Тан, посетившая Литву на прошлой неделе.

По ее словам, Национальный институт кибербезопасности Тайваня может принять решение об инвестировании в кибербезопасность Литвы уже на этой неделе.

«Как председатель правления я поделюсь историями своего визита в Литву, я поговорю с правлением Национального института кибербезопасности о близости ценностей и процветающих стартапах и единорогах, которых я встретил в Литве. На заседании правления мы решим, сколько инвестиций мы будем делать», — сказала она в интервью BNS.

И в Литве, и на Тайване есть хорошие компании, предоставляющие услуги кибербезопасности, и обе страны имеют международную репутацию в этой области, сказал Тан, добавив, что это сотрудничество будет основано на государственно-частном партнерстве и сотрудничестве с населением.

Министр экономики и инноваций Литвы Аушрине Армонайте заявила, что Литва является «чемпионом ЕС» в области финансовых технологий и надеется на сотрудничество с тайваньскими компаниями. Тан подтвердил возможность совместной работы двух стран в секторах финансовых технологий и информационных технологий.

По словам Танга, конкретных планов и инвестиционных решений тайваньских ИТ- и финтех-компаний в Литве можно ожидать после встречи представителей этих секторов. Делегация литовского ИТ-бизнеса посетит Тайвань в конце этого года…» ***(Taiwan vows to invest in Lithuania's cyber security – Taiwanese minister // Lithuanian Radio and Television (LRT) (https://www.lrt.lt/en/news-in-english/19/1867649/taiwan-vows-to-invest-in-lithuania-s-cyber-security-taiwanese-minister). 16.01.2023).***

***

«Украина сделала еще один шаг к углублению своих связей с НАТО, подписав соглашение об официальном оформлении своего участия в Объединенном центре передовых технологий в киберзащите (CCDCOE) альянса по безопасности.

CCDCOE функционирует как центр знаний по киберзащите, исследовательское учреждение, а также центр обучения и учений, который помогает членам с технологиями, обменом информацией об угрозах и политическим опытом. Членство в CCDCOE не ограничивается странами НАТО.

Украина подала заявку на вступление в эстонский центр в августе 2021 года. В апреле прошлого года 27 стран-спонсоров в руководящем комитете единогласно поддержали Украину в качестве участника CCDCOE, тем самым предоставив другому государству-члену доступ к «ценному первому ручное знание нескольких противников».

Эта формулировка была намеком как на тактику кибервойны, которую Россия использовала до и во время своего незаконного вторжения в Украину, так и на более ранние атаки Москвы на украинские электросети и другие цифровые объекты.

Новое техническое соглашение, которое должны подписать все страны-члены центра, официально закрепит участие Украины в группе киберзащиты.

«В течение прошлого года мы уже активно сотрудничали с Объединенным центром передовых технологий киберзащиты НАТО», — говорится в заявлении главы государственного спецназа Украины Юрия Щиголя.

Действительно, страна Щеголя стала эпицентром противодействия российским кибератакам. Группа реагирования на компьютерные чрезвычайные ситуации Украины (CERT-UA) только в прошлом году отследила 2100 инцидентов и кибератак, и более 1500 из них произошли после полномасштабного военного вторжения России в феврале.

Директор CCDCOE и его руководитель по международным связям посетили Украину в ноябре 2022 года, чтобы обсудить ее опыт противодействия российским кибератакам. «Надеюсь, что наше сотрудничество в этом году только укрепится», — добавил Щиголь.

Регистр обратился к прибалтийским государствам-членам центра за комментариями и не получил немедленного ответа.

Том Келлерманн, старший вице-президент по киберстратегии поставщика программного обеспечения Contrast Security, который также занимал должности в сфере кибербезопасности в правительстве США, назвал этот шаг «историческим». Во-первых, Украина может использовать центр, чтобы поделиться тем, что она узнала, выдержав кибератаки со стороны Кремля.

«Украина находится в осаде в результате скоординированных разрушительных российских кибератак с 13 января 2022 года. Это значительно повысит ситуационную осведомленность НАТО в связи с кампаниями элитных российских групп APT, что позволит НАТО защитить критически важные инфраструктуры от растущих российских кибератак», — сказал он. Регистр.

Это также означает «резкий сдвиг» как в доктрине США, так и в НАТО в отношении наступательных киберкампаний, направленных на срыв российских атак, добавил Келлерманн.

«С 2013 года, когда генерал Герасимов произнес свою знаменитую речь о гибридной войне и пользе кибератак, Россия относительно безнаказанно атакует Украину и членов НАТО в результате коллективного киберответа», — сказал он.

«Теперь России придется играть в обороне». ***(Jessica Lyons Hardcastle. Ukraine slides closer to NATO with buckets of experience fending off Moscow's cyberattacks // The Register (https://www.theregister.com/2023/01/24/ukraine_nato_cyber_defense/). 24.01.2023).***

***

«На этой неделе Организация Объединенных Наций начнет слушания по своему первому в истории глобальному соглашению о киберпреступности, чтобы сосредоточиться на реагировании государств на киберпреступность и скоординированном обмене разведданными. Предлагаемый договор направлен на юридическую классификацию различных киберпреступлений и выработку единого международного ответа.

В 2019 году Генеральная Ассамблея ООН приняла резолюцию о «противодействии использованию информационно-коммуникационных технологий в преступных целях».

Последнее слушание, которое пройдет в Вене с 9 по 20 января, будет посвящено тому, как государства должны реагировать на киберпреступления, и мерам, которые правоохранительные органы могут принять для борьбы с преступлениями. В рамках слушаний редакционный комитет примет рекомендации от ключевых заинтересованных сторон, таких как представители государства и члены организаций гражданского общества.

Предлагаемый договор определяет киберпреступность как любые «уголовные преступления, совершенные умышленно и незаконно» с использованием ИТ-устройств. Далее в нем перечислены различные виды преступной деятельности, которые считаются незаконными. К ним относятся, среди прочего, незаконный доступ, вмешательство в сеть и взлом оборудования или программного обеспечения, что приводит к компрометации критически важной инфраструктуры или утечке конфиденциальных государственных данных.

Определяя и четко определяя, что представляет собой различные киберпреступления, договор стремится предоставить государствам правовую основу для судебного преследования потенциальных преступников, которые могут варьироваться от опытных национальных хакеров до сотрудников, которые незаконно получают доступ к конфиденциальным правительственным данным.

В проекте предложения также изложены меры, которые могут принять государства, такие как предоставление правоохранительным органам права собирать данные в режиме реального времени, изымать устройства, используемые для киберпреступлений, координировать свои действия со спецслужбами и оказывать помощь жертвам различных киберпреступлений.

Критики отвечают

Комментируя проект договора, Интерпол, который опубликовал свои рекомендации перед предстоящим слушанием, говорит, что необходима более тонкая координация между национальными киберагентствами, «чтобы охватить

широкий спектр киберпреступлений». По словам агентства, предложение также направлено на решение проблемы занижения сведений о киберпреступлениях в правоохранительные органы путем улучшения каналов связи.

Международная торговая палата Великобритании рекомендовала, чтобы преступления, которые уже включены в уголовный список, уже рассматривались как преступные действия, а не «просто незаконные» действия.

ICC также заявила, что более широкая классификация вторжения в сеть как уголовного преступления повлияет в равной степени на специалистов по тестированию на проникновение и исследователей безопасности, поскольку их работа связана с компрометацией сетей, доступом к ним, а также просмотром и извлечением информации. Поэтому агентство рекомендует, чтобы проект договора обновил сферу действия преступления, «чтобы гарантировать, что действия, которые проводятся добросовестно в законных целях, такие как тестирование на проникновение, не подпадают под действие конвенции».

Январские слушания — это четвертый раунд переговоров по договору. Пятый и шестой раунды слушаний пройдут в сентябре, после чего договор будет представлен Генеральной Ассамблее ООН для доработки. Соглашение должно вступить в силу в начале 2024 года». ***(Akshaya Asokan. UN to Hold Hearing on Proposed Cybercrime Treaty // Information Security Media Group, Corp. (https://www.govinfosecurity.com/un-to-hold-hearing-on-proposed-cybercrime-treaty-a-20884). 08.01.2023).***

***

«Airbus в очередной раз проявил интерес к кибербезопасности, большим данным и цифровому бизнесу Atos стоимостью 4,8 миллиарда долларов, на этот раз в качестве миноритарного акционера, сообщает Les Echos.

По словам Les Echos, голландский производитель самолетов начал предварительные переговоры о приобретении неконтролирующей доли в бизнесе Atos Evidian, который Atos намеревается выделить в отдельную публичную компанию к концу 2023 года. После разделения Atos сосредоточится исключительно на своем бизнесе по инфраструктуре и управлению данными стоимостью 6,99 млрд долларов, а также на подразделении бизнес-решений и платформ стоимостью 4,38 млрд долларов.

«Компания провела предварительные обсуждения с потенциальными будущими заинтересованными сторонами из числа меньшинств в отношении сферы деятельности, объединенной под названием «Evidian», — сообщает Atos в заявлении Information Security Media Group. «Эти обсуждения недостаточно продвинуты, чтобы можно было дать дальнейшие комментарии».

Конгломерат со штаб-квартирой в Париже заявляет, что намерен сохранить до 30% акций Evidian после разделения и будет использовать выручку от продажи доли в Evidian для финансирования своего плана преобразования оставшейся части Atos. Продажи в подразделениях инфраструктуры и управления данными, а также бизнес- и платформенных решений упали на 3% и 7,9% соответственно в 2020 году.

Airbus сообщает ISMG, что не комментирует рыночные слухи или спекуляции. «Как глобальная компания, мы ведем постоянные обсуждения с нашими партнерами, клиентами и поставщиками по всей отрасли, но эти разговоры носят частный характер».

Миноритарный пакет будет представлять стратегический интерес для Airbus, ключевого подрядчика оборонной промышленности, сообщает Les Echos. По словам Les Echos, купив долю в Evidian, Airbus облегчит доступ к защищенным системам связи, которые она устанавливает на производимые ею военные машины.

Последний повод для приобретения появился через 10 месяцев после того, как французская телекомпания BMV сообщила, что Airbus рассматривает возможность приобретения Atos из-за своего интереса к сфере кибербезопасности. В то время Airbus решила не покупать Atos в целом, поскольку не интересовалась другой деятельностью компании, в то время как Atos в марте 2022 года утверждала, что ее подразделение Evidian не выставлено на продажу.

Инвесторы в Atos положительно отреагировали на сообщения об интересе к Airbus, в результате чего акции компании выросли на 26,9%, или на 2,42 доллара, до 11,43 доллара за акцию на торгах с момента публикации отчета Les Echos 1 января. Аналогичным образом, акции Airbus выросли на 3,9%., или 4,36 доллара, до 111,02 доллара за акцию с момента появления отчета Les Echos.

Airbus делает все возможное для обеспечения кибербезопасности

Исторически у Airbus было три подразделения: бизнес коммерческих самолетов стоимостью 40,11 млрд долларов, который вырос на 6% в 2021 году; оборонный и космический бизнес стоимостью 11,3 миллиарда долларов, который сократился на 2% в 2021 году; и вертолетный бизнес стоимостью 7,22 миллиарда долларов, который вырос на 4% в 2021 году. Кибербезопасность была частью оборонно-космического подразделения Airbus и включает в себя центры операций по обеспечению безопасности, службы реагирования на инциденты и криптографию для стран НАТО.

В июне компания объявила о планах объединить все существующие службы кибербезопасности в единое подразделение под названием Airbus Protect и инвестировать в укрепление общей деятельности Airbus в области кибербезопасности. Airbus Protect дебютировал 1 июля 2022 года. В компании работает более 1000 сотрудников во Франции, Великобритании, Испании и Германии, и она занимается промышленной кибербезопасностью, критической инфраструктурой и услугами по обеспечению безопасности.

В прошлом году Airbus купил немецкого поставщика криптографических и коммуникационных систем DSI Datensicherheit, чтобы лучше обслуживать компании в космическом, авиационном, военно-морском и наземном секторах. По словам Airbus, сделка объединит команды по кибербезопасности, специализирующиеся на криптографии для защиты, с космическими заказчиками и программами.

Кроме того, Airbus управляет дочерней компанией по кибербезопасности Stormshield в Европе, в которой работает 400 человек, которая продает данные, конечные точки и технологии сетевой безопасности. В прошлом году Airbus заявила, что расширит исследования и разработки Stormshield, чтобы обогатить

портфолио компании в области сетевой безопасности, шифрования данных, обнаружения и реагирования конечных точек.

Разговоры об Airbus последовали за отказом Atos от Onepoint

Предварительные переговоры Airbus о продаже доли в Evidian начались всего через три месяца после того, как компания отклонила предложение конкурента Onepoint на сумму 4,12 млрд долларов о полной покупке Evidian. Onepoint планировала объединиться с британским фондом прямых инвестиций ICG для финансирования сделки, которая, по словам основателя Onepoint Дэвида Лаяни, создаст 20 000 рабочих мест в Европе.

Однако в сентябре Atos заявила, что ее совет директоров единогласно решил, что предложение Onepoint не отвечает интересам компании и ее заинтересованных сторон.

Выручка бизнеса Atos Evidian в первой половине 2022 года увеличилась до 2,49 млрд долларов, что всего на 2% выше, чем 2,44 млрд долларов годом ранее в постоянной валюте, благодаря росту выше рынка благодаря практике кибербезопасности компании. В Evidian работает 50 000 сотрудников, занимающихся цифровым преобразованием стоимостью 3,43 млрд долларов, и 9 000 сотрудников, обслуживающих практику работы с большими данными и безопасностью стоимостью 1,38 млрд долларов.

Атос говорит, что практика Evidian в области кибербезопасности имеет высокую операционную прибыль, исчисляемую однозначными числами, и была признана Gartner ведущим поставщиком управляемых услуг безопасности в мире. Практика больших данных и безопасности Atos выиграла от агрессивной стратегии приобретения: компания купила немецкого специалиста по криптографии Cryptovision в сентябре 2021 года и канадскую консалтинговую фирму по кибербезопасности In Fidem в январе 2021 года.

В конце 2020 года Atos приобрела австрийского консалтингового провайдера SEC Consult Group и нидерландскую компанию Motiv ICT Security, а также провайдера управляемого обнаружения и реагирования Paladion из Рестона, штат Вирджиния, и фирму Digital Security со штаб-квартирой в Париже». ***(Michael Novinson. Report: Airbus Eyes Minority Stake in Atos Security Business // Information Security Media Group, Corp. (https://www.govinfosecurity.com/report-airbus-eyes-minority-stake-in-atos-security-business-a-20854). 04.01.2023).***

***

«В этом году на 10-й ежегодный конкурс на лучшую научную работу по кибербезопасности было представлено 28 публичных номинаций.

10-й ежегодный конкурс на лучшую научную работу по кибербезопасности отмечает лучшую фундаментальную статью по кибербезопасности, опубликованную в 2021 году. Победителем стала статья «Проверка гиперсвойств с помощью временной логики действий (TLA)», авторами которой являются Лесли Лэмпорт и Фред Б. Шнайдер из Microsoft Research and Корнельского университета, соответственно, отвечает на ключевой вопрос: как вы можете гарантировать, что компьютерный алгоритм верен?

В документе, опубликованном на симпозиуме IEEE Computer Security Foundations 2021 года, говорится, что множество доступных инструментов безопасности обычно исследуют определенные фрагменты кода, а не сам алгоритм. Вместо этого подхода Лэмпорт и Шнайдер предлагают, чтобы для проверки точности алгоритма (и, возможно, системы) можно было обратить внимание на теоретические и практические достижения.

Лэмпорт и Шнайдер показывают, как подтвердить, что алгоритм удовлетворяет определенным гиперсвойствам, необходимым для определения правильности. Гиперсвойства — это наборы свойств, которые могут выражать политики безопасности, такие как безопасный поток информации, которые не могут быть реализованы сами по себе. Их следует понимать с точки зрения многократных запусков программы, например, предсказывает ли значение одной переменной значение другой, т. е. происходит ли утечка информации.

В статье-победителе отражен революционный прорыв, заключающийся в том, что эти гиперсвойства могут быть сформулированы с использованием временной логики действий (TLA), которая представляет собой способ описания систем с помощью единой математической формулы. Эта связь с установленным набором инструментов позволяет изучать гиперсвойства в будущих исследованиях и разработках в области кибербезопасности.

«Эта статья является одним из лучших примеров за десять лет конкурса, который подчеркивает вершину практических исследований в области кибербезопасности: достижения, основанные на прочной фундаментальной работе», — заметил директор по исследованиям Агентства национальной безопасности (АНБ) г-н Джил Эррера.

Второй документ «Использование оборонительных технологий политическими активистами во время суданской революции», написанный Алаа Даффалла, Люси Симко, Тадаёси Коно и Александру Г. Бардас из Корнельского университета, Университета Джорджа Вашингтона, Вашингтонского университета и Университета Канзаса соответственно, получает почетное упоминание. В их статье исследуется практика 13 суданских активистов и то, как можно использовать технологии во времена политических раздоров. Авторы исследуют потребности в компьютерах и конфиденциальности в условиях репрессивного режима. Этот документ также был представлен на симпозиуме IEEE 2021 года по безопасности и конфиденциальности.

В этом году на 10-й ежегодный конкурс на лучшую научную работу по кибербезопасности было представлено 28 публичных номинаций, и победитель был выбран г-ном Эррерой, работавшим с группой выдающихся экспертов, включая следующих: Уитфилд Диффи, советник по кибербезопасности; Дэн Гир, In-Q-Tel; Эрик Гросс, советник по кибербезопасности; Пол Кохер, независимый исследователь; Джон Лаунчбери, Galois, Inc.; Кэрри Гейтс, Банк Америки; Шон Пейсерт, Национальная лаборатория Лоуренса Беркли; Фил Венейблс, Google; Арун Вишванат, советник по кибербезопасности; Мэри Эллен Зурко, Линкольнская лаборатория Массачусетского технологического института; и Радиа Перлман, DELL EMC…». ***(Winning Cybersecurity Paper Addresses Algorithm Accuracy // Homeland Security Today (https://www.hstoday.us/subject-matter-***

areas/cybersecurity/winning-cybersecurity-paper-addresses-algorithm-accuracy/). 10.01.2023).

***

«…Директор Агентства кибербезопасности и безопасности инфраструктуры (CISA) Джен Истерли встретилась с Bloomberg TV на выставке Consumer Electronics Show, чтобы обсудить важность безопасности и прозрачности, поскольку технологии продолжают развиваться для потребителей.

Во время крупнейшей в мире выставки технологий директор Истерли попросил технологических лидеров относиться к кибербезопасности как к основному бизнес-риску, а к лидерам отрасли и создателям использовать безопасность по умолчанию и безопасность по умолчанию при выводе новых продуктов на рынок.

Во время беседы с Эдом Ладлоу из Bloomberg TV директор Истерли подчеркнула, что «когда люди создают технологии, они не должны ограничиваться стоимостью, возможностями, производительностью и скоростью выхода на рынок. Они должны помнить об элементарной безопасности. Безопасность не должна следовать кривой инноваций. Безопасность должна двигаться вместе с кривой инноваций».

Далее она сказала: «Кибербезопасность, кибербезопасность — это общественное благо. Речь идет о социальной устойчивости. Со всем, что связано в эти дни, вы не можете просто беспокоиться о своей собственной компании. Мы должны перестать ставить самосохранение выше сотрудничества».

Она назвала этот подход «правильным для ваших клиентов».

Она также призвала руководителей бизнеса «рассматривать кибербезопасность как основной бизнес-риск»…» ***(CISA Director Calls on Technology Makers to Prioritize Security // Homeland Security Today (https://www.hstoday.us/federal-pages/dhs/cisa-director-calls-on-technology-makers-to-prioritize-security/). 07.01.2023).***

***

«Кибератаки резко возросли в последние годы, при этом система здравоохранения и другие критически важные секторы все чаще подвергаются цифровым атакам, поскольку угроза вредоносных программ, таких как программы-вымогатели и иностранные шпионские программы, продолжает развиваться.

В частности, в прошлом году официальные лица и законодатели вновь сосредоточили свое внимание на кибербезопасности и стремились защитить критически важные секторы страны от растущих киберугроз. Ожидается, что этот вопрос будет продолжать занимать центральное место в следующем году, поскольку многие из этих угроз все еще обостряются, а киберсектор сталкивается с постоянной нехваткой рабочей силы в своих усилиях по укреплению цифровой защиты США.

Вот четыре кибер-проблемы, которые, как ожидается, станут приоритетными в 2023 году.

Угрозы критическим секторам

Финансовый, энергетический и медицинский секторы сталкиваются со стремительным ростом числа взломов. Кибератаки украли у компаний в этих отраслях сотни миллионов долларов, раскрыли данные и даже нарушили работу основных служб, как, например, когда атака программы-вымогателя вынудила закрыть Colonial Pipeline в 2021 году, что привело к нехватке газа в нескольких штатах.

В частности, за последние несколько лет в секторе здравоохранения наблюдается рост числа кибератак, особенно атак программ-вымогателей, нацеленных на больницы с целью получения доступа к конфиденциальной информации, такой как данные пациентов или медицинские исследования и технологии. Растущие угрозы для этого сектора вызвали тревогу в Вашингтоне, и сенатор Марк Уорнер (штат Виргиния), председатель сенатского комитета по разведке, предупредил этой осенью, что кибератаки могут привести к задержкам в лечении и даже к смерти пациентов.

Официальные лица уже активизировали свои усилия по защите важнейших секторов от этих развивающихся угроз и указали, что это останется главным приоритетом в этом году.

Энн Нойбергер, заместитель советника Белого дома по национальной безопасности по кибербезопасности и новым технологиям, заявила в октябре, что администрация Байдена уделяет «неустанное внимание» обеспечению безопасности таких секторов, особенно тех, где сбои могут привести к опасностям, например, в больницах, нефтегазовой отрасли и компаний, занимающихся транспортировкой химических веществ.

«Наши опасения переросли в то, что нас больше всего беспокоит деградация или сбои в работе критически важных служб», — сказал Нойбергер.

Но законодатели и отраслевые эксперты призвали федеральные агентства еще больше активизировать свои усилия в последние месяцы.

Защита критической инфраструктуры, такой как секторы энергетики и здравоохранения, играет ключевую роль в снижении киберрисков, сказала Жозефин Вольф, доцент политики кибербезопасности в Школе права и дипломатии им. Флетчера Университета Тафтса.

«Я бы сказал, что во всех этих областях мы еще многое можем сделать, чтобы попытаться укрепить оборону и повысить устойчивость», — сказал Вольф.

В письме, адресованном Министерству здравоохранения и социальных служб в августе, сенатор Ангус Кинг (штат Мэн) и член палаты представителей Майк Галлахер (штат Висконсин) выразили признательность за шаги, предпринятые администрацией Байдена в ответ на киберугрозы для сектор здравоохранения, но заявил, что необходимы дополнительные действия.

«Однако мы по-прежнему обеспокоены отсутствием надежного и своевременного обмена действенной информацией об угрозах с отраслевыми партнерами и необходимостью резкого расширения возможностей и ресурсов Департамента. В условиях экспоненциального роста киберугроз мы должны

уделить первоочередное внимание устранению пробелов в кибербезопасности сектора [здравоохранения и общественного здравоохранения]», — написали они.

Зинет Кемаль, инженер по безопасности облачных вычислений в Best Buy, сказал, что правительство должно продолжать работать с лидерами отрасли для выявления и устранения уязвимостей, обнаруженных в критических секторах, а также для создания планов действий в чрезвычайных ситуациях для реагирования на киберинциденты.

«Я думаю, что им нужно работать с отраслью, чтобы обеспечить защиту систем от киберугроз», — сказала она.

Атаки программ-вымогателей

В последние годы наблюдается особенно резкий всплеск атак программ-вымогателей, особенно нацеленных на здравоохранение и финансовый сектор.

Только в прошлом году группы вымогателей вызвали сбои в работе нескольких больничных систем, временно закрыли школы в некоторых частях США, осуществили многомиллионные взломы ряда компаний и вынудили Коста-Рику объявить чрезвычайное положение в мае из-за шквала атак. повлияло на его государственные услуги.

Ожидается, что в этом году борьба с программами-вымогателями в стране и за рубежом также будет иметь приоритет, поскольку США и их союзники объединились, чтобы противостоять возросшей угрозе. В 2021 году администрация Байдена вместе с несколькими другими странами запустила свою первую ежегодную инициативу, направленную на глобальную борьбу с программами-вымогателями.

В ноябре Белый дом провел второй саммит Международной инициативы по борьбе с программами-вымогателями, на который он пригласил более 30 стран обсудить шаги, которые они могут предпринять для сдерживания распространения программ-вымогателей во всем мире.

«Программы-вымогатели — это карманная проблема, которая ежегодно затрагивает тысячи компаний и частных лиц по всему миру», — говорится в пресс-релизе Белого дома.

Во время саммита страны изложили несколько инициатив, в том числе создание международной целевой группы по борьбе с программами-вымогателями, активный обмен информацией между государственным и частным секторами и принятие совместных мер, чтобы остановить участников программ-вымогателей, использующих криптовалютную экосистему.

Ожидается, что целевая группа по борьбе с программами-вымогателями, которую возглавляет Австралия, начнет работу в январе, сообщает CyberScoop.

Австралия возглавляет целевую группу, «потому что у них было несколько очень крупных атак программ-вымогателей», в том числе атака, направленная на одну из крупнейших частных медицинских страховых компаний страны, сообщил CyberScoop высокопоставленный чиновник администрации.

Вольф сказала, что, хотя программы-вымогатели, безусловно, останутся горячей темой в этом году, она считает, что США и их союзники в некоторой степени достигли своих возможностей, когда дело доходит до решения этой

проблемы, если только другие крупные страны, такие как Россия, не решат присоединиться и поддержать инициативу.

«Я думаю, что с этой инициативой мы, скорее всего, увидим, что такие страны, как Соединенные Штаты и Великобритания, попытаются помочь странам с меньшими возможностями в расследовании программ-вымогателей и наращивании своих возможностей», — сказала она.

Иностранное шпионское ПО

В прошлом году иностранное шпионское ПО привлекло внимание после разногласий вокруг израильской компании по разработке шпионского ПО NSO Group, которая была занесена в черный список Министерством торговли в 2021 году за якобы содействие незаконному наблюдению за государственными чиновниками, журналистами, диссидентами и правозащитниками.

Конгресс С тех пор предпринял шаги для рассмотрения обвинений. В июле комитет Палаты представителей по разведке включил в Закон о полномочиях разведки положение, разрешающее директору национальной разведки запрещать разведывательному сообществу США покупать и использовать иностранное шпионское ПО.

Законопроект также позволит президенту налагать санкции на иностранных правительственных чиновников и фирмы, которые нацелены на американских чиновников с помощью шпионских программ. Закон был включен в Закон о государственной обороне 2023 года и с тех пор стал законом.

Сторонники иностранных шпионских программ надеются, что в будущем будет сделано больше для решения этой проблемы, поскольку угрозы продолжают развиваться.

Майк Секстон, старший советник по киберполитике в программе национальной безопасности Third Way, сказал, что, хотя в прошлом году были предприняты некоторые действия по противодействию иностранным шпионским программам, предстоит еще многое сделать.

«Я думаю, что внесение NSO Group в черный список в 2021 году было действительно хорошо, но я думаю, что важно не останавливаться на достигнутом», — сказал Секстон.

Нехватка рабочей силы

Растущие киберугрозы привели к обострению давней нехватки рабочей силы в отрасли, поскольку как федеральные агентства, так и частные компании изо всех сил пытались занять ключевые роли в киберпространстве.

Отрасль стремилась решить проблему нехватки, инвестируя в развитие рабочей силы, и ожидается, что она продолжит делать это в будущем.

Министерство внутренней безопасности заявило, что решение проблемы нехватки является главным приоритетом для агентства. Ранее компания решала эту проблему в 2021 году, проведя 60-дневный спринт для найма специалистов по кибербезопасности. Из 500 предложений о работе, разосланных отделом, отдел смог нанять около 300 новых кибер-сотрудников.

Национальный кибер-директор Крис Инглис, который, как ожидается, уйдет на пенсию в ближайшие месяцы, также подтолкнул правительство к найму большего количества технических и кибер-специалистов.

«Нам удалось заполнить две трети вакансий, в которых есть слова «кибер» и «ИТ», и это хорошая новость», — сказал Инглис во время кибер-мероприятия, состоявшегося в октябре.

Однако он сказал, что предстоит еще долгий путь, потому что в то время треть этих рабочих мест все еще была вакантной.

Инглис также провел в июле саммит по кибер-трудовым ресурсам и образованию, в ходе которого участники обязались улучшить разнообразие и инклюзивность в кибер-сфере, а также создать национальную кибер-кадровую и образовательную стратегию.

Эксперты говорят, что ожидают большего государственного финансирования, предназначенного для помощи в обучении рабочей силы и образовательных инициатив, включая партнерство с частным сектором и университетами для увеличения потока кибер-работников.

«Для устранения этого пробела в будущем, я думаю, важно, чтобы организации и правительства инвестировали в программы обучения и образования, которые готовят следующее поколение профессионалов в области кибербезопасности», — сказал Кемаль». ***(Ines Kagubare. Four cyber concerns looming in the new year // Nexstar Media Inc. (https://thehill.com/policy/cybersecurity/3793535-four-cyber-concerns-looming-in-the-new-year/). 02.01.2023).***

***

«В настоящее время кибербезопасность является развивающейся отраслью. Крупным и малым организациям нужны специалисты по технологиям, которые могут защитить технологические стеки от внутренних и внешних угроз. Но какие навыки вам нужны, чтобы добиться успеха в роли кибербезопасности?

Обладание правильным сочетанием навыков (и получение работы) может привести к значительной компенсации. По данным Lightcast, который собирает и анализирует миллионы объявлений о вакансиях со всей страны, средняя зарплата специалиста по кибербезопасности составляет 96 257 долларов в год, и эта цифра, очевидно, может расти с опытом и специальными навыками.

Lightcast также прогнозирует, что позиции в области кибербезопасности вырастут на 23,1% в течение следующих 10 лет. Текущее время, необходимое для заполнения позиции, составляет 44 дня, что свидетельствует о высоком уровне спроса. Однако, несмотря на голод работодателей, вам все равно нужно будет продемонстрировать, что у вас есть все необходимое для выполнения работы.

Необходимые навыки кибербезопасности

Lightcast перечисляет следующие «необходимые навыки» для должности в области кибербезопасности, т. е. многие работодатели хотят, чтобы кандидаты обладали хотя бы некоторыми из следующих навыков:

Информационные системы
питон
линукс
Криптография

Управление проектом
Обслуживание клиентов
Аутентификация
Разработка программного обеспечения
Программная инженерия

Чтобы эффективно защищать системы, вы должны понимать, как они работают, отсюда и необходимость разработки программного обеспечения и инженерных знаний. Овладение некоторыми ключевыми принципами кибербезопасности, включая аутентификацию и криптографию, также является необходимым условием для работы.

В последние годы Python стал вездесущим языком, полезным в различных контекстах, помимо кибербезопасности. Эксперты по кибербезопасности также рекомендуют ознакомиться с Golang и Java, а также с Linux.

Определение навыков кибербезопасности

Далее следуют «определяющие навыки», которые Lightcast определяет как повседневные навыки, необходимые специалистам по кибербезопасности для выполнения своих задач в меру своих возможностей:

Информационная безопасность
Сетевая безопасность
Структура кибербезопасности NIST
Охранные операции
Обнаружения вторжений
Проверка на проницаемость
Оценка уязвимости
Splunk

Опять же, это имеет смысл: знание того, как выполнять основные задачи работы (такие как тестирование на проникновение и принципы сетевой безопасности), жизненно важно. Знание «наступательных» и «защитных» кибернавыков откроет широкий спектр возможностей.

Отличительные навыки кибербезопасности

Затем идут «отличительные навыки» Lightcast, которые определяются как продвинутые навыки, которые специалисты по кибербезопасности могут использовать, чтобы выделиться на переполненном рынке. Как вы заметите, многие из этих навыков составляют анализ высшего уровня; используйте их, чтобы предоставлять точную и понятную оценку угроз другим сотрудникам организации, а также план действий по устранению любых уязвимостей:

Анализ угроз
Информационная гарантия
Моделирование угроз
Знание кибербезопасности
Анализ уязвимостей
ИСО 27001
Оценка кибербезопасности
Разведка и анализ угроз
Безопасность данных

Предотвращение потери данных

Доказательство того, что у вас есть навыки

Учитывая нынешний дефицит талантов в области кибербезопасности, компании не обязательно будут требовать, чтобы все кандидаты на работу имели формальное образование и ученые степени, но любой, кто претендует на должность в области кибербезопасности, должен будет доказать, что он обладает навыками и опытом, необходимыми для выполнения этой работы. Ожидайте прохождения раундов технических собеседований, особенно если вы претендуете на руководящую должность.

Многие эксперты по кибербезопасности также проходят сертификацию, чтобы показать, что они обладают необходимыми навыками для успешной защиты систем. Согласно Lightcast, вот сертификаты, которые чаще всего появляются в объявлениях о вакансиях, связанных с кибербезопасностью:

CISSP

Security Clearance

SANS/GIAC

CISM

CompTIA Security+

CISA

Information Systems Certification

CCNA

ITIL

Также имейте в виду, что многие рабочие места, связанные с кибербезопасностью, прямо требуют определенных сертификатов, таких как CISSP, хотя вы можете убедить рекрутера или менеджера по найму, что ваш опыт эффективно заменяет сертификат». ***(Nick Kolakowski. Cybersecurity Skills You Need for Every Career Stage // Dice (https://www.dice.com/career-advice/cybersecurity-skills-you-need-for-every-career-stage). 06.01.2023).***

***

«По мере того, как организации становятся все более цифровыми, внедряя новые технологии, приложения и услуги, какие тенденции кибербезопасности мы можем ожидать в ближайшие 12 месяцев?

…в наступающем году мы можем ожидать, что злоумышленники продолжат искать способы использования уже существующих уязвимостей в организациях, а также недавно появившихся, поскольку организации идут в ногу с новыми инновациями и приложениями технологий, чтобы оставаться впереди. из пакета в постоянно развивающемся цифровом мире.

Защита удаленных и гибридных сотрудников

Хотя удаленная и гибридная работа, безусловно, снова сократилась в этом году, количество людей, работающих удаленно, остается выше, чем до пандемии: около 22% рабочей силы в Великобритании работали по крайней мере один день в неделю из дома, а 13% работали исключительно дома в сентябре. 2022 г. Поскольку самой большой уязвимостью кибербезопасности в любой организации

являются ее собственные сотрудники, это добавит дополнительный риск организациям по всей Великобритании.

Успешное использование уязвимой системы позволяет злоумышленнику выполнять широкий спектр вредоносных действий, особенно если использование уязвимости позволяет злоумышленнику получить доступ к критически важным бизнес-приложениям, которые лежат в основе каждой организации. Это может привести к значительному влиянию на жизненно важные области бизнеса, такие как цепочки поставок и производственные процессы, и даже позволить злоумышленникам перенаправить финансовые платежи и скомпрометировать очень конфиденциальные и потенциально строго регулируемые данные.

Вот почему снижение риска для критически важных бизнес-систем и приложений, связанного с человеческим фактором или новыми сложными системами или технологиями, должно оставаться приоритетом номер один для любой организации в 2023 году.

Большая зависимость от облачных технологий подвергает бизнес большему риску

Бесспорно, что сейчас мир внедряет облачные вычисления все более быстрыми темпами. На самом деле, многие организации по всей Великобритании описывают себя как «облачные» организации, поскольку они продолжают отдавать приоритет использованию и внедрению облачных предложений при поиске новых технологий. Хотя это приводит к повышению эффективности, производительности и зачастую безопасности для этих организаций, быстрое внедрение облачных технологий также приносит с собой ряд новых проблем безопасности, во многих случаях вызванных отсутствием ясности в отношении обязанностей по внедрению и обслуживанию. безопасности, когда речь идет об облачных развертываниях.

Чрезмерная зависимость от облака без учета безопасности приложений и служб в облаке может привести к тому, что критически важные бизнес-приложения будут подвержены угрозам, особенно в связи с серьезностью атак на цепочки поставок программного обеспечения, которые нацелены на менее безопасные элементы в цепочке поставок. вероятно, увеличится в следующем году.

Повышенное использование связности между приложениями и системами

По мере того, как организации становятся все более цифровыми, внедряя новые технологии, приложения и услуги для внедрения инноваций, повышения эффективности, обеспечения устойчивости и сохранения конкурентоспособности, они также становятся все более взаимосвязанными. Это связано с тем, что все эти технологии должны иметь возможность взаимодействовать друг с другом, чтобы обеспечить эффективность бизнес-процессов при одновременном снижении дублирования и избыточности данных.

Однако эти взаимосвязи и API-интерфейсы создают уникальные уязвимости в программных системах, предоставляя злоумышленникам возможность внедрить вредоносный код в любое из приложений, подключенных через незащищенные каналы связи. Уязвимость Log4j является особенно ярким примером этой подверженности риску кибербезопасности, поскольку уязвимый компонент используется бесчисленным количеством приложений и потенциально может быть

использован из открытых API-интерфейсов, которые требуются приложениям. Однако это открывает двери для вредоносных действий во всей системе или сети.

Log4j — это библиотека ведения журналов с открытым исходным кодом, которая обычно используется приложениями и службами в Интернете, и в следующем году злоумышленники продолжат использовать неисправленные уязвимости Log4j, о которых сообщила директор Агентства кибербезопасности и безопасности инфраструктуры США Джен Истерли. назвала самую серьезную уязвимость, которую она видела в своей карьере, а также увеличила их внимание к использованию библиотек с открытым исходным кодом.

Последствия геополитической напряженности продолжаются

Неудивительно, что по мере того, как геополитическая напряженность во всем мире продолжает расти, предприятия все больше внимания уделяют обеспечению своей устойчивости к таким геополитическим рискам, отдавая приоритет безопасности инфраструктуры в 2023 году. Однако кибербезопасность в государственном секторе по-прежнему серьезно отсутствует, особенно поскольку безопасность личной информации частных лиц, с которой сектор ежедневно справляется, имеет жизненно важное значение для конфиденциальности и соблюдения законов и правил о защите данных.

В течение 2022 года мы стали свидетелями бесчисленных атак на здравоохранение, образование, коммунальные услуги и другие важные сферы государственного сектора. Учитывая рост напряженности, решение этой проблемы становится еще более важным в 2023 году, и это станет главным приоритетом в повестке дня правительства в следующем году. Мы видим, как это уже воплощается в жизнь в решении Австралии разработать новую стратегию кибербезопасности после серии тяжелых атак на страну.

Экономические ограничения порождают новые тенденции в области кибербезопасности

Часто подход, используемый предприятиями для защиты критически важных бизнес-приложений, представляет собой широкую модель «глубокой защиты», в которой для защиты критически важных систем применяются технологические уровни. Однако при таком подходе не уделяется должного внимания безопасности каждого приложения, в результате чего предприятия становятся уязвимыми для злоумышленников, стремящихся воспользоваться существующими уязвимостями.

Кроме того, текущие проблемы нестабильной и сокращающейся экономики во всем мире означают, что расходы на кибербезопасность должны быть более целенаправленными и целенаправленными для борьбы с растущими (и все более изощренными) угрозами. Таким образом, организации будут более глубоко задумываться о стоимости атаки и будут стремиться улучшить свою защиту к 2023 году. Поэтому возможности управления уязвимостями, специально разработанные для защиты наиболее важных для бизнеса активов и систем организации, будут играть жизненно важную роль. роль в стратегии кибербезопасности в следующем году». ***(What cybersecurity trends can we expect to see in 2023 // Open Access Government (https://www.openaccessgovernment.org/cybersecurity-trends-to-expect-in-2023-digital-technologies-applications-services/150943/). 09.01.2023).***

***

«За последние десять лет произошло много технологических усовершенствований, от более простых вариантов банковского обслуживания с помощью мобильного банкинга до сравнительно простых решений для транзакций, инвестирования и заимствования; каждый день что-то новое доступно для изучения в цифровом виде. FinTech, обычно называемый финансовыми технологиями, упрощает управление многими задачами, которые являются частью повседневной жизни. Несмотря на то, что этот сектор существует уже очень давно, некоторые важные проблемы, такие как кибербезопасность, все еще необходимо решить, потому что многие все еще воспринимают FinTech как относительно новую концепцию. Однако, если эти проблемы не будут решены, они могут привести к серьезным проблемам в будущем.

Утечки данных происходят в результате многочисленных краж и взломов, и основная причина — отсутствие эффективных мер безопасности. Банки по закону обязаны ускорить внутреннюю защиту, в то время как финтех-компании сравнительно освобождены от этих требований…

Основные угрозы кибербезопасности в финтех-секторе

Подавляющее большинство финансовых учреждений в значительной степени полагаются на приложения, помогающие пользователям совершать транзакции. Разработчики приложений должны знать об опасностях и трудностях, чтобы принять эффективные меры безопасности для их смягчения.

Некоторые из примеров недостатков безопасности в Fintech перечислены ниже:

Проблемы безопасности с облачными вычислениями

Данные больше не нужно хранить на домашних компьютерах или в близлежащих центрах обработки данных. Облачные вычисления теперь являются основой для предоставления финансовых услуг через Интернет. Крайне важно знать о некоторых проблемах безопасности, поскольку облачные технологии становятся все более распространенными. Облачные вычисления предлагают различные преимущества, такие как скорость, доступность и масштабируемость. Однако из-за большого объема данных, проходящих через облако, хакерам легче проводить кибератаки. Финансовые учреждения должны убедиться, что выбранные ими облачные сервисы надежны. Незначительное нарушение может быстро превратиться в безвозвратную потерю. Одной из основных причин уязвимостей безопасности в облачных вычислениях является неправильная конфигурация облачных ресурсов.

Безопасность данных

Одной из самых больших проблем для финтех-сектора является кража личных данных и утечка данных. Для защиты платежной системы финтех-компании используют одноразовые пароли и другие методы аутентификации. Хакеры по-прежнему могут получить доступ к этим системам, похищая финансовые и личные данные. Финансовые компании всегда подвергались опасности утечки данных, поскольку кибератаки с каждым днем становятся все более изощренными, а обеспечение полной безопасности в цифровой сфере является довольно сложной задачей.

Вредоносные атаки

Наиболее частым видом киберрисков, затрагивающих сектор финансовых услуг, являются атаки вредоносных программ. Пользователи уязвимы для атак вредоносных программ при использовании ненадежного стороннего программного обеспечения, электронной почты или веб-сайтов. Атаки вредоносного ПО с большей вероятностью распространяются быстро и приводят к непоправимому ущербу.

Сторонние сервисы

Еще одна угроза безопасности, которая затрагивает банки и другие финансовые учреждения, — это доступ третьих лиц. Финансовые компании часто полагаются на стороннее программное обеспечение. Но хакеры часто используют эти сторонние программы в качестве шлюза. Они дают хакерам возможность выдавать себя за авторизованных пользователей и получать доступ к системам без авторизации, что ставит под угрозу безопасность данных. Финансовые учреждения должны выбирать надежного поставщика при работе со сторонним программным обеспечением.

Как избежать недостатков безопасности в Fintech — лучшие практики

Вот некоторые важные решения Fintech, которые следует учитывать при создании безопасных приложений.

Шифрование данных

При использовании шифрования информация кодируется и становится неразборчивой до тех пор, пока не будут использованы определенные ключи. Вы можете зашифровать свои данные, используя один из следующих алгоритмов:

RSA

TwoFish

3DES

Технологии безопасной аутентификации

Реализуйте следующие меры для защиты своего финтех-приложения от целевых внутренних и внешних угроз безопасности:

Система одноразовых паролей

Смена пароля

Мониторинг

Время сеансов входа

Адаптивная аутентификация

Управление доступом на основе ролей

В соответствии с вашей принадлежностью к определенной организации ролевой контроль доступа изменяет ваш уровень доступа. Даже если вы занимаете в компании должности ИТ-специалиста, заказчика, менеджера и т. д., вам не будет разрешен доступ к областям, не входящим в вашу компетенцию. Эта функция значительно снижает киберугрозы, как внутренние, так и внешние.

Крайне важно выбрать лучший бизнес по разработке программного обеспечения с соответствующим уровнем компетенции при создании вашего финтех-приложения, которое будет соответствовать всем вашим потребностям.

DevSecOps

В сочетании с текущими разработками в области кибербезопасности жизненный цикл разработки программного обеспечения повышает безопасность финтех-приложений. DevSecOps значительно упрощает разработку безопасного финансового приложения. Ключевым компонентом этой идеи является кибербезопасность в сочетании с другими важными элементами, такими как процесс тестирования.

Важность кибербезопасности в финтехе

Финтех-стартапы и фирмы предоставляют более гибкие товары и услуги по сравнению с банками. Кроме того, они обеспечивают более быстрое время выхода на рынок, что имеет решающее значение с точки зрения бизнеса. Из-за быстрых циклов выпуска финтех-компании часто упрощают свои продукты или исключают критически важные функции. Из-за этого финтех-компании часто лишь частично или полностью защищают свои решения, особенно когда они не могут сразу увидеть преимущества для своего бизнеса. Фирмы Fintech также могут снизить свои нефункциональные стандарты безопасности данных из-за отсутствия осведомленности о кибербезопасности и неправильного представления о том, что полностью безопасные продукты недостаточно гибки с точки зрения бизнеса.

Это часто приводит к созданию товаров, которые функциональны, но недостаточно защищены, что может привести к значительным затратам на безопасность, когда эти продукты масштабируются и должны быть должным образом защищены или исправлены. В результате ведение бизнеса с финтех-стартапами может быть более рискованным, чем доверие крупным банкам.

В целом, финтех-компания может с большей вероятностью столкнуться с нарушением безопасности, чем строго регулируемый банк, но последствия могут быть одинаковыми, поскольку обе компании обрабатывают одни и те же данные...» ***(Why is Cybersecurity crucial to the Fintech sector? // Techstrong Group (https://securityboulevard.com/2023/01/why-is-cybersecurity-crucial-to-the-fintech-sector/amp/). 19.01.2023).***

***

«Многие из вас путаются с терминами кибербезопасность и информационная безопасность и думают, что это одно и то же и синонимы. Однако на самом деле оба эти термина различны и смешиваются друг с другом.

Кибербезопасность — одна из важных бизнес-функций, направленная на защиту ИТ-инфраструктуры, такой как данные, приложения, коммуникационная инфраструктура и сеть. Поскольку организации сталкиваются с постоянными угрозами в киберпространстве, такими как DDoS, программы-вымогатели, вредоносные программы и утечки данных, кибербезопасность помогает отслеживать и смягчать угрозы для устранения бизнес-рисков.

Вместо этого информационная безопасность является частью программы кибербезопасности, которая в основном направлена на защиту данных от нарушений и повреждений. Бизнес, который работает с мотивом «данные означают жизненную кровь», должен быть чрезвычайно сосредоточен на информационной

безопасности, так как любая небольшая небрежность в этом может сломать бизнес на постоянной ноте.

По мере того, как компании переходят на цифровые технологии, становится чрезвычайно сложно защитить свою ИТ-инфраструктуру и данные от сбоев, взломов и других критических угроз.

Карьерные пути, связанные с информационной и кибербезопасностью

Поскольку оба эти слова технически перекрывают друг друга, например, в образовании, навыках и общих методах обеспечения безопасности, компании предлагают рабочие места, которые имеют общие карьерные пути.

Например, в потоке информационной безопасности преобладают такие роли, как аналитик по информационной безопасности, специалист по информационной безопасности, консультант по ИТ-безопасности с пакетом заработной платы от 80 000 до 120 000 долларов США.

Что касается кибербезопасности, преобладают такие роли, как аналитик по кибербезопасности, консультант по кибербезопасности, тестер проникновения, инженер по кибербезопасности со взаимозаменяемыми должностными инструкциями и с теми же пакетами заработной платы, как указано выше». ***(Naveen Goud. Difference between Cybersecurity and Information Security // Cybersecurity Insiders (https://www.cybersecurity-insiders.com/difference-between-cybersecurity-and-information-security/). 19.01.2023).***

***

«…Карьера в области кибербезопасности становится все более популярной и полезной для многих профессионалов. Специалисты по кибербезопасности защищают сети, системы и программы от цифровых атак. Это означает, что они являются первой линией защиты данных от злоумышленников.

Кибербезопасность — это высокотехнологичная область, требующая от людей различных навыков, таких как понимание сетей и разработки программного обеспечения, а также знание бизнес-процессов.

Карьера в области кибербезопасности динамична и постоянно развивается, что делает ее захватывающим вариантом для тех, кто ищет вызовы в своей профессиональной жизни.

Кибербезопасность — это постоянно растущая область, предоставляющая множество возможностей для карьерного роста. Профессионалы в этой области должны обладать знаниями в широком спектре технологий, таких как компьютерные сети, разработка программного обеспечения и управление базами данных.

Кибербезопасность и повседневные операции

По мере того, как компании все больше и больше полагаются на технологии для повседневных операций и коммуникаций, значение кибербезопасности значительно возрастает. С изменениями приходят и новые угрозы, а это означает, что технические ноу-хау также должны постоянно обновляться для эффективной защиты данных от злонамеренных третьих лиц.

Если вы заинтересованы в том, чтобы войти в сферу кибербезопасности, то, будучи хорошо информированным о тенденциях и обновлениях, вы сможете преуспеть в своей карьере.

Точно так же кибербезопасность — это приятная карьера. Для тех, кто увлечен защитой компаний от кражи данных. И другие вредоносные угрозы. Специалисты по кибербезопасности должны быть в курсе новейших технологий и быстро адаптироваться для выявления и анализа потенциальных киберугроз.

Те, кто занимается этой областью, могут найти полноценную работу, где им будут постоянно бросать вызов, сохраняя при этом данные в безопасности.

Преимущества карьеры в кибербезопасности

Кибербезопасность становится все более важной областью в современном цифровом мире. С развитием технологий важно обеспечить безопасность конфиденциальной информации и данных. В результате существует высокий спрос на людей, обладающих знаниями, навыками и опытом для защиты этих данных от злоумышленников.

Специалисты по кибербезопасности пользуются большим спросом, и у тех, кто хочет войти в эту захватывающую отрасль, есть множество вакансий. Поскольку заработная плата часто в несколько раз выше, чем у среднего ИТ-специалиста, кибербезопасность может стать отличным выбором карьеры.

Конкурентоспособная заработная плата и льготы

Кибербезопасность становится все более привлекательным вариантом карьеры из-за конкурентоспособной заработной платы и льгот, таких как возмещение расходов на обучение.

Эти рабочие места часто очень увлекательны и интересны, позволяя профессионалам со страстью к технологиям и решению проблем преуспеть. Кибербезопасность также распространяется на другие отрасли, такие как финансы, здравоохранение или правительство, а это означает, что эти люди могут иметь возможность работать в различных областях, внося значительный вклад в общество.

Неудивительно, что кибербезопасность становится популярной среди тех, кто хочет изменить наш цифровой мир.

Опять же, потребность в специалистах по кибербезопасности будет только расти по мере того, как мир становится все более взаимосвязанным. Однако вместе с этим появляется отличная возможность для тех, кто хочет оставаться на шаг впереди в отношении полезной и востребованной карьеры.

Предлагая огромный потенциал с точки зрения заработной платы и удовлетворенности работой, кибербезопасность делает ее жизнеспособным вариантом для многих людей.

Навыки, необходимые для карьеры в области кибербезопасности

Кибербезопасность становится все более важным выбором карьеры. Он может предложить захватывающую и полезную работу с целым рядом различных возможностей для работы. Однако, чтобы добиться успеха, специалисты по кибербезопасности должны обладать сильными техническими навыками, такими как практические знания распространенных языков программирования и систем, обычно используемых в ИТ.

В дополнение к общим языкам программирования — кто-то, кто вступает в сферу кибербезопасности, должен понимать основные принципы кибербезопасности и практиковать эффективные методы предотвращения злонамеренных действий в Интернете.

При правильном сочетании технических знаний и глубокого понимания принципов информационной безопасности профессия, связанная с кибербезопасностью (techlores dot com/кибербезопасность без опыта), может стать невероятно полезной профессией.

У вас есть умение решать проблемы и аналитическое мышление?

Кибербезопасность — захватывающая карьера, требующая навыков решения проблем и аналитического мышления. С ростом риска кибератак эта профессия становится все более важной. Специалисты по кибербезопасности должны уметь быстро и критически мыслить под давлением, чтобы наилучшим образом защищаться от угроз для бизнеса или сети организации.

Они также должны обладать знаниями в области разработки программного обеспечения, программирования и вычислительных систем. Кибербезопасность — это высококонкурентная сфера, которая может быть чрезвычайно полезной для тех, кто обладает нужным набором навыков.

В целом, карьера в области кибербезопасности — отличный выбор для людей, которые обладают отличными навыками общения и решения проблем. Кроме того, сильные коммуникативные навыки необходимы для успешного сотрудничества как с коллегами, так и с клиентами для решения любых проблем безопасности, которые могут возникнуть.

Хотя эта область может быть выгодной, начинающие специалисты по кибербезопасности должны понимать важность продолжения своего образования и быть в курсе текущих тенденций.

Преимущества работы в сфере кибербезопасности

Кибербезопасность — это быстрорастущая область, в которой доступно множество вакансий по всему миру. Поскольку компании все больше зависят от цифровых технологий и хранения данных, кибербезопасность стала важным компонентом защиты их ценной информации и активов.

Эксперты по кибербезопасности должны быть в курсе последних угроз и методов защиты от киберпреступлений и утечек данных. Неудивительно, что с ее быстрым ростом кибербезопасность становится все более популярным вариантом карьеры для тех, кто ищет работу в технологической отрасли.

Все более популярный карьерный путь

Работа в сфере кибербезопасности становится все более популярной карьерой, поскольку она дает возможность оставаться в курсе последних технологий и приобретать ценные отраслевые навыки. Кибербезопасность — это практика защиты цифровых систем, сетей и устройств от вредоносных атак, что делает ее очень востребованной нишей в технологической отрасли.

Профессионалы в этой области должны хорошо разбираться в компьютерных системах и быть готовыми быстро адаптироваться к постоянно меняющимся технологиям.

По мере того, как киберугрозы становятся все более сложными, растет спрос на квалифицированных специалистов по кибербезопасности, что делает эту область выгодным вариантом для тех, кто хочет начать свою карьеру.

Помимо того, что профессия становится все более востребованной, карьера в области кибербезопасности также очень выгодна в финансовом отношении. Специалисты по кибербезопасности обычно зарабатывают больше, чем другие технические специалисты. Поскольку потребность в кибербезопасности продолжает расти, это делает эту профессию одной из самых многообещающих и хорошо оплачиваемых на сегодняшний день.

Карьера и доступные сертификаты

Профессии в области кибербезопасности становятся все более важными в наш цифровой век. С появлением цифровых технологий у карьеры в области кибербезопасности есть множество путей на выбор.

Существуют практические технические роли, такие как компьютерная криминалистика и тестирование на проникновение, на более управленческие должности, такие как директор по информационной безопасности и инженер по кибербезопасности, возможности в этой области огромны.

Специалисты по кибербезопасности должны хорошо разбираться в алгоритмах шифрования, анализе вредоносных программ и управлении рисками. При наличии соответствующей квалификации, опыта и обучения карьера в области кибербезопасности может быть очень выгодной как в финансовом, так и в профессиональном плане.

Сертификаты полезны при приеме на работу в области кибербезопасности

В связи с экспоненциальным ростом утечек данных и других кибератак компании ищут высококвалифицированных специалистов, способных защитить их ИТ-инфраструктуру. Те, кто хочет заниматься кибербезопасностью в качестве карьеры, имеют множество доступных сертификатов. Например, CompTIA Security+, CISSP и CISA, которые могут помочь им углубить свой опыт и подготовиться к более продвинутой работе.

Работодатели также предпочитают тех, кто имеет дополнительную подготовку в области компьютерных наук или смежных областях, так как это повышает ценность чьего-либо профиля при подаче заявления на должность в области технологий.

Таким образом, становится ясно, что кибербезопасность — это отличный и полезный выбор карьеры. Благодаря востребованным навыкам и большему количеству компаний, предлагающих специализированные программы обучения, чтобы быть в курсе новейших технологий. Есть много возможностей для тех, кто заинтересован в работе в области кибербезопасности.

Вопросы, которые следует задать при выборе карьеры в области кибербезопасности

Квалифицированным специалистам поручено защищать безопасность личных и коммерческих данных. Чтобы продолжить карьеру в области кибербезопасности, в зависимости от должности необходимы различные квалификации.

Как минимум, для большинства должностей требуется высшее образование в области компьютерных наук и математики или в другой смежной области, такой как информационные технологии или информационные системы.

Дополнительные квалификации могут включать сертификаты, такие как сертифицированный специалист по безопасности информационных систем (CISSP), сертификаты этического взлома и опыт программирования, среди других специализированных навыков.

В связи с растущим спросом на специалистов по кибербезопасности лица с такой квалификацией могут рассчитывать на выгодную карьеру в этой растущей области.

Знай свою технологию

Работа в области кибербезопасности требует больших технических знаний и опыта.

Те, кто хочет продолжить карьеру в этой области, должны быть знакомы с компьютерным программированием: разработка программного обеспечения, системное администрирование, сети и криминалистика.

Опыт работы в одной или нескольких из этих областей может дать соискателям преимущество при поиске работы. Кроме того, работодатели считают, что сертификаты безопасности очень ценны и могут еще больше повысить перспективы трудоустройства.

В дополнение к специализированным навыкам для успеха в кибербезопасности необходимо развитие прочных и межличностных навыков, таких как решение проблем, общение и критическое мышление.

Однако карьеру в области кибербезопасности можно начать со степени бакалавра в области компьютерных наук, кибербезопасности или информационных технологий.

Также доступны сертификаты для специализации в конкретных областях, от учебных лагерей до спонсируемых государством учебных занятий, и даже для получения ученых степеней, таких как степень магистра и доктора наук; нет недостатка в образовательных возможностях.

Заключение

В заключение, возможности для карьеры в области кибербезопасности огромны и постоянно растут. Поскольку все больше компаний, чем когда-либо, полагаются на технологии, потребность в специалистах по кибербезопасности для защиты своих данных и систем быстро растет…» ***(Mohsin Rasool. Is Cybersecurity a Good Career? // ReadWrite (https://readwrite.com/is-cybersecurity-a-good-career/). 17.01.2023).***

***

«Компания Allied Market Research опубликовала отчет под названием «Рынок оборонной кибербезопасности по типам (решения для защиты конечных точек, решения для сетевой безопасности, решения для защиты Помещения, облако), по решениям (анализ угроз и управление реагированием, управление идентификацией и доступом, управление предотвращением потери данных, управление безопасностью и уязвимостями, унифицированное

управление угрозами, корпоративные риски и соответствие требованиям, управляемая безопасность, другие), по приложениям (военные, общедоступные Коммунальные услуги, коммуникационные сети, прочее): глобальный анализ возможностей и отраслевой прогноз на 2022–2031 годы». Согласно отчету, глобальная индустрия оборонной кибербезопасности заработала 21,3 миллиарда долларов в 2021 году и, по оценкам, достигнет 43,4 миллиарда долларов к 2031 году, что свидетельствует о среднегодовом темпе роста в 7,7% с 2022 по 2031 год. В отчете представлен подробный анализ меняющихся рыночных тенденций, топ сегменты, ключевые инвестиционные карманы, цепочка создания стоимости, региональный ландшафт и конкурентный сценарий…

Судя по заявкам, военный сегмент был крупнейшим рынком в 2021 году, на его долю приходилось более одной трети мирового рынка оборонной кибербезопасности, и ожидается, что он сохранит свой лидирующий статус в течение прогнозируемого периода. Это связано с растущей частотой и изощренностью кибератак из-за растущей зависимости военных организаций от интернет-сети. Чтобы противостоять всем этим уязвимостям, основное внимание уделяется внедрению решений кибербезопасности в оборонном секторе. С другой стороны, в сегменте сетей связи, по прогнозам, будет наблюдаться самый быстрый среднегодовой темп роста в размере 9,0% с 2022 по 2031 год. Это связано с тем, что различные сектора внедряют больше технологий для улучшения своих коммуникаций и инфраструктуры, и параллельно растет киберугроз для этих сетей…

В зависимости от типа сегмент безопасности конечных точек занимал наибольшую долю рынка, составляющую более двух пятых мирового рынка оборонной кибербезопасности в 2021 году, и ожидается, что он сохранит свое доминирующее положение в течение прогнозируемого периода. Это связано с тем, что решения для защиты конечных точек являются одним из важнейших активов оборонного сектора. Высокий уровень проникновения в этот сегмент объясняется растущим использованием автоматизации и поведенческого анализа для обнаружения угроз, растущим объемом данных по вертикалям и растущими инвестициями ключевых игроков. С другой стороны, в сегменте решений для сетевой безопасности прогнозируется самый большой среднегодовой прирост в 8,5% с 2022 по 2031 год. Это связано с увеличением частоты и изощренностью кибератак из-за растущей зависимости военных организаций от Интернета. сеть. Чтобы противостоять всем этим уязвимостям, основное внимание уделяется внедрению решений сетевой безопасности в оборонном секторе…

В зависимости от региона Северная Америка была крупнейшим рынком в 2021 году, захватив почти треть доли мирового рынка оборонной кибербезопасности благодаря увеличению инвестиций в услуги кибербезопасности со стороны многих компаний в регионе. Тем не менее, ожидается, что Азиатско-Тихоокеанский регион будет лидировать по доходам и продемонстрирует самый быстрый среднегодовой темп роста в 9,2% в течение прогнозируемого периода. Это связано с высокими темпами модернизации полиции, увеличением ежегодных бюджетных расходов на внутреннюю безопасность и ростом числа случаев террористической деятельности в регионе…» ***(Defense Cyber Security Market to***

Reach $43.4 Billion, Globally, by 2031 at 7.7% CAGR: Allied Market Research // Cision US Inc. (https://www.prnewswire.com/news-releases/defense-cyber-security-market-to-reach-43-4-billion-globally-by-2031-at-7-7-cagr-allied-market-research-301721155.html). 13.01.2023).

***

«Киберпреступность представляет собой одну из самых больших угроз для современного бизнеса. Наша жизнь все больше интегрируется с цифровыми технологиями, и в результате преступники находят новые и улучшенные способы нападения на нашу личную информацию и наши финансы с помощью угроз кибербезопасности.

Для компаний поддержание надежной и эффективной стратегии кибербезопасности абсолютно необходимо перед лицом растущих угроз. Предприятия должны уметь выявлять угрозы, прежде чем предпринимать шаги для защиты от них. Давайте рассмотрим некоторые из основных угроз кибербезопасности и обсудим, как предприятия могут действовать упреждающе в своих усилиях по самозащите. Читай дальше, чтобы узнать больше.

Каковы основные угрозы кибербезопасности?

Угрозы кибербезопасности проявляются в различных формах, и многие из них могут иметь серьезные последствия для бизнеса. Системы могут быть повреждены, конфиденциальные данные могут быть украдены, а средства и финансы могут стать целью.

Вредоносное ПО, пожалуй, самая распространенная угроза кибербезопасности, с которой мы сталкиваемся сегодня. Сокращенное от вредоносного программного обеспечения, вредоносное ПО — это общий термин для вредоносного программного обеспечения, включая вирусы, программы-шпионы и программы-вымогатели, которые могут заражать компьютеры и распространяться по сетям. Заражение вредоносным ПО может иметь ряд различных последствий, включая блокировку или повреждение сетевых компонентов, потерю данных или дальнейшую установку вредоносного кода.

Атаки на цепочку поставок программного обеспечения — это когда киберпреступники нацелены на программное обеспечение, которое все еще находится в стадии разработки. Тайно устанавливая мошеннический код в программное обеспечение на ранней стадии, эти преступники затем запускают атаки в будущем, когда окончательный продукт доставляется клиентам.

Атаки с использованием социальной инженерии — это когда преступники манипулируют людьми, заставляя их выполнять действия, которые дают преступникам доступ к конфиденциальным системам или выявляют уязвимости. Фишинг включает в себя одну из наиболее распространенных форм атак социальной инженерии. Его можно использовать для кражи данных кредитной карты или паролей.

С таким широким спектром различных угроз кибербезопасности, как компании могут быть активными в своем оборонительном подходе? Давайте узнаем.

Выявление слабых сторон

Первым шагом в управлении уязвимостями является выявление потенциальных слабых мест в системе. Современные цифровые системы и сети часто бывают большими и сложными, состоящими из различных взаимосвязанных частей. Эти системы необходимо регулярно проверять и оценивать на наличие потенциальных недостатков, прежде чем предпринимать шаги по их устранению.

Оцените потенциальные угрозы

После выявления слабых мест их необходимо оценить, чтобы установить, какие из них представляют наибольшую угрозу. Этот шаг имеет решающее значение и может быть использован для начала формулирования плана действий, прежде чем двигаться вперед. Не все слабые места можно исправить сразу, поэтому, оценивая каждое из них и определяя, какие из них представляют наибольшую угрозу, бизнес может в первую очередь устранить наиболее важные из них.

Исправление проблем

Выявив и оценив недостатки системы, предприятия могут предпринять шаги по их устранению. Завершение зависит от характеристик этой конкретной слабости. Это может потребовать использования специальных инструментов или знаний. Некоторые слабые места можно исправить или изменить, чтобы временно уменьшить угрозу, которую они представляют, в то время как другие необходимо устранить немедленно, и может потребоваться капитальный ремонт некоторой или всей системы.

Регистрация действий

Регистрация и отчетность обо всех действиях — фундаментальная часть эффективной стратегии безопасности. Это может дать компаниям ключевое представление о силе и эффективности их общих методов обеспечения безопасности. Кроме того, это может помочь им сделать выводы о том, где они могут ошибаться. Это помогает им снизить риск повторного появления подобных уязвимостей в будущем.

Заключение

Угрозы кибербезопасности являются одной из самых больших угроз, с которыми сегодня сталкивается бизнес. Таким образом, чтобы защитить себя от атак киберпреступников, хакеров и мошенников, предприятия должны внедрить эффективную и комплексную стратегию безопасности. Воспользуйтесь этим руководством, чтобы узнать, как компании могут проявлять инициативу в отношении кибербезопасности». ***(How Can Businesses Be Proactive About Cyber Security Threats? // DevX (https://www.devx.com/security/how-can-businesses-be-proactive-about-cyber-security-threats/). 18.01.2023).***

***

«В 2022 году активность сделок по слияниям и поглощениям (M&A) в области кибербезопасности была сдержанной, причем снижение было более заметным в стоимостном выражении.

По данным аналитической компании GlobalData, общий объем сделок по слиянию и поглощению за год снизился на 14,6%, а стоимость сделки упала на 56,7% по сравнению с 2021 годом.

По данным аналитической компании, в 2022 году в сфере кибербезопасности было заключено в общей сложности 410 глобальных сделок по слияниям и поглощениям, при этом раскрытая стоимость этих сделок составила 48,3 миллиарда долларов.

Общая стоимость сделок по слияниям и поглощениям оставалась выше 100 миллиардов долларов в 2021 году, но в 2022 году этот импульс не сохранился.

«Однако в 2022 году не было объявлено ни о каких сделках на сумму более 10 миллиардов долларов. В результате в 2022 году произошло значительное [по сравнению с прошлым годом] падение общей стоимости сделок», — сказал ведущий аналитик GlobalData Ауроджиоти Бозе.

«Несмотря на то, что общая активность в секторе слияний и поглощений оставалась невысокой, снижение более заметно в стоимостном выражении, чем в объемном, что свидетельствует о том, что инвесторы все более осторожно подходят к крупным инвестициям в условиях нестабильности на рынке».

Стоимость сделок M&A достигла рекордного уровня в 2018 году, составив 126,7 млрд долларов, а 2021 год стал рекордным по объему сделок. В основном это произошло из-за крупных сделок, таких как приобретение McAfee за 14 миллиардов долларов консорциумом и покупка Thoma Bravo Proofpoint за 12,3 миллиарда долларов.

Начиная с 2022 года, Google усилила свою кибербезопасность, купив Mandiant за 5,4 миллиарда долларов США, компанию, ответственную за раскрытие информации об атаке SolarWinds.

В рамках полностью денежной сделки, оцениваемой в 23 доллара США за акцию, 600 консультантов по безопасности Mandiant и более 300 аналитиков присоединились к Google Cloud, поскольку последний стремится «продвинуть свои предложения по безопасности».

В локальном масштабе в течение 2022 года на рынке Новой Зеландии происходили слияния и поглощения между MSSP Advantage, базирующейся в Палмерстон-Норт, и Nspire Technolgies; В течение 2022 года CyberCX осуществила ряд приобретений, включая New Zealand MSSP Cyber Research NZ, Consegna и Tracer Cloud.

В ходе своего первого приобретения в новозеландском регионе за 11 лет Fujitsu приобрела компанию InPhySec, занимающуюся кибербезопасностью, чтобы расширить свои возможности в сфере услуг безопасности и предоставить клиентам Fujitsu в Новой Зеландии доступ к специализированным консультациям по вопросам безопасности и управляемым услугам.

В октябре консалтинговая фирма Deloitte Australia укрепила свои позиции в области кибербезопасности, купив сиднейскую компанию Hacktive, занимающуюся вопросами кибербезопасности.

Компания по предоставлению ИТ-услуг со штаб-квартирой в Сиднее Avocado Consulting приобрела мельбурнского специалиста по безопасности Cyberisk.

В июле публично зарегистрированный поставщик кибербезопасности Cipherpoint приобрел компанию Excite IT, занимающуюся управляемыми ИТ и услугами безопасности, за 3,25 миллиона долларов.

В мае Orro Group приобрела базирующегося в Брисбене поставщика ИТ-услуг RIOT Solutions для дальнейшего развития своих возможностей в области кибербезопасности и цифровых сетей.

Базирующийся в Брисбене поставщик управляемых услуг (MSP) Wyntec купил консалтинговую фирму по кибербезопасности Layer 8 Security за нераскрытую сумму, создав в апреле комплексную компанию по комплексной кибербезопасности и ИТ-услугам.

Чтобы расширить возможности своих приложений, безопасности, данных и искусственного интеллекта (ИИ), Canon Business Services ANZ (CBS) в январе приобрела партнера Microsoft Satalyst». ***(Julia Talevski. Global cyber security M&A activity declined in 2022 // IDG Communications, Inc. (https://www.arnnet.com.au/article/704884/global-cyber-security-ma-activity-declined-in-2022/?fp=2&fpid=1). 20.01.2023).***

***

«План реагирования на киберинциденты — это набор руководств и протоколов, призванных помочь организации обнаруживать, реагировать, сдерживать и управлять любой формой нарушения кибербезопасности. В нем описывается, как лучше защитить организацию от программ-вымогателей, утечек данных и других угроз, а также описываются процедуры быстрого и эффективного реагирования на инциденты для минимизации рисков. План также включает подробную информацию о том, кто должен быть проинформирован в случае киберинцидента. Наконец, в нем содержатся рекомендации по обеспечению текущих мер безопасности после атаки.

В рамках различных требований соответствия организациям необходимо иметь задокументированный план реагирования на киберинциденты. Идея наличия задокументированного плана реагирования состоит в том, чтобы избежать неопределенностей и хаоса во время кибератаки.

К сожалению, многие предприятия пренебрегают обновлением своих планов реагирования на инциденты или их оценкой в реальных ситуациях. Согласно отчету VMware «State of Incident Response 2021», 49 % организаций испытывают нехватку инструментов, персонала и опыта, необходимых для выявления или устранения киберугроз.

Чтобы обеспечить комплексный план реагирования на кибер-инциденты, важно иметь заинтересованные стороны из ИТ и информационной безопасности в дополнение к другим ключевым отделам, таким как юридический, корпоративный коммуникационный, управленческий и HR. Кроме того, следует также включить контакты поставщиков, предоставляющих критически важные услуги, такие как облачная инфраструктура и решения для резервного копирования. Разработка эффективного плана имеет важное значение для любой организации. Чтобы сделать это успешно, каждый отдел должен назначить точку контакта с соответствующей контактной информацией, а также создать матрицу эскалации, в которой указано, кто должен быть уведомлен в случае серьезности инцидента. Кроме того, назначение ролей определенным лицам поможет обеспечить надлежащее время реагирования и разрешения проблем, когда это необходимо.

План также должен содержать подробную информацию о поставщике услуг киберстрахования и регулирующих органах, а также о том, когда их следует сообщить.

Несмотря на создание плана, его эффективность должна быть проверена в случае чрезвычайной ситуации. Такие рамки, как SOC 2 и PCI DSS, требуют, чтобы вы ежегодно тестировали свой протокол реагирования на инциденты. Точная структура вашего плана будет зависеть от особенностей вашего бизнеса, технологической базы и типа данных. В зависимости от того, какая структура управления рисками используется, уровни зрелости системы кибербезопасности и устойчивость к риску; необходимо обновлять или пересматривать этот план каждый семестр или квартал!

Кабинетные учения — наиболее типичный способ оценки плана. В этом процессе все заинтересованные стороны собираются вместе, и гипотетические ситуации взлома исследуются путем обсуждения или даже сценариев, которые приводят к ответным действиям. Как правило, предприятия используют пошаговый подход или функциональное упражнение, в котором каждый шаг выполняется, как указано в плане, за исключением фактических изменений, когда что-то пойдет не так, и т. д.

NIST опубликовал Руководство по программам тестирования, обучения и учений для ИТ-планов и возможностей (Специальная публикация NIST 800-84), чтобы помочь организациям в проектировании, разработке, проведении и оценке мероприятий по тестированию, обучению и тренировке (TT&E) для помощи персонала при подготовке к неблагоприятным ситуациям, связанным с ИТ.

Эффективный план реагирования на инциденты может эффективно свести к минимуму негативные последствия инцидентов безопасности, включая продолжительность и ущерб. Кроме того, это сокращает время восстановления и предотвращает потенциальную негативную огласку и опасения клиентов. Вместо того, чтобы тестировать план во время реального инцидента, когда мало места для ошибок или исправлений, рассмотрите возможность заблаговременного обнаружения недостатков, чтобы эффективно исправить их до того, как возникнет какая-либо проблема; часто привлечение внешнего консультанта, у которого есть непредвзятое мнение, может быть полезным при составлении таких планов.

В постоянно меняющейся среде рисков, вызванной передовыми технологиями, требованиями соответствия и растущими схемами мошенничества, план снижения этих рисков должен регулярно обновляться, чтобы обеспечить его эффективность.

Наиболее распространенный наблюдаемый сценарий — это сбой при восстановлении резервной копии или слишком большое время, затрачиваемое на восстановление резервной копии в случае инцидента. Обычно компании поддерживают резервное копирование критически важных данных, однако компании редко проверяют, можно ли эффективно восстановить резервную копию при необходимости. Такие сбои происходят из-за изменений в программном обеспечении для резервного копирования или доступности оборудования, шифрования из-за атаки программы-вымогателя и т. д. не удается эффективно восстановить.

Другим распространенным сценарием является атака программ-вымогателей или вредоносных программ. В таких случаях обработчик часто не знает, какие первоначальные шаги необходимо предпринять, чтобы сдержать распространение и убедиться, что доказательства сохранены для возможного расследования и анализа первопричин.

Регулярная практика тестирования помогает часто выявлять устаревшие компоненты плана. После каждого теста участники должны провести подведение итогов, чтобы обсудить наблюдения о том, что сработало хорошо, и разделы, которые можно было бы улучшить. Это также должно быть задокументировано как часть Отчета о действиях («PAR»). Эта документация служит поддающимся проверке доказательством того, что учения проводились, а PAR описывает операционные пробелы и планы по их устранению.

Поскольку мы стремимся защитить наши данные и цифровые активы, важно понимать, что нарушения возможны. По этой причине необходим актуальный план реагирования на инциденты — не только для того, чтобы направлять действия сотрудников во время таких событий, но и для того, чтобы он был эффективным. Это включает в себя поддержание программы в рабочем состоянии посредством последовательного тестирования и упражнений». ***(Amit Jaju, Amol Pitale. When Did You Last Test Your Cyber Incident Response Plan? // Ankura Consulting Group, LLC. (https://angle.ankura.com/post/102i4zk/when-did-you-last-test-your-cyber-incident-response-plan). 12.01.2023).***

***

«…ключевые тенденции и прогнозы в области кибербезопасности, которые организации могут ожидать в 2023 году.

1. Мошенничество в социальных сетях порождает новое поле битвы социальной инженерии

Противники и спонсируемые государством злоумышленники используют методы социальной инженерии в качестве первого шага (начальный вектор доступа) в крупномасштабных кампаниях, направленных на взлом систем, распространение программ-вымогателей или кражу конфиденциальной информации. В условиях постоянно растущей торговли в социальных сетях и торговых площадок люди все больше полагаются на показатели доверия, такие как количество связей или подписчиков у человека или учетной записи компании, проверена ли учетная запись и как долго учетная запись была активна, что делает их уязвимыми. к мошенничеству и кибератакам.

Цифры. показывают тревожную тенденцию В 2017 году около 5000 человек были обмануты на 42 миллиона долларов. К 2021 году почти 100 000 человек сообщили о мошенничестве на общую сумму 770 миллионов долларов. Специалисты по безопасности назвали социальную инженерию «самой опасной» угрозой в 2022 году.

2. Катастрофические атаки на критически важную инфраструктуру

Критическая инфраструктура всегда была главной целью киберпреступников и злоумышленников, спонсируемых государством. Учитывая российско-украинскую войну, кибератаки и угрозы выросли в геометрической прогрессии.

почти 90% Считается, что всей критической инфраструктуры США пострадали от успешной атаки программ-вымогателей в 2021 году. И большинство директоров по информационной безопасности (почти 80%) считают, что мир сейчас находится в «постоянном состоянии» кибервойны.

В условиях инфляции и роста стоимости жизни мир может стать свидетелем цифрового гражданского неповиновения в форме хактивизма, когда граждане нападают на собственное правительство или инфраструктуру, чтобы устроить протесты.

3. Дипфейковые атаки становятся более убедительными

Распространение дипфейков (искусственно обработанных аудио, видео и изображений) как инструмента для создания слоя доверия к мошенничеству и атакам социальной инженерии будет расти в геометрической прогрессии. Уровень зрелости технологии дипфейков достаточно убедителен, чтобы обмануть большинство ничего не подозревающих людей.

Относительно новая форма техники атаки, большинство организаций не знают об опасностях, которые представляют дипфейки, и поэтому ничего не делают для обучения сотрудников этому вопросу. Эта ситуация создает огромный риск, который может дорого обойтись им в 2023 году. Согласно последним исследованиям, дипфейк-контент растет более чем на 400% в год, а количество атак с использованием сфабрикованных аудио- и видеоматериалов также растет. Европол сообщил, что технология дипфейков вскоре может стать основным инструментом для киберпреступников.

4. Новые угрозы появляются вместе с Метавселенной

В последнее время метавселенная вызвала много шума, и известные бренды объявили о входе в несколько ведущих виртуальных миров. Хотя эта технология открывает возможности для социального взаимодействия, игр и коммерции, злоумышленники найдут способ взломать личные данные и извлечь или украсть конфиденциальные данные. Если взаимодействие метавселенной записано в блокчейне, вымогатели и киберпреступники могут отследить его, что приведет к очень изощренной и целенаправленной попытке мошенничества. Интерпол считает, что метавселенная проложит новые пути для киберпреступности.

5. Организации переключают свое внимание на создание культуры безопасности

В 2023 году не все будет безоблачно. Недавний опрос ClubCISO показывает, что переход на удаленную и гибридную работу положительно повлиял на отношение сотрудников к безопасности. Исследование показывает, что хорошая культура безопасности стала нормой для организаций, которые постоянно проходят обучение по вопросам безопасности.

Организации осознают, что причины, связанные с людьми, являются причиной 95% нарушений кибербезопасности, подчеркивая важность наличия надежной культуры безопасности. Сильная культура безопасности снижает риск атак и использует сотрудников в качестве последней линии защиты. Большинство (87%) руководителей технологических компаний считают, что сильная культура безопасности так же важна, как и технологический контроль...

Возможно, самый важный шаг, который может сделать любая организация в 2023 году, — это формирование культуры осведомленности и создание основы безопасности…» ***(Stu Sjouwerman. Five Cybersecurity Predictions For 2023 // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/01/24/five-cybersecurity-predictions-for-2023/?sh=6b9329a6df9b). 24.01.2023).***

***

«3 тенденции корпоративной безопасности, на которые следует обратить внимание в 2023 году

Ландшафт кибербезопасности подвижен и постоянно меняется. За последние несколько лет наблюдается значительный рост отраслевых атак, направленных на здравоохранение, цепочки поставок, образование и т. д. Эта тенденция, вероятно, сохранится в следующем году, и отрасли, находящиеся на более слабом уровне цифровой трансформации, становятся легкой мишенью для атаки киберпреступников.

По мере того, как наша планета совершает еще один оборот вокруг Солнца, мы с нетерпением ждем новых вызовов и возможностей 2023 года. Всегда интересно заглянуть в неизвестное и предсказать, что принесет эта новая солнечная орбита.

Но если последние годы нас чему-то и научили, так это тому, что такая задача на самом деле является трудным делом. Я уверен, что ни один из прогнозов, сделанных нами в начале 2020 года, не смог подготовить нас к тому, что грядет в последующие годы. Таким образом, этот ритуал прорицания, который мы практикуем каждый год, направлен не на то, чтобы сосредоточиться на более мелких деталях, а на то, чтобы дать представление об общем направлении, в котором, кажется, движется мир.

Gartner использовала фразу «преодолеть неопределенность» в качестве темы своего стратегического отчета о дорожной карте на ближайшие годы. Это действительно подходящая фраза для определения 2023 года. Рябь, вызванная кипящей геополитической напряженностью, вызванной вопросом России и Украины, назревающими опасениями в области кибербезопасности и надвигающейся на горизонте глобальной рецессией, указывают на ожидающую нас неопределенность.

Из-за этого корпоративная безопасность стала одним из главных приоритетов для бизнеса в наступающем году, поэтому вот взгляд на предстоящие тенденции 2023 года, на которые компаниям следует обратить внимание.

1. Адаптируемая защита и улучшенная видимость для конечных точек

Конечные точки продолжают оставаться главной целью для опытных хакеров. Злоумышленники теперь используют конечные точки в качестве стартовой площадки для проведения более прибыльных атак, таких как программы-вымогатели и компрометация корпоративной электронной почты, а не просто забирают у них конфиденциальные данные. Кроме того, компаниям приходится иметь дело с растущим числом устройств, включая устройства, принадлежащие сотрудникам за пределами корпоративных сетей, и устройства IoT, такие как виртуальные личные помощники, которым требуется доступ к

корпоративным сетям, службам или базам данных. Следовательно, платформы для защиты конечных точек и средства управления конечными точками остаются высокоприоритетными.

Ландшафт кибербезопасности подвижен и постоянно меняется. За последние несколько лет наблюдается значительный рост отраслевых атак, направленных на здравоохранение, цепочки поставок, образование и т. д. Эта тенденция, вероятно, сохранится в следующем году, и отрасли, находящиеся на более слабом уровне цифровой трансформации, становятся легкой мишенью для киберпреступников. - атаки. В такой парадигме решения для обнаружения таких угроз, платформы для защиты корпоративных устройств и управления ими, а также другие предложения SaaS могут обеспечить видимость, защиту и оптимизированную платформу управления для обслуживания множества развернутых конечных точек.

2. Интеграция, сотрудничество и партнерство

Появление облака и последующая миграция к нему позволили организациям установить гибкие границы, чтобы предоставить клиентам более всеобъемлющее решение. Каждый поставщик SaaS движется к этому подходу, чтобы объединить сильные стороны нескольких инструментов и предоставить единую консоль для беспрепятственного управления.

Примером такого сотрудничества является известность и распространение SASE (Secure Access Service Edge). Представленная Gartner в 2019 году, SASE представляет собой концепцию кибербезопасности, которая объединяет несколько решений для сетевого подключения и сетевой безопасности в единую услугу, предоставляемую через облако. По прогнозам, к 2023 году глобальные расходы на SASE вырастут на 8 миллиардов долларов, что является явным свидетельством его важности и ценности.

В 2023 году также появятся решения по безопасности и управлению, интегрирующие искусственный интеллект в свой существующий набор инструментов. В последние годы ИИ стал важным фактором автоматизации в системах безопасности. Например, интеллектуальные системы обнаружения угроз, такие как решения для обнаружения и реагирования на конечных точках, используют ИИ и машинное обучение для обнаружения и реагирования на уязвимости нулевого дня, которые могут нанести вред вашему бизнесу. В наступающем году будет много решений, интегрирующих технологию искусственного интеллекта, чтобы еще больше укрепить свою безопасность.

3. Воспитание культуры безопасности

Развитие и создание культуры осведомленности о рисках кибербезопасности является наиболее важным действием, которое необходимо предпринять в любой фирме. Работодатели и сотрудники больше не могут считать кибербезопасность проблемой, которую должен решать ИТ-отдел. На самом деле описание работы каждого в 2023 году должно включать понимание опасностей и принятие простых мер безопасности!

Многие стратегии ИТ-безопасности следуют реактивному, а не упреждающему подходу, который включает в себя вливание денег для восстановления после атаки и восстановления репутации бренда. Злоумышленники пользуются этим и нацеливаются на слабые звенья, чтобы нанести ущерб.

Фишинговые атаки используют методы «социальной инженерии», чтобы обманом заставить жертв раскрыть конфиденциальные данные или загрузить вредоносное ПО на свои компьютеры.

Любой может научиться распознавать эти нападения и принимать простые меры безопасности, чтобы защитить себя, не нуждаясь в технических знаниях. Точно так же необходимо обучать всех и регулярно обновлять базовые навыки безопасности, такие как безопасное использование пароля и изучение двухфакторной аутентификации (2FA). Если организация хочет обеспечить устойчивость и подготовку в течение следующих 12 месяцев, принятие простых мер безопасности, подобных этим, для продвижения культуры осведомленности о кибербезопасности, должно стать важным аспектом их стратегии безопасности.

Более того, в условиях, когда глобальная экономика предсказывает глобальную рецессию, предприятия любого размера могут ожидать сокращения бюджета в течение года. В такой ситуации обучение ваших сотрудников и обеспечение их четкого понимания методов кибербезопасности может обеспечить надежную защиту, которая может выступать в качестве первой линии защиты, защищая ваш бизнес.

Делая первые шаги в 2023 году, каждое предприятие и отрасль должны подготовиться к новому году и тем вызовам, которые он принесет с собой. В то время как прогнозы и тенденции служат ориентирами, которые помогают нам ориентироваться в предстоящих испытаниях, история цифрового мира показала, что мы всегда должны готовиться к худшему и ожидать неожиданное…» ***(Apu Pavithran. 3 Enterprise Security Trends to Watch Out For in 2023 // Entrepreneur (https://www.entrepreneur.com/leadership/3-enterprise-security-trends-to-watch-out-for-in-2023/441779). 20.01.2023).***

***

Сполучені Штати Америки та Канада

«Криптовалютная биржа заплатит штраф в размере 50 миллионов долларов и инвестирует 50 миллионов долларов в повышение соответствия требованиям AML

В среду Coinbase согласилась на урегулирование с финансовым регулятором Нью-Йорка в размере 100 миллионов долларов в связи с нарушениями кибербезопасности и несоблюдением руководящих принципов по борьбе с отмыванием денег, которые позволяли преступникам использовать платформу для мошенничества, отмывания денег и других незаконных действий.

Криптовалютная биржа заплатит штраф в размере 50 миллионов долларов за нарушение банковского законодательства Нью-Йорка и правил виртуальной валюты, денежных переводов, мониторинга транзакций и кибербезопасности Департамента финансовых услуг штата Нью-Йорк, сообщил Департамент финансовых услуг штата Нью-Йорк. Ожидается, что Coinbase инвестирует дополнительно 50 миллионов долларов для проведения необходимых проверок биографических данных AML и реализации других программ соответствия в

течение следующих двух лет. Сделка также требует, чтобы Coinbase наняла независимого наблюдателя, назначенного DFS, как минимум на год для оценки проблем с соблюдением требований и внесения исправлений.

Мировое соглашение является одним из крупнейших в этой сфере и соответствует аналогичным штрафам, связанным с ПОД, наложенным NYDFS на традиционные банки, такие как Wells Fargo и Deutsche Bank, за последние пять лет, считает Авива Литан, вице-президент Gartner, специализирующийся на развивающихся технологий, рассказывает Информационная безопасность Media Group.

На самом деле урегулирование могло бы быть более существенным, если бы отказы от AML и «Знай своего клиента» действительно были бы такими же небрежными, как утверждает штат Нью-Йорк, говорит Трой Лич, эксперт Конгресса по вопросам безопасности платежей и ключевой архитектор Совета по стандартам PCI.

Неадекватные сдержки и противовесы

По словам государственного финансового регулятора, программа соответствия Coinbase не поспевает за ее ростом на протяжении многих лет, что делает ее уязвимой для потенциальной преступной деятельности.

«Очень важно, чтобы все финансовые учреждения защищали свои системы от злоумышленников, и ожидания департамента в отношении программ защиты потребителей, кибербезопасности и борьбы с отмыванием денег столь же строги для компаний, занимающихся криптовалютой, как и для традиционных финансовых учреждений», — Адриенн. Об этом говорится в заявлении управляющего финансовыми службами А. Харриса.

Поскольку Coinbase работает под лицензией Bitlicense в штате, она обязана соблюдать требования финансового регулятора Нью-Йорка. Агентство обнаружило в ходе проверки и последующего принудительного расследования, что Закон Coinbase о банковской тайне и программа AML, включая ее систему «знай своего клиента», комплексную проверку клиентов, мониторинг транзакций, отчеты о подозрительной деятельности и системы соблюдения санкций, были «неадекватными для поставщика финансовых услуг. размера и сложности Coinbase», — говорится в сообщении агентства.

К концу 2021 года у Coinbase было «неуправляемое» месячное отставание, состоящее из более чем 100 000 непроверенных предупреждений о мониторинге транзакций и более 14 000 клиентов, требующих усиленной комплексной проверки. Но у компании не было ни персонала для решения проблемы, ни ресурсов и инструментов. По словам агентства, требования Coinbase к адаптации клиентов были просто «простой галочкой».

Нерасследованные предупреждения также привели к тому, что Coinbase регулярно не расследовала и не сообщала о подозрительной деятельности, требуемой законом, говорится в сообщении. Bitlicense требует, чтобы лицензиат уведомлял отдел о событии кибербезопасности не позднее, чем через 72 часа после его обнаружения. Но Coinbase сообщила о фишинговой афере, в результате которой 6000 ее клиентов потеряли 1,5 миллиона долларов через пять месяцев после события в 2021 году, хотя она возместила средства клиентам и сотрудничала

с правоохранительными органами, чтобы поймать преступников. Агентство добавляет, что с тех пор Coinbase обновила свои внутренние процедуры, чтобы обеспечить своевременное уведомление об инцидентах.

Криптокомпания также не проверяла клиентов на предмет санкций, разрешала использование виртуальных частных сетей и маршрутизатора Onion, которые потенциально позволяли преступникам скрывать свое местоположение, и не проводила ежегодную оценку рисков.

Свободные проверки биографических данных могут облегчить преступникам создание учетных записей под вымышленными именами для отмывания украденных денег через биржу. По словам Литана, при неадекватном мониторинге транзакций учетные записи клиентов могут быть легко взломаны, а находящиеся на них средства - легче украсть.

«Мы очень откровенно высказывались о проблемах с незаконным финансированием в этой сфере. Именно поэтому наша структура требует от крипто-компаний того же стандарта, что и для банков», — сказал Харрис The New York Times.

Криптовалютная биржа заявила, что с тех пор она решила проблемы, поднятые NYDFS. Пол Гревал, главный юрисконсульт Coinbase, говорит, что расследование агентства было сосредоточено на его программе соблюдения требований в 2018 и 2019 годах и невыполненных работах до 2021 года. «Мы серьезно отнеслись к опасениям NYDFS и приняли существенные меры для устранения этих исторических недостатков», — заявила компания. Он также «регулярно проводит упреждающие расследования, чтобы удалить злоумышленников с нашей платформы и работает с правоохранительными органами, чтобы обеспечить их привлечение к ответственности», — говорится в сообщении в блоге.

По словам Сара Бет Феликс, соучредителя и главного сотрудника по борьбе с отмыванием денег в Acceleron Bank, приказ финансового регулятора касается регистрации предприятий, а также того, как полномочия на совершение транзакций были предоставлены представителю компании, которому не было разрешено совершать сделки от имени бизнеса. По ее словам, это также относится к нескольким банкам. «В целях ОД и мошенничества всегда полезно знать, с кем вы ведете бизнес и кто имеет право совершать транзакции по счету», — сказала она.

Хотя это действие сосредоточено на Coinbase, другие криптовалютные биржи потенциально могут иметь аналогичный недостаток контроля.

«К сожалению, Coinbase приходится нести основную тяжесть надзора, потому что другие биржи имеют гораздо меньше контроля, чем Coinbase», — говорит Литан. «Но они являются лидером по доле рынка и, безусловно, имели свои проблемы. Все биржи, включая Coinbase, должны гораздо лучше защищать средства и счета клиентов, и мы надеемся, что это действие приведет к достижению этой цели».

По словам Литана, из-за отсутствия четких правил кибербезопасности и соблюдения требований в космосе такие агентства, как NYDFS, проложили путь к регулированию пространства, добиваясь улучшений. Исторически, по ее словам,

нормативные акты и соблюдение требований заставляли банки совершенствовать свои меры и операции по борьбе с отмыванием денег и выявлению мошенничества.

Положительным моментом в этом случае является то, что он, вероятно, заставит биржи и других хранителей уделять больше внимания проверке биографических данных и соблюдению требований при создании новых учетных записей клиентов и потенциально сократить отмывание украденных или других незаконных средств, проходящих через этих хранителей, говорит Литан.

По ее словам, урегулирование также потребует больших инвестиций в обеспечение соблюдения нормативных требований и выявления мошенничества, чем сегодня тратит большинство бирж. «Традиционным финансовым компаниям, которые уже вложили значительные средства в соблюдение нормативных требований и обнаружение мошенничества, потребуются лишь дополнительные обновления для управления этими новыми типами функций цифровой валюты», — добавляет она.

Лич говорит, что это урегулирование, вероятно, окажет меньшее влияние на более широкое регулирование криптовалюты, чем банкротство и скандал в FTX, потому что Coinbase решила находиться под дополнительным контролем правительства, будучи публичной компанией. «Крах FTX и потеря миллиардов потребительских средств из-за того, что криптовалютные биржи не соблюдают базовые методы кибербезопасности, вероятно, станут большим катализатором изменений и попыток регулирующего надзора», — говорит он.

Фактически, устранение нарушений Coinbase может улучшить принятие цифровых активов и помочь другим организациям, которые хранят криптовалюты, говорит он. «Мы видели, как акции Coinbase выросли после урегулирования. Вы видите, что руководство Coinbase признает заинтересованность в том, чтобы поступать правильно, и активно сотрудничает с политиками, чтобы создать справедливый путь вперед, который действительно контролирует защиту прав потребителей», — говорит он.

По словам Лича, соблюдение крипто-компаниями тех же стандартов, что и традиционные финансовые организации, поможет убедить пользователей в том, что регулирующие органы гарантируют, что биржи работают на законных основаниях с надлежащим контролем. Одним из недостатков использования одних и тех же нормативных критериев является то, что компании web3 могут столкнуться с теми же централизованными процессами, что и традиционные финансовые компании. «Ожидается, что традиционные финансовые учреждения будут соответствовать десяткам нормативных рамок, часто имея одни и те же средства контроля, подтвержденные независимо десятками различных регулирующих органов. Часть движения за децентрализованное финансирование заключается не в том, чтобы избежать ответственности, а в том, чтобы изменить то, как мы оцениваем добросовестность и должную осмотрительность торговли цифровыми активами», — говорит он». ***(Rashmi Ramesh. AML, Cybersecurity Noncompliance Costs Coinbase $100M // Information Security Media Group, Corp. (https://www.govinfosecurity.com/aml-cybersecurity-noncompliance-costs-coinbase-100m-a-20869). 05.01.2023).***

***

«Группа крупных финансовых регуляторов США во вторник забила тревогу по поводу того, что банковские организации держат в качестве основных криптовалют, назвав цифровые активы в децентрализованных сетях «весьма вероятно, несовместимыми с безопасными и надежными банковскими требованиями».

В совместном заявлении Федеральной резервной системы, Федеральной корпорации по страхованию депозитов и Управления валютного контролера говорится, что регулирующие органы также обеспокоены бизнес-моделями, которые сильно зависят от операций с цифровыми активами или сосредоточены на криптовалютах.

Послание приходит после нестабильного года для криптовалюты, который, по мнению критиков, продемонстрировал, возможно, эндемические недостатки. В прошлом году Terra-Luna, алгоритмический стейблкоин, предположительно привязанный к курсу доллара США, потерпел крах. Криптовалютная торговая платформа FTX, позиционируемая как ворота криптовалюты в мейнстрим, рухнула на фоне обвинений федеральной прокуратуры в том, что она была коррумпирована с самого начала. Эти громкие сбои в сочетании с падением стоимости и сохраняющейся неопределенностью в отношении безопасности децентрализованных финансовых платформ привели криптовалюты к тому, что в отрасли называют «криптозимой».

Меморандум регуляторов может усилить холодность, усилив восприятие криптовалюты как второстепенной инвестиции. Регуляторы написали, что риски криптоактивов, которые «нельзя смягчить или контролировать», не должны мигрировать в банковскую систему.

Бустеры криптовалюты проигнорировали сообщение регуляторов. «Здесь нет ничего нового и ничего полезного, кроме сообщения «держитесь подальше от криптографии». Слишком поздно», — сказал Авива Литан, вице-президент Gartner, специализирующийся на новых технологиях.

Литан сообщил Information Security Media Group, что регулирующие органы ошибочно принимают действия частных компаний за лежащую в их основе технологию. Обвинять открытые децентрализованные сети в схемах Понци «все равно что обвинять дома в финансовом кризисе, обеспеченном ипотечными ценными бумагами», — сказала она.

Недавно регулирующие органы предприняли меры по защите инвесторов с помощью таких шагов, как мартовское распоряжение президента Джо Байдена и рекомендации федерального агентства по пресечению незаконного использования цифровых активов.

В октябре Совет по надзору за финансовой стабильностью США, возглавляемый министром финансов Джанет Йеллен и состоящий из глав всех основных федеральных органов финансового регулирования, единогласно одобрил отчет, в котором делается вывод о том, что деятельность криптовалютных активов представляет риск для стабильности, если торговля будет расти без дополнительных мер регулирования. Он рекомендовал ряд изменений, включая принятие законодательства, предоставляющего федеральным финансовым

регуляторам право устанавливать правила на спотовом рынке криптоактивов, не являющихся ценными бумагами, таких как биткойн.

Совсем недавно сенаторы Элизабет Уоррен, штат Массачусетс, и Роджер Маршалл, штат Канзас, представили Закон о борьбе с отмыванием денег в сфере цифровых активов на слушаниях в Банковском комитете Сената. Законодательство предлагает поставить активы, включая криптовалюту, в один ряд с традиционными финансовыми правилами для устранения рисков национальной безопасности, в том числе кибербезопасности, которые они представляют, сказал Уоррен в то время». ***(Rashmi Ramesh. Regulators Warn Banks of Digital Asset Risks // Information Security Media Group, Corp. (https://www.govinfosecurity.com/regulators-warn-banks-digital-asset-risks-a-20846). 03.01.2023).***

***

«США возглавят Коалицию Freedom Online Coalition, сосредоточившись на продвижении цифровых свобод и обеспечении соблюдения стандартов и мер защиты ИИ.

В течение 2023 года США будут возглавлять Коалицию за свободу в Интернете, группу из 35 правительств, занимающихся продвижением цифровых гражданских свобод, что означает, что США впервые возглавили организацию с момента ее образования в 2011 году.

Государственный департамент США объявил об избрании США на пост председателя еще в июне 2022 года и подтвердил свое официальное вступление в должность в среду. Агентство подтвердило свои приоритетные области на год своего руководства, включая защиту гражданских свобод в Интернете, борьбу с цифровым авторитаризмом, таким как слежка и цензура, и, в частности, обеспечение соблюдения мер безопасности, связанных с искусственным интеллектом.

Предстоящие политики, связанные с искусственным интеллектом, в целом связаны с введением глобальных стандартов использования ИИ.

«Благодаря нашему руководству этой коалицией мы намерены сосредоточиться на… продвижении норм, принципов и гарантий в отношении разработки и использования искусственного интеллекта», — подтвердил Nextgov представитель Госдепартамента.

Согласно Программе действий FOC на 2023 год, ее внимание к ИИ обеспечит соответствие использования технологии правам человека. Организация отмечает, что часть ее целей включает сотрудничество с другими аналогичными группами, а именно с Глобальным партнерством по искусственному интеллекту.

Другие цели включают защиту свобод в Интернете и расширение доступа к цифровым технологиям.

США были одним из основателей FOC вместе с Нидерландами, которые провели первое собрание, и другими странами-членами, включая Канаду, Данию, Эстонию, Финляндию, Францию, Германию, Гану, Швейцарию и Великобританию. С тех пор коалиция добавила еще 24 страны-члена». ***(Alexandra Kelley. U.S. Officially Leads the Freedom Online Coalition for the First Time // Nextgov***

(https://www.nextgov.com/technology-news/2023/01/us-officially-leads-freedom-online-coalition-first-time/382229/). 26.01.2023).

***

«В отчете CISA, который был предусмотрен Законом о кибербезопасности K-12 от 2021 года, изложены различные шаги, которые начальные и средние школы могут предпринять для усиления своей киберзащиты.

Во вторник Агентство по кибербезопасности и безопасности инфраструктуры опубликовало отчет, в котором излагаются различные шаги, которые должны предпринять школы и округа K-12 для улучшения своей практики кибербезопасности на фоне роста числа атак программ-вымогателей и других цифровых угроз, нацеленных на начальные и средние учебные заведения по всей стране.

В отчете предложены три добровольных рекомендации, которые помогут школам укрепить свою киберзащиту, в том числе инвестировать в наиболее эффективные меры безопасности и разработать «зрелый план кибербезопасности», выявляя и устраняя нехватку ресурсов и уделяя особое внимание «сотрудничеству и обмену информацией».

В отчете CISA выделены отдельные шаги, которые школы могут предпринять для выполнения этих рекомендаций, такие как внедрение многофакторной аутентификации для защиты учетных записей и данных в Интернете, разработка плана реагирования на киберинциденты и работа над получением финансирования от Государственной и местной программы грантов в области кибербезопасности и других подобных программ., чтобы улучшить свои методы кибербезопасности.

«Поскольку учебные заведения K-12 используют технологии, чтобы сделать образование более доступным и эффективным, злоумышленники в киберпространстве усердно работают, пытаясь использовать уязвимости в этих системах, угрожая способности нашей страны обучать наших детей», — говорится в заявлении директора CISA Джен Истерли. «Сегодняшний отчет служит первым шагом на пути к более сильному и безопасному кибер-будущему для школ нашей страны с упором на простые, приоритетные действия, которые школы могут предпринять для заметного снижения кибер-рисков».

В 2022 году не менее 45 школьных округов США подверглись атакам программ-вымогателей, включая атаку программ-вымогателей на Объединенный школьный округ Лос-Анджелеса прошлой осенью, в результате которой хакеры утекли 500 ГБ украденных данных. В то время как CISA заявила, что общее количество киберинцидентов, затрагивающих школы K-12, «невозможно надежно определить количественно из-за отсутствия консолидированных данных», оно добавило, что «зарегистрированные инциденты в период с 2018 по 2021 год выросли с 400 в 2018 году до общего количества инцидентов». более 1300» в 2021 году.

Рост числа кибератак, направленных против школ и округов, подчеркнул нехватку ресурсов, которыми в настоящее время располагают школьные администраторы и преподаватели для смягчения угроз. CISA, которое отметило,

что оно «организовало и содействовало проведению серии круглых столов для прослушивания и получения отзывов с ключевыми группами заинтересованных сторон» для сбора информации для отчета, заявило, что педагоги и школьный персонал выразили агентству особую озабоченность по поводу нехватки кадров и финансирования, необходимых для адекватно решать проблемы, связанные с кибербезопасностью.

Участники слушаний подчеркнули «крайнее неравенство в наличии талантов и финансировании», когда речь идет об управлении киберрисками, а также тот факт, что «в большинстве округов нет штатных сотрудников по кибербезопасности, а в некоторых небольших школьных округах может даже не быть нанять штатный ИТ-персонал». В тех случаях, когда школа или школьный округ нанимали специалиста по кибербезопасности, заинтересованные стороны отмечали, что эти сотрудники часто «не имеют актуальной подготовки или опыта, отчасти из-за ограниченных ресурсов для профессионального развития».

«Мы узнали, что сектор больше всего нуждается в ресурсах, простоте и расстановке приоритетов», — говорится в сообщении CISA. «Соответственно, этот отчет стремится прорваться сквозь шум и предложить четкие шаги, которые имеют приоритет, чтобы помочь организациям K-12 в первую очередь внедрить наиболее эффективные средства контроля кибербезопасности».

Отчет CISA был предусмотрен Законом о кибербезопасности K-12, который требовал от агентства «изучения рисков кибербезопасности, с которыми сталкиваются начальные и средние школы, и разработки рекомендаций, включающих руководящие принципы кибербезопасности, призванные помочь школам справиться с этими рисками». Закон, внесенный сенаторами Гэри Питерсом, штат Мичиган, и Риком Скоттом, штат Флорида, был подписан президентом Джо Байденом в октябре 2021 года.

В своем заявлении Петерс назвал отчет «важным шагом к тому, чтобы помочь школам K-12 по всей стране защитить себя от кибератак, которые подвергают риску личную информацию учащихся и сотрудников».

«Школы K-12 все чаще становятся мишенью для хакеров-преступников, и этот новый ресурс от CISA делает понятные руководства по рискам кибербезопасности доступными для школ, которые в них больше всего нуждаются», — добавил он.

CISA также выпустила онлайн-инструментарий, который расширяет рекомендации отчета, чтобы помочь школам K-12 и школьным округам управлять киберрисками и снижать их, включая ссылки на бесплатные ресурсы, связанные с кибербезопасностью, и тренинги для специалистов в области образования.

CISA назвала отчет «отправной точкой» и заявила, что продолжит «сотрудничать с образовательным сообществом K-12 и работать с поставщиками технологий, чтобы поощрять предоставление бесплатных или недорогих инструментов и продуктов безопасности, которые являются безопасными по умолчанию». ***(Edward Graham. CISA Releases Guide to Help Safeguard K-12 Schools from Cyber Threats // Nextgov (https://www.nextgov.com/cybersecurity/2023/01/cisa-releases-guide-help-safeguard-k-12-schools-cyber-threats/382149/). 24.01.2023).***

***

«NOAA рассчитывает на поддержку отрасли, чтобы активизировать свои усилия в области кибербезопасности

Агентство ищет подрядчика для обеспечения круглосуточной поддержки для обнаружения и мониторинга угроз кибербезопасности.

Согласно запросу информации, отдел кибербезопасности Национального управления океанических и атмосферных исследований (NOAA) ищет помощь в поддержке миссии агентства по кибербезопасности.

В заявлении, поданном в пятницу, отмечается, что миссия направлена на «защиту и защиту использования киберпространства от кибератак, а также на защиту информации и информационных систем NOAA от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения».

Согласно заявке, Центр кибербезопасности NOAA — или NCSC — будет иметь возможность предоставлять центр операций по обеспечению безопасности как услугу для своих партнеров — DOC и его бюро — и что NCSC также отвечает за операции по обеспечению безопасности предприятия Министерства торговли. Center — или ESOC — и связанные с ним технические требования. Кроме того, согласно запросу информации, NCSC предоставит NOAA и его партнерам «комплексные услуги по кибербезопасности… в качестве общей услуги».

В частности, как отмечается в заявке, NCSC и ESOC предоставят несколько предложений поддержки, а именно: Операционный центр безопасности NOAA, поддержку инфраструктуры, услуги корпоративной кибербезопасности, сам Центр управления корпоративной безопасностью Министерства торговли и инженерные услуги ESOC Министерства торговли.

NOAA ищет подрядчика, который может предоставить следующее: способность обнаруживать потенциальные угрозы кибербезопасности и реагировать на них круглосуточно и без выходных, отслеживая события, выполняя анализ безопасности и используя корреляцию событий. Это может быть выполнено с помощью информации о безопасности и управления событиями, а также с помощью платформы управления безопасностью, автоматизации и реагирования, а также каналов аналитики ИТ-безопасности для NOAA SOC и ESOC.

Кроме того, NOAA ищет круглосуточную поддержку для корпоративных услуг кибербезопасности NCSC, включая межведомственное доверенное подключение к Интернету, инструменты непрерывной диагностики и смягчения последствий, а также поддержку ИТ-операций для NCSC. Наконец, как отмечается в заявке, NOAA просит подрядчика предоставить ESOC Министерства торговли инженерные услуги для интеграции данных и сервисов.

NOAA изложило спецификации и требования к основному подрядчику, такие как предыдущие работы в аналогичной области.

Первоначально NOAA подала уведомление 12 января, но обновила его 20 января, чтобы отразить другой код Североамериканской системы отраслевой классификации или NAICS, который используется для классификации предприятий. Агентство отметило, что в настоящее время оно ищет источники только для информации и целей планирования, оно не обязуется подавать запрос…» ***(Kirsten Errick. NOAA Looks to Industry Support to Boost its Cybersecurity***

Efforts // Nextov (https://www.nextgov.com/cybersecurity/2023/01/noaa-looks-industry-support-boost-its-cybersecurity-efforts/382083/). 23.01.2023).

***

«Во вторник Microsoft представила более безопасные возможности для своих государственных заказчиков с помощью облака Microsoft Office 365 Government Secret, которое, согласно заявлению компании, теперь общедоступно для оборонных, разведывательных и других государственных заказчиков.

«Этот релиз — серьезное обязательство предоставить самые передовые, безопасные и совместимые инструменты для повышения производительности и совместной работы, которые помогут защитить секретные данные», — сказал Пол Лоример, корпоративный вице-президент Office 365 для предприятий и облачных технологий, в своем блоге. «Мы готовы помочь федеральным гражданам США, Министерству обороны, разведывательному сообществу и партнерам из правительства США, работающим в сфере секретности, с нашим передовым программным обеспечением как услугой».

Согласно сообщению в блоге, Office 365 Secret будет включать в себя первый выпуск возможностей для Exchange, Outlook и других приложений Microsoft 365 на уровне секретной классификации.

Объявление Microsoft было сделано после того, как она стала одним из нескольких лауреатов контракта Министерства обороны США на 9 миллиардов долларов США по совместному ведению боевых действий в облаке (или JWCC), в котором также участвовали Amazon Web Services, Google и Oracle. Контракт, о котором было объявлено в декабре, поможет Пентагону внедрить возможности облачных вычислений в министерство обороны. Каждая компания будет соревноваться за выполнение отдельных задач по контракту.

Хотя у Microsoft есть секретная и сверхсекретная аккредитация для своего облака Azure, добавление Office 365 Secret означает, что Microsoft предлагает инструменты повышения производительности на уровне воздействия 6, который зарезервирован для секретных данных. Microsoft заявила, что эта новая среда позволяет агентствам «использовать весь облачный опыт, чтобы не только создать инфраструктурную платформу для сбора, обработки и операционализации данных, но и обеспечить облачную совместную работу и общение в секретной среде». ***(Kirsten Errick. Microsoft Office 365 Now Available to Customers at Secret Classification // Nextov (https://www.nextgov.com/cxo-briefing/2023/01/microsoft-office-365-now-available-customers-secret-classification/382175/). 25.01.2023).***

***

«В среду Национальное управление архивов и документации (NARA) опубликует обновление правительственных правил хранения документации, устанавливающее новые требования о том, как долго федеральные агентства должны хранить журналы кибербезопасности и другие сетевые данные.

Общее расписание записей, или GRS, устанавливает типы записей, которые агентства должны хранить, и срок, прежде чем они могут быть удалены или иным образом уничтожены, что известно как инструкции по утилизации.

Новые инструкции по размещению в Transmittal 33, которые должны быть опубликованы в среду на веб-сайте NARA и в Федеральном реестре, включают требования к хранению двух типов записей журнала кибербезопасности: полные данные захвата пакетов, которые должны храниться не менее 72 часов, и события кибербезопасности. журналы, которые должны храниться до 30 месяцев. Оба типа записей могут храниться дольше, согласно NARA, как «разрешенные для использования в бизнесе».

Новые правила являются первым обновлением раздела GRS о записях безопасности информационных систем с момента его создания в 2014 году.

Данные захвата пакетов, также известные как PCAP, представляют собой краткое изложение всех пакетов данных, которые перемещаются по сети. Эти данные имеют решающее значение для проведения судебной экспертизы кибербезопасности, поскольку они регистрируют историю всех перемещений данных между всеми подключенными устройствами в сети.

Журналы событий кибербезопасности еще более детализированы, поскольку они используются для записи всех данных и действий, предпринятых для «обнаружения, расследования и устранения киберугроз», говорится в сопроводительном документе.

Оба отчета были первоначально упомянуты в широкомасштабном указе о кибербезопасности от мая 2021 года. ЭО было продолжено в меморандуме от августа 2021 года, в котором агентствам предписывалось работать с Агентством кибербезопасности и безопасности инфраструктуры и ФБР после инцидента, связанного с безопасностью, включая обмен ключевыми журналами безопасности.

В новом соглашении NARA уточняется, как долго эти записи должны храниться, и систематизируются правила хранения.

В обновлении отмечается, что обе записи «не являются медиа-нейтральными», и правило применяется только к электронным версиям этих записей. В передаче также было ясно, что политика хранения охватывает только журналы, а не базовые данные, которые регистрируются.

«Этот график охватывает записи, созданные и поддерживаемые федеральными агентствами, связанные с защитой безопасности систем и данных информационных технологий и реагированием на инциденты компьютерной безопасности», — говорится в документе. «Это расписание не распространяется на системные данные или контент». ***(Aaron Boyd. NARA to Publish First Update to Cybersecurity Records Rules Since 2014 // Nextgov (https://www.nextgov.com/cybersecurity/2023/01/nara-publish-first-update-cybersecurity-records-rules-2014/381662/). 10.01.2023).***

***

«…Согласно отчету, подготовленному Управлением генерального инспектора внутренних дел, который был опубликован в пятницу, слабые методы кибербезопасности Департамента внутренних дел, в том числе

использование сотрудниками легко взламываемых паролей и непоследовательное развертывание многофакторной идентификации, делают агентство уязвимым для фишинговых атак и взломов.

В отчете OIG говорится, что в ходе расследования ему удалось взломать 18 174 из 85 944 паролей активных пользователей, или 21%, «включая 288 учетных записей с повышенными привилегиями и 362 учетных записи высокопоставленных государственных служащих США». В отчете добавлено, что инспекторы смогли взломать 16% учетных записей пользователей Interior «за первые 90 минут тестирования».

OIG заявила, что это произошло из-за «устаревших и неэффективных» требований Министерства внутренних дел к сложности паролей, которые позволяли пользователям выбирать пароли, которые легко взломать, и «позволяли постороннему персоналу использовать одни и те же изначально слабые пароли».

«Например, наиболее часто повторно используемый пароль (Password-1234) использовался для 478 уникальных активных учетных записей», — отмечается в отчете. «На самом деле, пять из 10 наиболее часто используемых паролей в отделе включали вариант «пароль» в сочетании с «1234»; эта комбинация в настоящее время соответствует требованиям департамента, хотя взломать ее несложно».

В отчете говорится, что Министерство внутренних дел «не смогло обеспечить соблюдение собственных политик управления учетными записями в отношении отключения учетных записей и смены паролей», что, как отмечается, имело решающее значение для усилий агентства по обеспечению кибербезопасности, поскольку «неиспользуемые учетные записи представляют более высокий риск для систем и сетей отдела, поскольку они предлагают больше возможностей». чтобы злоумышленник мог получить несанкционированный доступ». Хотя политика Министерства внутренних дел требует, чтобы неактивные учетные записи были отключены через 45 дней, в отчете говорится, что «6 243 из всех активных учетных записей не использовались более 45 дней».

«Департамент не смог отключить эти учетные записи в соответствии со своей собственной политикой и вместо этого оставил реализацию и обеспечение соблюдения этой политики бюро и офисам», — говорится в отчете, добавляя, что рецензенты OIG «взломали 23% (1405) этих учетных записей».

OIG также обнаружила, что министерство внутренних дел не в полной мере использовало многофакторную аутентификацию во всем отделе, «в том числе для 89% своих ценных активов (активы, которые могут серьезно повлиять на способность отдела вести бизнес в случае компрометации), что сделало эти системы уязвимыми для паролей. компрометирующие атаки». В отчете добавлено, что многофакторная аутентификация «является высокоэффективным методом защиты учетных записей», даже если пароль скомпрометирован, поскольку она обеспечивает дополнительный уровень безопасности, прежде чем пользователи смогут получить доступ к внутренним приложениям.

OIG сослался на атаку программы-вымогателя Colonial Pipeline в мае 2021 года как «пример потенциальных последствий отсутствия многофакторной аутентификации и слабых методов управления учетными записями», а также

признал, что аналогичное нарушение во внутренних делах «не приведет к таким же широкомасштабным нарушениям работы предприятий и потребителей».

В отчете OIG предложено восемь рекомендаций, которые помогут усилить практику управления учетными записями пользователей, в том числе внедрение многофакторной аутентификации, «которую нельзя обойти, чтобы разрешить однофакторную аутентификацию для всех приложений», пересмотр «политики сложности пароля и управления учетными записями» и запрет на использование связанных учетных записей. одинаковые пароли.

Министерство внутренних дел согласилось со всеми восемью рекомендациями OIG, хотя министерство отказалось от содержащихся в отчете ссылок на атаку Colonial Pipeline в контексте своих методов кибербезопасности, отметив, что оно «имеет ключевые меры безопасности, которые снижают риск использования аналогичных методов из-за позицию глубокоэшелонированной защиты». ***(Edward Graham. Interior's Cyber Practices Allow for Easily Crackable Passwords, Watchdog Finds // Nextgov (https://www.nextgov.com/cybersecurity/2023/01/interiors-cyber-practices-allow-easily-crackable-passwords-watchdog-finds/381620/). 10.01.2023).***

***

«Предлагаемое Федеральной комиссией по связи (FCC) правило требует, чтобы поставщики телекоммуникационных услуг немедленно уведомляли потребителей и федеральные агентства о любых нарушениях, связанных с «собственной сетевой информацией клиента».

Федеральная комиссия по связи в пятницу предложила новое правило, согласно которому поставщики телекоммуникационных услуг должны немедленно уведомлять потребителей и федеральные правоохранительные органы о любых нарушениях конфиденциальных данных.

В соответствии с предложенным правилом FCC, агентство отменит «текущий семидневный обязательный период ожидания для уведомления клиентов о взломе» и потребует, чтобы обо всех выявленных нарушениях данных сообщалось потребителям, а также FCC, ФБР и секретной службе как можно скорее. они идентифицируются, если иное не указано федеральными должностными лицами.

Кроме того, это предложение расширит определение нарушения данных, данное Федеральной комиссией по связи, «включив в него непреднамеренный доступ, использование или раскрытие информации о клиентах», а не просто ограничит его случаями, когда внешний субъект получил несанкционированный доступ к конфиденциальной информации, как в случае с действующее правило агентства.

Текущее правило сообщения об утечке данных FCC, которое агентство приняло в 2007 году, требует, чтобы провайдеры с более чем 5000 клиентов уведомляли правоохранительные органы о нарушениях, связанных с «собственной сетевой информацией клиента», в течение семи дней, в то время как нарушения затрагивают поставщиков с менее чем 5000 клиентов. 5000 клиентов должны быть зарегистрированы в течение 30 дней.

«Закон требует от операторов защищать конфиденциальную информацию о потребителях, но, учитывая увеличение частоты, сложности и масштабов утечек данных, мы должны обновить наши правила, чтобы защитить потребителей и ужесточить требования к отчетности», — заявила председатель FCC Джессика Розенворсел. «Этот новый процесс позволит по-новому взглянуть на наши правила отчетности об утечках данных, чтобы лучше защитить потребителей, повысить безопасность и уменьшить влияние будущих нарушений».

Rosenworcel ранее распространил предложение об усилении требований к отчетности об утечках данных в январе 2022 года.

В последние годы участились случаи утечек данных в федеральном правительстве и частном секторе, причем операторы связи, в частности, сталкивались с громкими утечками конфиденциальной информации о пользователях за последнее десятилетие. В августе 2021 года T-Mobile сообщила об утечке данных, которая затронула примерно 50 миллионов ее клиентов. FCC также оштрафовала AT&T на 25 миллионов долларов в 2015 году за расследование утечки данных в трех колл-центрах телекоммуникационного гиганта в период с 2012 по 2014 год, в результате которой пострадали сотни тысяч клиентов.

В пресс-релизе FCC говорится, что предложенное правило, которое было принято комиссией 4–0 голосами, было частью усилий по лучшему согласованию правил агентства «с недавними изменениями в федеральных законах и законах штатов о нарушении данных, охватывающих другие сектора». Все 50 штатов внедрили законы о раскрытии информации об утечке данных для частных лиц, при этом ряд этих требований был реализован с тех пор, как в 2007 году были приняты текущие правила Федеральной комиссии по связи США об утечке данных.

У общественности будет 30 дней, чтобы представить комментарии к уведомлению о предлагаемом нормотворчестве после его публикации в Федеральном реестре, и 60 дней, чтобы представить ответные комментарии». ***(Edward Graham. FCC Rule Would Require Telecom Providers to Immediately Disclose Sensitive Data Breaches // Nextgov (https://www.nextgov.com/cybersecurity/2023/01/fcc-rule-would-require-telecom-providers-immediately-disclose-sensitive-data-breaches/381597/). 09.01.2023).***

***

«…В четверг компания Clever из Сан-Франциско опубликовала отчет Cybersecure 2023, основанный на опросах, проведенных в октябре 2022 года среди более чем 800 администраторов и более 3000 учителей в США. что школы нуждаются в более качественном обучении, технологиях и персонале для поддержки усилий по кибербезопасности, согласно пресс-релизу Clever, опубликованному в четверг.

Дэн Кэрролл стал одним из основателей Clever более десяти лет назад и является директором по продуктам компании. Он сказал, что с момента запуска Clever единственное, что, по словам ИТ-администраторов, не дает им спать по ночам, — это конфиденциальность и безопасность. Но в последние годы, с ростом количества программ-вымогателей и хакеров — ярким примером этого является недавний взлом Объединенного школьного округа Лос-Анджелеса — забота о

безопасности выходит за рамки ИТ-руководителей, сказал он. Это признание в сочетании с прошлогодним отчетом компании, показывающим, что 90 процентов учителей продолжают использовать цифровые инструменты после пандемии в своих классах, побудили компанию провести опрос.

«Тот факт, что это действительно становится проблемой всей экосистемы — вы знаете, то, что сейчас сказали бы суперинтенданты, — это то, что не дает им спать по ночам, — заставил нас задуматься о том, чтобы по-настоящему погрузиться и получить широкое представление об экосистеме и понять, как люди думают об этих проблемах сегодня», — сказал Кэрролл в интервью Government Technology.

Опрос показал, что учителя и администраторы по-разному относятся к вероятности кибератаки на территории их школы. Менее половины опрошенных учителей сказали, что утечка в их школе вероятна, в то время как две трети администраторов считают, что это вполне вероятно. Двадцать пять процентов респондентов-администраторов заявили, что их округ уже становился жертвой той или иной формы взлома, фишинга, утечки данных или других кибер-инцидентов в течение года, предшествовавшего опросу.

Когда дело доходит до безопасности, учителя и администраторы в равной степени (34%) считают, что устройства могут быть лучшей возможностью для хакеров проникнуть в систему и взломать систему. Но когда вопрос перешел к риску безопасности человека, было много обвинений, сказал Кэрролл.

«Когда вы спрашиваете учителей: «Где самый большой человеческий риск?» они думали, что это студенты, но если спросить администраторов, они подумали, что это учителя», — сказал Кэрролл. «Я думаю, что это просто отличный пример того, что мы все видим разных людей и наблюдаем некоторые небезопасные методы использования паролей или небезопасные технические методы».

Согласно отчету, две трети учителей считают, что студенты являются источником уязвимости людей в отношении кибербезопасности, тогда как 19 процентов администраторов считают, что так считают. Впоследствии 66 процентов администраторов считали учителей уязвимым местом, а 27 процентов учителей смотрели на себя в зеркало как на проблему. Вряд ли какая-либо забота была дарована административному персоналу.

Аналогичные тенденции были выявлены в отношении уязвимости человека в отношении конфиденциальности данных. Но Кэрролл сказал, что это беспокойство выходит за рамки какой-либо отдельной группы.

«Администраторы, преподаватели и студенты — все они были своего рода переносчиками, которые несут ответственность за нарушения в разных местах, — сказал он. — И это просто указывает на необходимость действительно всеобъемлющей программы обучения и образования».

В отчете говорится, что, несмотря на опасения по поводу взлома, 63 процента администраторов и более половины опрошенных учителей заявили, что они согласны или полностью согласны с тем, что их округ имеет ресурсы для надлежащей подготовки или решения проблем цифровой безопасности. Иметь ресурсы — это одна часть, а использовать их с пользой — другая…

Около четверти опрошенных учителей заявили, что не проходили никакой подготовки по вопросам конфиденциальности или безопасности. Двенадцать процентов администраторов заявили, что они также не прошли обучение. На вопрос, что было бы полезно для повышения цифровой безопасности в их округе, 34 процента учителей ответили, что это преданный своему делу персонал, а 31 процент сказали, что больше или лучше обучение. Администраторы в основном считали, что обучение поможет (39%), лучшими техническими решениями являются следующие лучшие варианты (24%), за ними следует специальный персонал (19%). 18% респондентов-педагогов признали, что более совершенные технологии улучшат безопасность.

Чтобы улучшить ситуацию, округам, вероятно, потребуется увеличить расходы. Почти две трети администраторов заявили, что их расходы увеличатся в ближайшие несколько лет; 12 процентов заявили, что расходы значительно увеличатся. По его словам, более половины администраторов заявили, что федеральное финансирование стимулов поможет этим усилиям. Кэрролл советует тщательно обучить всех в округе, приобрести современные инструменты и нанять квалифицированный персонал, который сможет создать автоматизированную систему с несколькими уровнями защиты…» ***(Giovanni Albanese. Report: 25% of Districts Victimized by Cyber Attacks in 2022 // e.Republic LLC (https://www.govtech.com/education/k-12/report-25-of-districts-victimized-by-cyber-attacks-in-2022). 05.01.2023).***

***

«В 2022 году Канадская комиссия по радио, телевидению и телекоммуникациям продолжала обеспечивать соблюдение канадского законодательства о борьбе со спамом (широко известного как «CASL»).

CASL устанавливает всеобъемлющий режим правонарушений, механизмов правоприменения и потенциально суровых наказаний, предназначенных для запрета отправки нежелательных коммерческих электронных сообщений (CEM), несанкционированной коммерческой установки и использования компьютерных программ в компьютерной системе другого лица и других форм онлайн-мошенничества. Ниже приведены некоторые ключевые аспекты CASL:

CASL создает режим отказа, который запрещает, с некоторыми исключениями, отправку CEM, если только получатель не дал согласия (прямого или подразумеваемого в определенных обстоятельствах) на получение CEM, и CEM не соответствует предписанным формальностям (например, информация о отправителя и эффективный и оперативно реализованный механизм отказа от подписки).

CASL также запрещает, за некоторыми исключениями, установку и использование компьютерной программы в компьютерной системе другого лица в ходе коммерческой деятельности без явного согласия владельца или авторизованного пользователя компьютерной системы.

CASL возлагает ответственность на организации и отдельных лиц (включая корпоративных директоров и должностных лиц) за прямые и косвенные/косвенные нарушения CASL. CASL обеспечивает должную осмотрительность защиты.

Нарушения CASL могут привести к нормативным штрафам в размере до 10 миллионов долларов США за нарушение для организации и 1 миллион долларов США за нарушение для физического лица. CASL включает частное право на иск, которое не имеет силы.

Канадская комиссия по радио, телевидению и телекоммуникациям (CRTC) обеспечивает соблюдение правил CASL в отношении CEM и компьютерных программ. С момента вступления в силу CASL в 2014 году CRTC принял меры в отношении организаций и физических лиц, нарушивших CASL, и принял исполнительные решения и принял добровольные обязательства (расчеты).

правоприменение CRTC

В январе 2022 года CRTC опубликовала соглашение об урегулировании принудительных мер CRTC в отношении лица, предположительно проводившего массовые спам-кампании без согласия в нарушение правил CASL CEM. Обязательство требовало от физического лица уплаты административного денежного штрафа в размере 7500 долларов вместо штрафа в размере 75000 долларов, наложенного сотрудниками CRTC в уведомлении о нарушении от марта 2021 года.

В январе 2022 года CRTC объявил о штрафах на общую сумму 300 000 долларов США четырем канадцам за их участие в рынке Dark Web, известном как «Canadian HeadQuarters», который был отключен после того, как сотрудники CRTC выполнили ордера. Четыре человека якобы отправили мошеннические электронные письма, имитирующие известные бренды, чтобы получить конфиденциальную личную информацию.

В мае 2022 года CRTC выпустила Решение о соответствии и правоприменении CRTC 2022-132, отменяющее уведомления о нарушении, выданные в 2018 году сотрудниками CRTC в отношении двух компаний за якобы содействие распространению вредоносной рекламы в нарушение правил CASL по установке компьютерного программного обеспечения на другой компьютер. компьютерная система человека. CRTC обнаружил, что имеющиеся доказательства, состоящие из косвенных доказательств, а не данных с жесткого диска рассматриваемых компьютерных систем, не доказывают с точки зрения вероятности того, что вредоносная реклама была успешно установлена на компьютерных системах. В результате компании не были обязаны платить административные денежные штрафы, указанные в уведомлениях о нарушении…» ***(Bradley Freedman. Canada's Anti-Spam Legislation – 2022 Year in Review // Borden Ladner Gervais LLP ("BLG") (https://www.blg.com/en/insights/2023/01/canadas-anti-spam-legislation-2022-year-in-review). 05.01.2023).***

***

«Агентство национальной безопасности (АНБ) переименовало Дейтонский государственный колледж в Национальный центр академического мастерства в области киберзащиты до 2028 года.

Штат Дейтона предлагает расширенный технический сертификат в области кибербезопасности и киберкриминалистики, а также степень бакалавра наук в

области информационных технологий, которые вместе составляют основу программы обучения DSC, одобренной АНБ.

«Кибербезопасность — это высокотехнологичная и постоянно развивающаяся область, — сказал Данте Леон, заместитель вице-президента Daytona State. «Это переименование является свидетельством приверженности наших преподавателей и сотрудников подготовке студентов с навыками, необходимыми им для успешной работы в промышленности, правительстве и за ее пределами».

Центр академического мастерства в области киберзащиты в Дейтонском государственном колледже был создан в 2013 году благодаря гранту программы передового технологического образования Национального научного фонда. С момента своего основания центр, расположенный в Колледже передовых технологий DSC, сосредоточился на обучении в важнейших областях кибербезопасности и киберкриминалистики. В 2016 году Агентство национальной безопасности / Центральная служба безопасности присвоило центру статус Национального центра академического превосходства в области киберзащиты (CAE-CD).

«Способность [DSC] соответствовать растущим требованиям программных критериев сослужит хорошую службу стране, способствуя защите национальной информационной инфраструктуры», — сказала д-р Карен Леушнер, руководитель программы Национального центра академического превосходства АНБ.

«Наша миссия в штате Дейтона — предвидеть потребности в образовании и рабочей силе граждан и предприятий округов Волусия и Флаглер, — сказала д-р Эми Локлир, исполнительный вице-президент и проректор штата Дейтона. «Наши программы кибербезопасности и киберкриминалистики являются ключевым элементом нашей долгосрочной стратегии, направленной на удовлетворение постоянно меняющихся потребностей нашего региона». ***(National Security Agency Redesignates DSC's Academic Excellence in Cyber Defense // FlaglerLive (https://flaglerlive.com/185303/national-security-agency-redesignates-dscs-academic-excellence-in-cyber-defense/). 17.01.2023).***

***

«Офис генерального инспектора (OIG) в НАСА заявляет, что практика управления программными активами агентства по аэронавтике и космонавтике в настоящее время подвергает его операционным, финансовым рискам и рискам кибербезопасности, поскольку управление жизненным циклом программного обеспечения в значительной степени децентрализовано и ситуативно. OIG обнаружила, что усилиям по внедрению общекорпоративной программы управления активами программного обеспечения препятствуют проблемы с бюджетом и кадрами, а также сложность и объем лицензионных соглашений агентства.

OIG оценила систему управления программными активами НАСА как «базовую» — это самый низкий из четырех вариантов рейтинга в модели зрелости и оптимизации управления программными активами, разработанной Microsoft и принятой Международной организацией по стандартизации/Международной

электротехнической комиссией. Следовательно, OIG заявила, что НАСА, скорее всего, пройдет несколько лет от перехода к модели корпоративных вычислений, в которой ИТ-возможности, такие как управление программными активами и кибербезопасность, централизованы и консолидированы. Тем временем OIG обнаружила, что агентству еще предстоит внедрить основные передовые методы или полностью внедрить федеральные инструкции, необходимые для надлежащего управления его программой управления активами программного обеспечения. Наблюдательный орган заявил, что НАСА не внедрило централизованный инструмент управления программными активами для обнаружения, инвентаризации и отслеживания данных о лицензиях, как того требует федеральная политика.

Этот недостаток привел к тому, что НАСА потратило около 15 миллионов долларов за последние пять лет на неиспользованные лицензии, сумма, которую OIG определила как расточительную и поэтому ставит под сомнение.

Аудит показал, что NASA не внедрило общекорпоративные процессы, необходимые для надлежащего управления рисками кибербезопасности, связанными с управлением программными активами. В частности, OIG обнаружила, что программное обеспечение, загруженное с привилегированным доступом, не отслеживается на предмет соответствия лицензии и управления жизненным циклом и может непреднамеренно создавать киберуязвимости, включая вредоносные программы, в сети НАСА. Кроме того, инспекторы отметили, что у НАСА нет последовательного общеагентского процесса ограничения привилегированного доступа или использования разрешений «наименьших привилегий», который дает пользователям только те разрешения на программное обеспечение, которые необходимы для их работы. OIG заявила, что за последние 15 лет в рамках трех общекорпоративных контрактов на управление ИТ НАСА изо всех сил пыталось получить контроль над использованием привилегированного доступа.

Согласно анализу OIG, данные показали, что в период с 2020 по 2022 год почти 11 000 пользователей во всем агентстве получили привилегированный доступ, в основном для установки программного обеспечения. Вызывает тревогу тот факт, что наблюдательный орган обнаружил, что всем примерно 6500 пользователям другого Центра НАСА был предоставлен привилегированный доступ к своим компьютерам — по сути, включая возможность загружать и устанавливать программное обеспечение по своему желанию. Должностные лица НАСА сообщили OIG, что, хотя использование привилегированного доступа примерно 6500 пользователями в Центре на протяжении многих лет подвергалось тщательной проверке, операционные ограничения, конфликты из-за сложности и масштаба федеративной среды НАСА, а также финансирование продолжают откладывать ограничения на привилегированный доступ.

OIG также обнаружила, что программные приложения для миссий и организаций, разработанные внутри компании, страдают от недостатка централизации и прозрачности инвентаризации, что ограничивает возможности агентства по выявлению дублирующегося или устаревшего программного обеспечения. Инспекторы обнаружили, что политика НАСА по управлению

программными активами не является всеобъемлющей или стандартизированной, что оставляет неясными роли, обязанности и процессы. Кроме того, было обнаружено, что должности отдела управления программными активами и менеджера программного обеспечения агентства не согласованы и не подчиняются директору по информационным технологиям, как того требует федеральная политика.

Аудит OIG также показал, что у НАСА нет последовательных процедур юридического представительства во время переговоров по контрактам на программное обеспечение и проверок поставщиков, что может привести к увеличению расходов агентства из-за штрафов за нарушения лицензионных соглашений на программное обеспечение. Кроме того, OIG заявила, что обучение использованию и управлению лицензиями на программное обеспечение не является последовательным во всем агентстве, поскольку устаревшее веб-обучение назначается персоналу случайным образом, а общий курс обучения лицензированию программного обеспечения, доступный для всех сотрудников, отсутствует.

Наблюдательный орган заявил, что НАСА не удалось внедрить процессы, необходимые для управления финансовыми рисками, поскольку закупки программного обеспечения недостаточно отслеживаются и санкционируются Управлением главного информационного директора (OCIO), что позволяет некоторым пользователям обходить авторизацию OCIO (и проверку группы управления программными активами). приобретать программное обеспечение с помощью альтернативных средств, таких как карты покупки. Кроме того, OIG заявила, что нынешние усилия НАСА по составлению полного и точного отчета о годовых расходах на программное обеспечение отнимают много времени и в основном выполняются вручную.

По оценкам OIG, без этих недостатков НАСА могло бы сэкономить примерно 35 миллионов долларов (20 миллионов долларов на штрафах и переплатах и 15 миллионов долларов на неиспользованных лицензиях), а продвижение вперед могло бы сэкономить 4 миллиона долларов в течение следующих трех лет за счет внедрения общекорпоративной программы управления активами программного обеспечения.

OIG вынесла ряд рекомендаций, в том числе о том, чтобы НАСА разработало общеагентский процесс ограничения привилегированного доступа к компьютерным ресурсам в соответствии с концепцией минимальных привилегий, с которыми НАСА частично согласилось. Агентство заявило, что менеджер программных активов установит регулярный график отчетности перед директором по информационным технологиям агентства и высшим руководством, чтобы получить представление о деятельности по управлению программным обеспечением». ***(OIG Raps NASA Over Software Cybersecurity // Estonian Free Press (https://estonianfreepress.com/cybersecurity/oig-raps-nasa-over-software-cybersecurity/). 14.01.2023).***

***

«Президент Байден собирается одобрить политику, которая идет намного дальше, чем любые предыдущие усилия по защите частных компаний от злонамеренных хакеров, и ответит этим хакерам нашими собственными кибератаками.

35-страничный документ под названием «Национальная стратегия кибербезопасности» отличается от примерно дюжины подобных документов, подписанных президентами за последнюю четверть века, двумя важными моментами: во-первых, он налагает обязательные правила на широкий круг американских отраслей. Во-вторых, он уполномочивает оборонные, разведывательные и правоохранительные органы США переходить в наступление, взламывая компьютерные сети преступников и иностранных правительств в ответ или упреждая их атаки на американские сети.

«Наша цель состоит в том, чтобы сделать злоумышленников неспособными проводить устойчивые кибер-кампании, которые угрожали бы национальной безопасности или общественной безопасности Соединенных Штатов», — говорится в документе в пятистраничном разделе под названием «Прекращение и ликвидация угроз». к черновику, просматриваемому исключительно Slate. (Документ еще не был обнародован, хотя это произойдет после того, как Байден подпишет его, что ожидается где-то в этом месяце.).» ***(When It Comes to Cybersecurity, the Biden Administration Is Getting Much More Aggressive // Estonian Free Press (https://estonianfreepress.com/cybersecurity/when-it-comes-to-cybersecurity-the-biden-administration-is-getting-much-more-aggressive/). 17.01.2023).***

***

«В последние дни 2022 года и 117-го Конгресса президент Байден подписал HR7535, Закон о готовности к кибербезопасности квантовых вычислений, вступивший в силу. Закон признает будущую угрозу, которую квантовое дешифрование представляет для федеральных административных органов, и предписывает изучить криптографию данных агентств, чтобы подготовиться к тому времени, возможно, через много лет, когда квантовые вычисления смогут расшифровать эти данные...

Закон о готовности к кибербезопасности квантовых вычислений

Квантовая дешифрация также может поставить под угрозу правительственные секреты. Итак, когда на горизонте появилось квантовое дешифрование, Конгресс принял, а президент подписал Закон о готовности квантовых вычислений к кибербезопасности, чтобы смягчить надвигающуюся угрозу.

Закон признает угрозу, которую квантовые вычисления создают для национальной безопасности: (1) Криптография необходима для национальной безопасности Соединенных Штатов и функционирования экономики Соединенных Штатов. (2) Наиболее распространенные сегодня протоколы шифрования полагаются на вычислительные возможности классических компьютеров для обеспечения кибербезопасности. (3) Квантовые компьютеры могут когда-нибудь обрести способность раздвигать границы вычислений, позволяя нам решать

проблемы, которые до сих пор были неразрешимы, такие как целочисленная факторизация, которая важна для шифрования. (4) Быстрый прогресс квантовых вычислений предполагает, что сегодня противники Соединенных Штатов могут украсть конфиденциальные зашифрованные данные, используя классические компьютеры, и ждать, пока будут доступны достаточно мощные квантовые системы для их расшифровки.

Разделы 2(a), 3(d)(9) (определение «квантового компьютера» как «компьютера, который использует коллективные свойства квантовых состояний, такие как суперпозиция, интерференция и запутанность, для выполнения вычислений»).

Закон требует, чтобы директор Управления и управления и бюджета (OMB) разработал и издал руководство для административных органов «по переходу информационных технологий на постквантовую криптографию». Раздел 4(a). Это руководство должно включать «требование к каждому агентству о создании и ведении текущего перечня информационных технологий, используемых агентством, которые уязвимы для расшифровки с помощью квантовых компьютеров». Раздел 4(a)(1).

Следуя этому руководству, агентства затем отчитаются перед OMB о своем инвентаре ИТ, уязвимых для квантового дешифрования. Раздел 4(б). Через год после того, как NIST выпустит свои стандарты постквантовой криптографии, OMB выпустит дополнительные рекомендации, чтобы подготовить агентства к переходу своих данных на новые стандарты, устойчивые к квантовым вычислениям. Раздел 4(c). В течение этого периода и в течение следующих пяти лет OMB будет отчитываться перед Конгрессом о ходе миграции. Раздел 4(e). Этот длительный период свидетельствует о трудностях, с которыми агентства, многие из которых все еще полагаются на старые, устаревшие системы, столкнутся при пересмотре своих схем шифрования.

Закон освобождает все системы национальной безопасности. Раздел 5. Однако переход этих систем на постквантовую криптографию уже начался.

В то время как Закон будет иметь большое значение для защиты данных агентства от квантовой атаки, в некоторых отношениях кот уже вынут из мешка. Сегодняшние хакеры могут получать зашифрованные данные и хранить их годами, зная, что квантовый компьютер будущего сможет их расшифровать. Эту методику иногда называют «собрать сейчас, расшифровать позже», и Закон не может защитить уже скомпрометированные данные от последующего расшифрования. Тем не менее, признание правительством будущих угроз и смягчение их последствий является важным шагом на пути к защите своих данных в будущем». ***(Jacob W. S. Schneider. Quantum Computing: Examining the Quantum Computing Cybersecurity Preparedness Act // Holland & Knight LLP (https://www.hklaw.com/en/insights/publications/2023/01/quantum-computing-examining-the-quantum-computing-cybersecurity). 17.01.2023).***

***

«…Канадский центр кибербезопасности выпустил руководство, помогающее организациям управлять киберрисками при приобретении и использовании услуг управляемых информационных технологий.

Управляемые ИТ-услуги и киберриски

Многие организации привлекают специализированных поставщиков услуг, известных как поставщики управляемых услуг (MSP), для управления частью или всей инфраструктурой и услугами информационных технологий (ИТ) организации (включая инфраструктуру и услуги, предоставляемые поставщиками облачных услуг и другими третьими сторонами). Аутсорсинг услуг по управлению ИТ может обеспечить значительные преимущества, но также может представлять значительные риски для бизнеса и соответствия законодательству.

Организация, использующая управляемые ИТ-услуги, часто зависит от MSP (поскольку службы часто имеют решающее значение для повседневной работы организации) и уязвима для неправомерных действий со стороны MSP или его персонала (поскольку персонал MSP обычно имеет привилегированный удаленный доступ к ИТ-системы и данные организации). Кроме того, услуги MSP сопряжены с неотъемлемыми рисками кибербезопасности, поскольку киберпреступники нацелены на MSP, чтобы получить доступ к ИТ-системам и данным своих клиентов. Канадский центр кибербезопасности в Национальной оценке киберугроз на 2023–2024 годы предупреждает, что киберпреступники «почти наверняка» продолжат нацеливаться на MSP, чтобы максимизировать охват своих атак программ-вымогателей…

По этим причинам организациям следует выявлять и управлять кибер-рисками (а также другими деловыми и правовыми рисками) при приобретении и использовании управляемых ИТ-услуг...

Руководство по закупкам

В октябре 2020 года Канадский центр кибербезопасности выпустил руководство под названием « Вопросы кибербезопасности для потребителей управляемых услуг » (Руководство), чтобы помочь организациям определить, способен ли MSP эффективно и безопасно предоставлять услуги по управлению ИТ, и заключить соответствующее соглашение об услугах с MSP. В руководстве рассматриваются ключевые вопросы кибербезопасности, которые организациям следует учитывать при приобретении управляемых услуг у MSP. Ниже приводится резюме:

Безопасность данных. Организация должна определить виды данных, которые будут доступны для MSP, и определить меры безопасности, необходимые для защиты данных.

Соблюдение законодательства: Организация должна понимать свои обязательства в соответствии с законами общего применения и отраслевыми законами в отношении данных, которые будут доступны для MSP.

Оценка MSP: организация должна оценить адекватность внутренних средств контроля безопасности MSP по сравнению с признанными стандартами/структурами безопасности и с использованием сторонних аудиторских отчетов.

Контроль доступа: организация должна установить политики и процедуры, регулирующие доступ к данным организации и ИТ-системам (включая правила доступа к данным, основанные на принципе наименьших привилегий, механизмы аутентификации и авторизации, роли системного администратора, физический доступ к серверам, политики паролей и федеративные аутентификации) и указать соответствующие роли/обязанности организации и MSP.

Шифрование. Организация должна определить требуемый уровень шифрования для данных в пути и в состоянии покоя и оценить, может ли MSP поддерживать требуемое шифрование с помощью соответствующих методов и процедур (включая управление ключами).

Отчетность об инцидентах/реагирование на них: организация должна установить четкие требования к отчетности об инцидентах и реагированию на них и гарантировать, что MSP может поддерживать эти требования. В соглашении об услугах с MSP должны быть указаны ожидаемые сроки выполнения работ, средства связи, процессы эскалации, показатели для оценки производительности и финансовые средства правовой защиты в случае неудовлетворительной производительности.

Непрерывность бизнеса/аварийное восстановление. Организация должна определить свои требования к уровню обслуживания (т. е. качеству) и понять меры, применяемые MSP для предотвращения нарушения обслуживания и поддержки восстановления обслуживания в случае аварии.

Целостность цепочки поставок: организация должна понимать услуги третьих сторон (включая информационные и коммуникационные технологии), используемые MSP, и гарантии, которые MSP дает в отношении этих услуг.

Стратегии выхода. Организация должна понимать свои права на прекращение участия MSP и передачу данных альтернативному MSP.

Уничтожение данных: Организация должна установить политику хранения/удаления данных и убедиться, что MSP может поддерживать эту политику.

В Руководстве подчеркивается, что соглашение организации с MSP должно четко определять соответствующие роли и обязанности организации и MSP в отношении каждого из вопросов, подробно описанных в Руководстве…

Консультации по кибербезопасности

В мае 2022 года Канадский центр кибербезопасности объявил о выпуске рекомендаций по кибербезопасности под названием « Защита от киберугроз для поставщиков управляемых услуг и их клиентов» («Рекомендации»), выпущенных совместно с органами кибербезопасности Великобритании, Австралии, Новой Зеландии и США. В бюллетене отмечается рост числа киберпреступлений, направленных против MSP, и содержатся рекомендации для MSP и их клиентов по защите от киберугроз. В бюллетене поясняется, что он предназначен для «обеспечения прозрачных, хорошо информированных дискуссий между MSP и их клиентами» по вопросам кибербезопасности, что должно «привести к переоценке процессов безопасности и договорных обязательств с учетом допустимого риска клиентов».

В бюллетене рекомендуется, чтобы MSP и их клиенты применяли определенные и подробные базовые меры безопасности и оперативные средства контроля для предотвращения и снижения рисков кибербезопасности. Ниже приводится резюме:

Предотвратите первоначальную компрометацию, внедрив рекомендуемые контрмеры и средства контроля.

Включите/улучшите процессы мониторинга и ведения журналов для обнаружения угроз и храните журналы не менее шести месяцев.

Обеспечьте многофакторную аутентификацию для доступа к сетям и системам.

Управляйте внутренними архитектурными рисками и разделяйте внутренние сети, чтобы уменьшить масштабы и последствия компрометации.

Применяйте принцип доступа с наименьшими привилегиями во всех сетевых средах.

Откажитесь от устаревших учетных записей и инфраструктуры (включая системы и службы), чтобы ограничить поверхность атаки.

Применяйте обновления программного обеспечения и определяйте приоритетность обновлений безопасности для устранения известных уязвимостей программного обеспечения.

Резервное копирование систем и данных на регулярной основе в соответствии с целевыми точками восстановления и безопасное хранение резервных копий.

Разработайте и регулярно применяйте планы реагирования на инциденты и восстановления.

Упреждающее управление рисками цепочки поставок ИТ, в том числе рисками, связанными со сторонними поставщиками и субподрядчиками.

Содействуйте прозрачности с помощью договорных соглашений, которые четко определяют обязанности, включая четкое объяснение услуг MSP.

Управляйте проверкой подлинности и авторизацией учетной записи, используя передовые методы управления паролями и разрешениями.

В бюллетене рекомендуются конкретные действия MSP и клиента для каждой меры кибербезопасности, и подчеркивается, что соглашения с MSP должны касаться рекомендуемых мер кибербезопасности…» ***(Cyber risk guidance for customers and providers of managed IT services // Borden Ladner Gervais LLP (https://www.blg.com/en/insights/2023/01/cyber-risk-guidance-for-customers-and-providers-of-managed-it-services). 19.01.2023).***

***

Країни ЄС та Великобританія

«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. Бажаючі, які відповідають вимогам NCA, мають встигнути подати заявку до 10 січня. Якщо кандидатуру схвалять, спеціаліст отримуватиме зарплату від $ 48 200 до $ 52 400 на місяць.

У NCA заявили, що мають намір орієнтуватися на актуальні розслідування в криптовалютній галузі та ті, що ще з’являться, вимагаючи від кандидатів відповідних навичок та досвіду роботи з новими технологіями. В агентстві пообіцяли, що головним завданням нового відділу буде не розслідування криптопорушень, а їх попередження.

Британія вже сьогодні є одним із найактивніших гравців на ринку криптовалют. Разом із досить прогресивною законодавчою системою та бажанням запустити свій національний стейбкоїн, влада країни часто робить досить консервативні заяви та дії, спрямовані на жорстке регулювання криптовалютного сектору». ***(У Британії за полювання на хакерів та криптовалютних шахраїв платитимуть $ 48 200 на місяць // No worries! (https://noworries.news/u-brytaniyi-za-polyuvannya-na-hakeriv-ta-kryptovalyutnyh-shahrayiv-platytymut-48200-na-misyacz/). 07.01.2023).***

***

«Только что вступили в силу две ключевые директивы о критической и цифровой инфраструктуре, которые укрепят устойчивость ЕС к онлайн- и офлайн-угрозам, от кибератак до преступности, рисков для здоровья населения или стихийных бедствий.

Недавние угрозы критически важной инфраструктуре ЕС пытались подорвать нашу коллективную безопасность. Уже в 2020 году Комиссия предложила существенно обновить правила ЕС в отношении устойчивости критически важных объектов и безопасности сетей и информационных систем.

Две Директивы, вступающие в силу:

Директива о мерах по обеспечению высокого общего уровня кибербезопасности в Союзе (Директива NIS 2)

Директива об устойчивости критических объектов (Директива CER)

Директива NIS 2 обеспечит более безопасную и сильную Европу за счет значительного расширения секторов и типов критически важных объектов, подпадающих под ее действие. К ним относятся поставщики общественных сетей и услуг электронных коммуникаций, услуги центров обработки данных, управление сточными водами и отходами, производство критически важных продуктов, почтовые и курьерские услуги и органы государственного управления, а также сектор здравоохранения в более широком смысле. Кроме того, это укрепит требования к управлению рисками кибербезопасности, которые компании обязаны соблюдать, а также упростит обязательства по отчетности об инцидентах с более точными положениями об отчетности, содержании и сроках. Директива NIS2 заменяет правила безопасности сетей и информационных систем, первое общеевропейское законодательство о кибербезопасности.

В условиях все более сложной картины рисков новая Директива CER заменяет Европейскую директиву о критической инфраструктуре 2008 года. Новые правила повысят устойчивость критической инфраструктуры к целому ряду угроз, включая стихийные бедствия, террористические атаки, внутренние угрозы или саботаж. Будут охвачены 11 секторов: энергетика, транспорт, банковское дело, инфраструктура финансового рынка, здравоохранение, питьевая вода, сточные воды, цифровая инфраструктура, государственное управление, космос и продукты питания. Государствам-членам необходимо будет принять национальную стратегию и проводить регулярные оценки рисков для выявления организаций, которые считаются критически важными или жизненно важными для общества и экономики.

У государств-членов есть 21 месяц, чтобы включить обе Директивы в национальное законодательство. В течение этого времени государства-члены должны принять и опубликовать меры, необходимые для их соблюдения.

В декабре 2022 года Совет принял рекомендацию о общесоюзном подходе к координации для повышения устойчивости критически важной инфраструктуры, где государствам-членам предлагается ускорить подготовительную работу по переносу и применению NIS 2 и Директивы об устойчивости критически важных объектов. объекты (CER)». ***(New stronger rules start to apply for the cyber and physical resilience of critical entities and networks // European Commission (https://digital-strategy.ec.europa.eu/en/news/new-stronger-rules-start-apply-cyber-and-physical-resilience-critical-entities-and-networks). 16.01.2023).***

***

«В Словакии не хватает около 20 000 сотрудников для заполнения вакансий в области кибербезопасности, заявил во вторник глава Центра компетенции и сертификации в области кибербезопасности Иван Макатура.

Специалисты по кибербезопасности нужны фирмам и учреждениям, а также органам местного самоуправления. Государству также не хватает специалистов по кибербезопасности в сфере образования и здравоохранения. Центр собрал статистику востребованных вакансий в области кибербезопасности. Например, в операторах базовых услуг необходимо укомплектовать более 12 000 таких должностей, в средних компаниях – 2 700 и более 2 000 – в органах государственного управления.

Словакия начала частично решать проблему нехватки специалистов по кибербезопасности за счет переподготовки или специализации специалистов из аналогичных областей. Однако это лишь краткосрочное решение, сказал Макатура, который видит долгосрочное решение в значительном увеличении аккредитованных университетских программ в этой области». ***(Slovakia in need of almost 20,000 cyber security professionals // RTVS - Rozhlas a televízia Slovenska (https://enrsi.rtvs.sk/articles/news/313513/slovakia-in-need-of-almost-20000-cyber-security-professionals). 04.01.2023).***

***

«Недавнее изменение законодательства, касающееся кибербезопасности, актуально для отрасли медицинских технологий. Это обновление Директивы (ЕС) 2022/2555 о безопасности сетей и информационных систем NIS 2 («Директива»). Директива NIS 2 является частью Стратегии кибербезопасности ЕС и устанавливает меры по управлению рисками кибербезопасности и требования к отчетности для особо важных секторов. Это включает в себя индустрию медицинского оборудования.

Требования кибербезопасности для производителей медицинского оборудования и IVD в Директиве NIS 2

NIS 2 Директива, в дополнение к мерам безопасности информационных технологий, установленным в Регламенте (ЕС) 2017/745 о медицинских устройствах («MDR») и Регламенте (ЕС) 2017/746 2017 о медицинских устройствах для диагностики in vitro («IVDR») («Правила»), предъявляет к производителям медицинского оборудования и IVD дополнительные требования к кибербезопасности, установленные в Директиве NIS 2. Директива отменяет и заменяет Директиву NIS, вступившую в силу в 2016 году. Директива NIS устанавливает меры для обеспечения общего высокого уровня кибербезопасности для критически важных инфраструктур по всему ЕС. Учитывая растущее число киберугроз и кибератак, а также фрагментарное внедрение Директивы NIS в государствах-членах ЕС, Европейский парламент и Совет приняли Директиву NIS 2 в ноябре 2022 года.

Среди ключевых обновлений:

Расширение сферы применения: Материальная сфера применения Директивы NIS 2 была расширена и теперь охватывает производителей медицинских устройств и IVD. Эти производители классифицируются как «важные организации». Более того, производители подмножества устройств, считающихся «критически важными во время чрезвычайной ситуации в области общественного здравоохранения», квалифицируются как «основные организации». Разница между категориями заключается в том, что важные субъекты подлежат надзору ex post в отношении соблюдения требований, предусмотренных в Директиве NIS 2, в то время как существенные субъекты могут подвергаться как ex ante, так и ex post. надзорным мерам

Подробные меры по управлению рисками: как основные, так и важные организации должны принять меры по управлению рисками кибербезопасности, предусмотренные в статье 21 Директивы. Сюда входят экономические операторы по всей цепочке поставок, т. е. прямые поставщики и поставщики услуг, такие как поставщики услуг хранения и обработки данных и поставщики управляемых услуг безопасности.

Обязанности высшего руководства: «Органы управления» важных и существенных организаций обязаны контролировать реализацию мер по управлению рисками кибербезопасности и могут быть привлечены к ответственности за их несоблюдение. Директива NIS 2 не определяет термин «органы управления», оставляя на усмотрение национального законодательства отдельных государств-членов ЕС определение и определение территориального

охвата этого термина. Однако в Декларационной части 76 предполагается, что этот термин относится к высшему руководству и юридическим представителям.

Сдвинутые сроки для сообщения об инцидентах кибербезопасности: в соответствии с пересмотренными обязательствами по отчетности, предусмотренными в Директиве NIS 2, основные и важные организации должны:

уведомлять компетентные органы поэтапно, сначала путем направления «раннего предупреждения» в течение 24 часов после того, как стало известно о серьезных инцидентах в области кибербезопасности, а затем уведомления об инциденте в течение 72 часов;

подготовить промежуточный отчет по запросу компетентного органа или группы реагирования на инциденты компьютерной безопасности («CRIST»); и

представить окончательный отчет в течение 1 месяца после уведомления об инциденте. NIS об инцидентах нужно было уведомлять «без неоправданной задержки» Для сравнения, в соответствии с Директивой.

Создание европейской базы данных уязвимостей: Агентству Европейского союза по кибербезопасности («ENISA») поручено создать и поддерживать базу данных, которая будет включать информацию об общеизвестных уязвимостях продуктов и услуг. Раскрытие информации в базе данных является добровольным.

Административные штрафы: Статья 34 Директивы NIS 2 вводит административные штрафы для основных и важных субъектов, которые не внедрили меры по управлению рисками. Вводятся эквивалентные штрафы за неисполнение обязательств по отчетности. В случае обнаружения нарушения этих требований национальные органы власти могут наложить штраф в размере:

до 7 млн евро или 1,4% от общего мирового годового оборота по важным организациям; и

до 10 млн евро, или 2% от общего годового оборота по всему миру на предприятиях первой необходимости.

Следующие шаги

Директива NIS 2 была опубликована в Официальном журнале 27 декабря и вступит в силу через 20 дней после публикации. Затем у государств-членов ЕС будет 21 месяц, чтобы включить Директиву в национальное законодательство.

Производители медицинского оборудования должны начать рассматривать организационные, финансовые и технические меры, которые потребуются для соблюдения требований, установленных в Директиве NIS 2». ***(Elizabeth Anne Wright, Alexander Wenzel and Anastasia Vernikou. The NIS 2 Directive establishes new cybersecurity requirements for medical device manufacturers // Cooley (https://products.cooley.com/2023/01/03/the-nis-2-directive-establishes-new-cybersecurity-requirements-for-medical-device-manufacturers/). 03.01.2023).***

***

«…Новое исследование показало, что две трети владельцев малого бизнеса в Австралии считают, что технические знания приравниваются к навыкам кибербезопасности.

Но наше первое поколение цифровых аборигенов, поколение Z (родившееся между 1997 и 2010 годами), относится к числу наименее защищенных от киберугроз в стране.

Опрос показал, что представители поколения Z чаще всего оценивали кибербезопасность как низкую или среднюю угрозу для малого бизнеса, которым они владели или в котором работали.

Они также приложили больше усилий, чем другие группы, для выявления и предотвращения некоторых из наиболее распространенных кибератак, с которыми сталкиваются малые предприятия, таких как кража личных данных, атаки вредоносных программ и программы-вымогатели.

Согласно опросу, самая надежная пара рук в сообществе малого бизнеса, по-видимому, — это представители поколения X и миллениалы старшего возраста в возрасте 30 лет, которые, скорее всего, серьезно относятся к кибербезопасности.

Малый бизнес становится все более уязвимым

Опрос был проведен для Совета организаций малого бизнеса Австралии (COSBOA) в рамках инициативы Cyber Wardens.

В октябре COSBOA объявила о плане запуска пилотной программы Cyber Wardens в качестве нового ресурса для малого бизнеса Австралии, чтобы узнать, как защитить себя от киберугроз и мошенничества, которые обходятся экономике примерно в 29 миллиардов долларов в год.

Это объявление было сделано в разгар некоторых из самых серьезных утечек данных в Австралии, которые были нацелены на Optus, а затем на Medibank.

Когда произошли эти атаки, эксперты по кибербезопасности предупредили, что взломы сделали клиентов этих компаний уязвимыми для кражи личных данных и финансового мошенничества, и они раскритиковали крупные австралийские компании за недостаточно серьезное отношение к безопасности данных.

Но академические исследования также показывают, что малые предприятия сталкиваются со своими собственными проблемами, потому что они все чаще становятся привлекательными целями для киберпреступников, но им не хватает ресурсов крупных компаний для борьбы с ними.

COSBOA заявляет, что в этом году развернет бесплатную программу Cyber Wardens по всей стране для малого бизнеса Австралии.

В преддверии запуска компания 89 Degrees East попросила опросить владельцев и сотрудников малого бизнеса, чтобы оценить их отношение к киберугрозам и измерить их компетенции в области кибербезопасности.

COSBOA заявила, что результаты опроса содержат предупреждение.

Выяснилось, что представители поколения Z были одними из наименее кибербезопасных, им не хватало знаний и ключевых компетенций в области кибербезопасности по сравнению с их старшими коллегами.

Из всех возрастных групп представители поколения X и миллениалы старше 30 лет чаще всего серьезно относятся к кибербезопасности.

Старшие когорты также лучше знакомы с рисками кибербезопасности, чем поколение Z.

В целом, COSBOA сообщает, что только каждый пятый владелец и сотрудник малого бизнеса уверен в своей способности подготовиться (23%), бороться (21%) и восстановиться после (21%) киберугрозы.

В нем говорится, что результаты опроса также показывают, что владельцы малого бизнеса не должны полагаться на младших членов семьи или сотрудников для подготовки своего бизнеса к кибератакам и другим проблемам безопасности.

«Хорошим первым шагом является определение того, кто отвечает за киберзащиту вашего бизнеса», — сказал председатель COSBOA Мэтью Аддисон.

«Не думайте, что ваши дети или младшие сотрудники — самая надежная пара рук, когда дело доходит до онлайн-активности».

Что такое программа Cyber Wardens?

Программа Cyber Wardens была разработана в сотрудничестве с Commonwealth Bank (CBA), Telstra и Австралийским центром кибербезопасности (ACSC).

По данным ACSC, 43% всех киберпреступлений в Австралии совершаются против малого бизнеса.

COSBOA заявляет, что хочет, чтобы эта программа стала первой в Австралии сертификацией кибербезопасности на рабочем месте для сектора малого бизнеса.

В рамках программы участники пройдут обучение на основе основных восьми стратегий смягчения последствий ACSC и получат возможность:

Узнайте о распространенных киберугрозах, которые могут повлиять на их бизнес, и обновляйте свои знания о кибербезопасности.

Действуйте как кибер-чемпион, чтобы помочь повысить безопасность бизнеса, его сотрудников и помочь защитить своих клиентов.

Продвигайте передовые методы управления более безопасными парольными фразами в малом бизнесе.

Внедрить стандарты кибербезопасности на своих рабочих местах

Помогите малым предприятиям научиться мыслить о риске в том, как они управляют своим бизнесом

Знать, где можно получить дополнительную поддержку и сообщить о киберугрозах

Что насчет опроса?

Исследование было проведено организацией 89 Degrees East от имени COSBOA. Результаты были получены в результате опроса более 2100 владельцев бизнеса и сотрудников (564 владельца бизнеса и 1553 сотрудника).

Опрос проводился со 2 ноября по 7 декабря 2022 года.

Он проводился в режиме онлайн с участием участников из коммерческой исследовательской группы и организаций-членов COSBOA.

Выборка была набрана с управлением квотами, чтобы отразить профили населения по полу, возрасту и местоположению.

89 Degrees East сообщила, что опрос был разработан после первоначального обзора литературы, чтобы убедиться, что исследование основано на существующих данных о взглядах и опыте в области кибербезопасности». ***(Gareth Hutchens. Small business owners warned not to rely on Gen Z to handle cyber security // ABC (https://www.abc.net.au/news/2023-01-16/gen-z-are-least-aware-of-cyber-risks-cosboa-cyberwardens/101856932). 16.01.2023).***

***

Російська Федерація та країни ЄАЕС

«Згідно з заявою Олександра Бражнікова, директора РАКІБ (російська асоціація криптоіндустрії та блокчейну), уряди росії та Ірану вивчають можливість випуску власного стейблкоїна. Планується, що вартість цифрового активу буде прив'язана до золота.

За попередніми домовленостями, стейблкоїн використовуватимуть для міжнародних розрахунків у межах Перського регіону. Наявність таких планів підтвердили й у Державній думі рф. Втім, запуском стейблкоїна росіяни займуться лише після того, як вирішать питання, пов'язані з регулюванням крипторинку.

Іран вже тривалий час використовує криптовалюти для обходу санкцій. Ще наприкінці серпня прем'єр-міністр росії Михайло Мішустін повідомив про плани країни-окупанта наслідувати приклад Ірану. «Нам потрібно інтенсивно розвивати інноваційні напрямки, включаючи впровадження цифрових активів. Це безпечна альтернатива, яка може гарантувати безперебійну оплату постачання товарів з-за кордону та на експорт», — заявив тоді Мішустін…». ***(Росія та Іран розроблятимуть власну криптовалюту // No worries! (https://noworries.news/rosiya-ta-iran-rozroblyatymut-vlasnu-kryptovalyutu/). 16.01.2023).***

***

Інші країни

«Постоянное представительство Израиля при Организации Объединенных Наций в сотрудничестве с Национальным кибердиректором Израиля (INCD) и Team8 во вторник провело мероприятие по кибербезопасности в ООН.

Мероприятие проходило на фоне усиления кибератак по всему миру против частных компаний и стран. Выступавшие на мероприятии говорили о сотрудничестве, необходимом между странами и частными компаниями для защиты граждан от нападений.

В своем выступлении посол Израиля в ООН Гилад Эрдан сказал: «Являясь мощным центром киберзащиты, Израиль имеет глубокое чувство долга поддерживать других на местах. -выигрышная ситуация для всех. Более безопасное будущее для всех».

«Сегодня, в эпоху, когда поле боя перемещается из географических арен в цифровую сферу, ключом к достижению коллективной защиты является работа в качестве совместной глобальной команды. И ООН, центральная сцена международной дипломатии, является идеальным местом. для выполнения такой важной миссии», — добавил он.

«Именно здесь мы делимся передовым опытом, проводим обсуждения и учимся друг у друга. И именно здесь мы можем построить железный купол — защитный щит — против кибератак и цифровых угроз».

«Мы все обязаны работать бок о бок, чтобы обеспечить безопасность каждого из нас», — сказал Эрдан.

В рамках мероприятия высокопоставленные технические руководители обсудили сотрудничество с целью создания новых инструментов для борьбы с угрозами кибератак на жизненно важную гражданскую инфраструктуру, включая больницы, банки, государственные учреждения и многое другое.

Надав Зафрир, соучредитель и управляющий партнер Team 8, сказал: «Мы должны работать вместе, чтобы вывести все страны за черту кибербедности. Во-первых, мы должны признать, что цифровая инфраструктура является критически важной инфраструктурой. Мы должны понимать, что обмен знаниями правильное решение. Затем мы должны создать среду для мирового сотрудничества и разработать для этого технологии».

Первый заместитель национального кибер-директора США Кемба Энеас Уолден, соучредитель и управляющий партнер Team8 Надав Зафрир, главный специалист по информационным технологиям ООН, помощник генерального секретаря Бернандо Мариано Хоаким-младший и исполнительный директор INCD по международному сотрудничеству Авирам Атзаба обратился к мероприятию. Кроме того, Zafrir организовал панель с киберэкспертами из частного сектора, включая Microsoft, Rockwell Automation и JupiterOne. Эксперты обсудили продвижение партнерства между государственным и частным секторами в оборонной кибербезопасности». ***(Israeli UN mission hosts cyber security event at UN // Israel National News (https://www.israelnationalnews.com/news/366068). 18.01.2023).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Під час виступу на Всесвітньому економічному форумі у Швейцарії директор Федерального бюро розслідувань (ФБР) Крістофер Рей висловив стурбованість тим, як Китай використовуватиме алгоритми штучного інтелекту. За словами Рея, уряд Китаю планує займатися кіберзлочинною діяльністю за допомогою ШІ.

«Китайський уряд має найбільш масштабну хакерську систему, ніж будь-яка інша країна світу», — наголосив Рей. «Їхня програма штучного інтелекту не обмежена верховенством закону, вона побудована на основі величезної кількості інтелектуальної власності та конфіденційних даних, які вони [Китай] вкрали за ці

роки. Ці дані будуть використовуватися, найімовірніше, для злочинних цілей», — додав голова ФБР.

Також Крістофер Рей прокоментував поточний стан технологій: «ШІ — класичний приклад технології, на яку я щоразу реагую однаково. Я думаю: «Вау, ми можемо це зробити?» А потім згадую: «О боже, вони [Китай] теж можуть це зробити» і все стає не таким перспективним».

Наразі китайські розробники активно працюють над стратегією Multi-Domain Precision Warfare, аналогічною системі Пентагону Joint All-Domain Command and Control. Цим концепціям необхідні передові алгоритми штучного інтелекту та суперкомп'ютери для швидкої обробки великих даних, на основі яких військові отримують інформацію в режимі реального часу. Деякі американські експерти вважають, якщо у найближчі 5-10 років розпочнеться війна Китаю за Тайвань, то її результат залежатиме від можливостей штучного інтелекту та політичної волі Китаю.

На початку січня ми вже публікували інформацію від анонімних джерел, згідно з якою уряд Китаю планує створити власний штучний інтелект, щоб використовувати його у військових цілях. Все для того, щоб до 2035-го року «прокачати» Народно-визвольну армію Китаю до рівня армії США. Основна перешкода на цьому шляху — влада Америки, яка розуміє масштаби загрози та намагається обмежити постачання сучасної мікротехніки у Китай». ***(Штучний інтелект від Китаю назвали головною загрозою безпеці США // No worries! (https://noworries.news/shtuchnyj-intelekt-vid-kytayu-nazvaly-golovnoyu-zagrozoyu-bezpeczi-ssha/). 25.01.2023).***

***

«…Прокремлевская вредоносная хакерская группа KillNet временно отключила доступ к веб-сайтам немецких правительственных учреждений, аэропортов и финансовых учреждений в отместку за решение Берлина отправить танки Leopard 2 в Украину.

Канцлер Германии Олаф Шольц объявил в среду, что Германия поставит передовой боевой танк после нескольких недель давления со стороны союзников по НАТО в преддверии ожидаемого весной этого года наступления России на украинских защитников. Германия первоначально поставит 14 танков Leopard 2 и позволит другим странам, таким как Польша, отправить танки немецкого производства из своих запасов. «Леопард-2» — это серьезная модернизация советских танков Т-72, которые были основой украинской армии. Соединенные Штаты также пообещали предоставить 31 танк M1A2 Abrams, хотя официальные лица США представили эту поставку как долгосрочное обязательство, а не как немедленную поддержку украинской армии.

Федеральное управление информационной безопасности Германии, известное как BSI, сообщило Information Security Media Group, что распределенные атаки типа «отказ в обслуживании» KillNet малоэффективны.

«BSI не имеет признаков какого-либо прямого воздействия на соответствующий сервис и не ожидает, что это произойдет, если будут приняты обычные меры защиты от DDoS-атак», — сказал представитель.

KillNet входит в число немногих российских киберпреступных группировок, открыто присягнувших Москве. Группа, название которой происходит от инструмента, используемого для запуска DDoS-атак, инициировала множество таких атак против западных целей за 11 месяцев после эскалации вторжения России в Украину в феврале 2022 года. Атаки оказались скорее раздражающими, чем опасными.

Группа в своем Telegram-канале отреагировала на заявление Шольца, попытавшись сплотить других прокремлевских хакеров для проведения «полномасштабной кибератаки» и пометить свои усилия хэштегом «Германия RIP».

Активность группы вызвала реакцию Канады. Агентство, которое курирует кибербезопасность федерального агентства, призвало к «повышенной бдительности» после обещания правительства премьер-министра Джастина Трюдо отправить четыре танка Leopard 2 из своего арсенала в Украину.

Представитель Службы безопасности связи сообщил Канадской радиовещательной корпорации, что агентству известно о связанных с государством российских хактивистских группах, стремящихся скомпрометировать украинских союзников.

«CSE напоминает канадскому сообществу кибербезопасности о необходимости проявлять повышенную бдительность и укреплять свою осведомленность и защиту от злонамеренных киберугроз», — сказал представитель». ***(Mihir Bagwe. Russian Nuisance Hacking Group KillNet Targets Germany // Information Security Media Group, Corp. (https://www.govinfosecurity.com/russian-nuisance-hacking-group-killnet-targets-germany-a-21039). 27.01.2023).***

***

«…Национальное агентство по кибербезопасности Великобритании предупреждает, что британское гражданское общество и оборонные организации подвержены риску увеличения числа целевых фишинговых атак со стороны российских и иранских хакеров, спонсируемых государством, которые активно используют передовую социальную инженерию для кибершпионажа.

В предупреждении, опубликованном в четверг, Национальный центр кибербезопасности Великобритании предупредил, что российская передовая постоянная группа Seaborgium и иранская группа CharmingKitten используют ранее невиданную тактику для кражи жизненно важной информации, которую спецслужбы страны считают важной в рамках шпионских кампаний.

Журналисты, неправительственные организации, аналитические центры, оборонные организации и ученые в стране подвергаются риску увеличения числа кибератак, и агентство рекомендует этим группам активно отслеживать любые подозрительные ссылки, отправляемые по электронной почте, и использовать меры безопасности, такие как многофакторная аутентификация, чтобы избежать потенциальных крупных атак. масштабный компромисс.

«Мы настоятельно рекомендуем организациям и частным лицам сохранять бдительность в отношении возможных подходов и следовать рекомендациям по смягчению последствий, содержащимся в бюллетене, чтобы защитить себя в Интернете», — говорит Пол Чичестер, операционный директор NCSC.

Хотя в прошлом и Charming Kitten, и Seaborgium использовали целевой фишинг для сбора разведывательных данных, агентство сообщает, что последние кампании гораздо более изощренны и используют очень персонализированную тактику, чтобы заманить жертв нажать на ссылку.

К ним относятся использование поддельных учетных записей в социальных сетях законных людей для отправки вредоносных ссылок, иногда замаскированных под URL-адреса собраний Zoom, выдача себя за адреса электронной почты Outlook или Yahoo знакомых контактов и использование вредоносных доменов, напоминающих законные организации, для нападения на жертв. В одном случае, наблюдаемом NCSC, злоумышленники рассылали жертвам вредоносные ссылки через чат Zoom.

В отчете говорится, что когда жертвы нажимают на эти вредоносные ссылки, они перенаправляются на сайты для сбора учетных данных, замаскированные под страницы входа в законные службы. Затем хакеры используют украденные учетные данные для доступа к электронной почте жертвы, а также отправляют больше вредоносных ссылок на контакты жертв, добавил он.

«Несмотря на то, что вредоносные кампании используют схожие методы и преследуют схожие цели, эти кампании являются отдельными, и эти два участника не сотрудничают друг с другом», — говорится в сообщении NCSC.

В декабрьском отчете охранная фирма Proofpoint сообщила, что кампания CharmingKitten связана с шестью филиалами в группе APT. Согласно Proofpoint, последняя кампания началась в 2021 году и использует новое вредоносное ПО, получившее название GhostEcho, чтобы получить первоначальный доступ для хакеров для дальнейшего шпионажа. Среди жертв в основном офицеры обороны США и Израиля, а также активисты за права женщин и ученые из США и Европы.

Компания Proofpoint, которая активно отслеживала кампании «Очаровательного котенка» в течение многих лет, утверждает, что деятельность группы проверяется Корпусом стражей исламской революции в целях сбора разведданных. Группа преследует журналистов и активистов по всему Ближнему Востоку как минимум с 2013 года.

Seaborgium, который подозревается в связях с российским кибервоенным подразделением ГРУ, в основном нацелен на правительственных чиновников, аналитические центры и журналистов в Европе». ***(Akshaya Asokan. UK Warns of Surge in Russian, Iranian APT Phishing Threats // Information Security Media Group, Corp. (https://www.govinfosecurity.com/uk-warns-surge-in-russian-iranian-apt-phishing-threats-a-21030). 26.01.2023).***

***

«В среду резервист армии США был приговорен к восьми годам тюремного заключения по обвинению в шпионаже в пользу Китая.

Иностранный гражданин намеревался получить гражданство США и допуск к службе безопасности, чтобы получить должность в сфере кибербезопасности в федеральном правительстве.

В среду федеральный суд приговорил гражданина Китая, проживающего в Соединенных Штатах, к восьми годам тюремного заключения по одному пункту обвинения в том, что он действовал в качестве секретного агента Китайской Народной Республики.

Цзи Чаоцюнь, 31-летний житель Чикаго, зачисленный в резерв армии США, был завербован высокопоставленным офицером разведки КНР по имени Сюй Яньцзюнь еще будучи студентом. Сам Сюй был привлечен к ответственности и приговорен к 20 годам лишения свободы в федеральной тюрьме в ноябре прошлого года за свою роль в управлении группой американских агентов, связанных с аэрокосмической промышленностью.

Получив степень магистра электротехники в Иллинойском технологическом институте, Цзи поступил в резерв армии США в рамках программы под названием «Военные поступления жизненно важны для национальных интересов», которая позволяла набирать иностранных граждан с критически важными навыками. Чтобы принять участие в программе в 2016 году, Цзи ложно заявил, что не контактировал с иностранными правительствами и что у него не было отношений с иностранными шпионами.

Согласно судебным документам, Цзи надеялся получить гражданство США через программу армейских резервов, а затем искать работу в качестве специалиста по кибербезопасности в ЦРУ, ФБР или НАСА и иметь доступ к правительственным базам данных, в том числе к базам данных, посвященным научным исследованиям». ***(Adam Mazmanian. Chinese Spy Sentenced to 8 Years in Federal Prison // Nextgov (https://www.nextgov.com/cxo-briefing/2023/01/chinese-spy-sentenced-8-years-federal-prison/382290/). 27.01.2023).***

***

«Война на Украине показывает, почему цифровые гиганты будут играть все более важную роль в глобальной безопасности. Российско-украинская война — это первый в мире цифровой конфликт, который имеет серьезные последствия для национальной безопасности США и будущего конфликта. Хотя кибернаступление России в начале боевых действий было ожидаемым, неожиданностью стала способность Украины сдерживать атаки Москвы. Это стало результатом значительной поддержки Украины на раннем этапе такими цифровыми гигантами США, как Amazon Web Services (AWS) и Microsoft.

Американские ИТ-компании используют свое господство в сфере цифровых коммуникаций для извлечения данных из российских мобильных телефонов и общедоступных приложений в разведывательных целях и целях. Широкое использование дронов обеими сторонами обеспечивается сложными, часто коммерческими, информационными системами для навигации, целеуказания и сбора разведданных. Частная космическая связь имеет решающее значение для способности Украины защищать себя. Если и можно извлечь урок из почти года

войны, так это то, что американские коммерческие ИТ-фирмы будут играть все более важную роль в обеспечении глобальной безопасности.

Свою так называемую спецоперацию Россия начала с массированной кибератаки на гражданскую, военную и коммерческую инфраструктуру Украины. Это не стало неожиданностью для большинства экспертов в области обороны и кибер-специалистов. Российская киберкампания против Украины продолжается как минимум с момента захвата Крыма в 2014 году.

Большим сюрпризом стала относительная неэффективность российского кибернаступления. Российские кибероперации, по-видимому, оказали умеренное (если вообще возможно) влияние на способность Украины общаться, проводить правительственные и военные операции или управлять критически важной инфраструктурой. Вместо этого украинское правительство, экономика, инфраструктура и вооруженные силы, казалось, функционировали относительно беспрепятственно из-за российских кибероперaций, что вынуждает Москву больше полагаться на кинетические атаки.

Важной причиной, по которой Украине удалось смягчить воздействие российских кибератак, стала поддержка со стороны американских частных цифровых компаний, таких как AWS и Microsoft. Почти с первого дня российского вторжения AWS вмешался, чтобы помочь защитить критически важную информацию украинского правительства. Важные данные и программы, включая налоговую информацию, сведения об имуществе и банковских счетах, а также информацию о государственном персонале, были загружены на твердотельные компьютерные запоминающие устройства размером с чемодан с использованием возможности под названием Snowball Edge, которые были удалены от досягаемости российского оружия. Затем данные были переданы в систему облачных вычислений Amazon. Snowball Edge — это мобильная, гибкая система хранения/вычислений, которая будет интересна американским военным, поскольку она направлена на то, чтобы расширить возможности Объединенной вседоменной системы управления и контроля вплоть до тактического края.

Критическая роль, которую играет AWS, была недавно признана правительством Украины. Киев наградил AWS премией мира в Украине за поддержку Украины в текущем конфликте. По словам вице-премьер-министра Украины и министра цифровой трансформации Михаила Федорова, «Amazon AWS буквально спас нашу цифровую инфраструктуру».

AWS продолжает поддерживать Украину, расширяя спектр государственных и частных экономических отчетов, которые он защищает. Компания обязалась дополнительно выделить 75 миллионов долларов на оборону Украины.

Microsoft также предоставляет Украине критически важные средства киберзащиты. Как и AWS, Microsoft предложила обеспечить безопасное хранение данных Украины в своих облаках. Он также обеспечивает постоянное обнаружение и анализ угроз, что помогает лишить российских хакеров важной информации об украинской обороне, линиях снабжения и военных планах. Компания уже предоставила бесплатную техническую поддержку на сумму 400 миллионов долларов. Еще 100 миллионов долларов будет потрачено в 2023 году.

Google — еще один технологический гигант, вставший на защиту Украины. С самого начала войны компания стремилась нейтрализовать операции российского влияния и обеспечивала непрерывное реагирование на киберинциденты и отслеживание угроз.

В целом Украина продемонстрировала замечательную устойчивость к российским кибератакам, сбору цифровой разведывательной информации и операциям по оказанию влияния. Как заметил один западный аналитик: «Украина продемонстрировала огромную оборонительную мощь и стойкость на физическом поле боя, и то же самое можно сказать и о киберпространстве. Способность Киева использовать опыт многолетних российских кибератак в сочетании с мощной поддержкой западных правительств и, что особенно важно, технологических компаний позволила Украине развернуть киберзащиту в невиданных ранее масштабах и глубине».

Западные кибернавыки также использовались для поддержки наступательных операций Украины. Были широко распространены сообщения о том, что украинские военные использовали активное использование мобильных телефонов российскими солдатами как в разведывательных целях, так и для целей. Недавнему украинскому удару по плацдарму российских военных, который, как сообщается, привел к значительным жертвам, способствовали локальные излучения нескольких частных мобильных телефонов. Сообщается также, что несколько российских генералов были убиты, когда их позиции были определены в результате использования ими незащищенных коммерческих сотовых телефонов. Украина не отключала свои сети сотовой связи и не уничтожала ретрансляторы сотовых телефонов именно в надежде, что российские войска воспользуются их личными устройствами связи, тем самым создав уязвимость, которую можно использовать.

Когда российские командиры и солдаты использовали коммерческие устройства связи, приложения и сети, они создали беспрецедентную возможность для сбора разведывательной информации. Ключом к способности Украины использовать эту возможность стала помощь американских компаний, специализирующихся на добыче такой информации.

SpaceX — четвертый технологический гигант США, который помогает защищать Украину. Российские хакеры пытались вывести из строя коммерческие спутниковые сети, от которых зависит Украина. SpaceX продолжает предоставлять доступ к своей системе Starlink, несмотря на российские угрозы. Компания предоставила десятки тысяч антенн Starlink, чтобы Украина могла поддерживать внутреннюю и международную систему связи.

Украинский конфликт продемонстрировал, что можно защититься даже от сильного киберпротивника. Ключ в том, чтобы полагаться на постоянно растущие возможности частного сектора. В будущих высококлассных конфликтах ключевую роль будут играть частные ИТ-компании, такие как AWS, Microsoft и Google. Учреждению национальной безопасности США необходимо лучше заботиться о цифровых титанах, которые сыграли столь важную роль в создании современной глобальной экономики и которые станут основными игроками в глобальной безопасности». ***(Daniel Goure. Ukraine War Proves the U.S. Government Needs Tech Giants Like Google As Allies // 19FortyFive***

(https://www.19fortyfive.com/2023/01/ukraine-war-proves-the-u-s-government-needs-tech-giants-like-google-as-allies/). 07.01.2023).

***

«CNMF состоит из 39 объединенных кибергрупп, объединенных в шесть оперативных групп, в состав которых входит более 2000 солдат, моряков, морских пехотинцев, летчиков, береговой охраны, гвардейцев, а также гражданских лиц АНБ и РУМО.

Кибернациональные силы миссии официально стали новейшим подчиненным объединенным командованием Министерства обороны во время церемонии в штаб-квартире Киберкомандования США здесь, 19 декабря 2022 года, подчеркнув эволюцию стойких профессиональных киберсил сегодня и в будущем.

CNMF — это объединенные киберсилы вооруженных сил США, которым поручено защищать нацию в киберпространстве с помощью операций полного спектра, включая наступательные, оборонительные и информационные операции.

Генерал армии США Пол М. Накасоне, командующий Киберкомандованием США, был назначенным офицером и руководил церемонией возвышения.

«Эта команда [CNMF] настолько особенная, потому что она всегда была на переднем крае с точки зрения операций, которые мы проводили», — сказал Накасоне, который ранее был одним из ее командиров. «Это команда Киберкомандования США, которая всегда делала первый шаг вперед. Будущее сулит много сил Кибернациональной миссии».

CNMF поддерживает киберкомандование США и национальные приоритеты, такие как безопасность выборов, программы-вымогатели, кибершпионаж и другие кризисные и чрезвычайные операции.

По словам генерал-майора Уильяма Дж. Хартмана, командующего CNMF, обозначение объединенного командования отражает успех CNMF в защите на выборах, российско-украинский кризис, операции по борьбе с программами-вымогателями, глобальные операции по поиску и поддержку тысяч операции общегосударственного значения.

«На самом деле это назначение означает зрелость Кибернациональных сил миссии как перспективной организации для защиты нации», — добавил Хартман. «Речь идет о создании модели постоянной готовности, которая позволит нам оставаться в бою. Речь идет о наших людях: о том, как мы разрабатываем динамическую модель для найма, оценки, обучения и удержания самых талантливых киберсил в мире».

CNMF в прошлом и настоящем:

С момента своего создания в 2014 году Кибернациональные силы миссии Киберкомандования США быстро развивались, чтобы удовлетворить потребности нации, и участвовали или реагировали почти на каждый национальный кризис, с которым сталкивались США.

CNMF, официально активированный 17 января 2014 г., был создан, чтобы удовлетворить потребность Кибернетического командования США в гибких совместных силах, способных сражаться с противниками в киберпространстве. Первоначально CNMF была скомпрометирована из 21 команды, 13 групп кибер-национальных миссий и восьми групп прямой поддержки.

Сегодня CNMF состоит из 39 объединенных кибергрупп, организованных в шесть оперативных групп, в состав которых входит более 2000 солдат, моряков, морских пехотинцев, летчиков, береговой охраны, стражей, а также гражданских лиц АНБ и РУМО.

Миссия CNMF состоит в том, чтобы планировать, направлять и синхронизировать операции полного спектра в киберпространстве, чтобы сдерживать, разрушать и, при необходимости, побеждать враждебных кибернетических и злонамеренных субъектов влияния.

CNMF является частью усилий Министерства обороны по защите кибербезопасности как национальной безопасности и тесно сотрудничает с DHS, ФБР и другими агентствами, а также с отраслевыми, академическими и международными партнерами.

«Это была команда, которая с первого дня поняла, что наша сила исходит из ряда партнерских отношений», — сказал Накасоне. «Мы начинаем с агентства национальной безопасности, партнерства, которое существует между нашим командованием и нашим агентством».

По словам Хартмана, разведывательные данные АНБ лежат в основе операций CNMF и способствуют достижению результатов миссии. «Это также благодаря ФБР, DHS и другим правительственным агентствам, которые полностью сотрудничают в выполнении работы нации», — добавил он.

Эволюция CNMF до объединенного командования является признанием его текущих операций и вклада в решение проблем национального значения.

«Сегодня мы — совместная сила, сосредоточенная на национальных приоритетах», — добавил Хартман. «Мы зрелые, мы гибкие. Мы безжалостны. Мы постоянно адаптируемся к потребностям нации».

Что такое подчиненная единая команда?

Боевой командир создает подчиненное объединенное командование после разрешения министра обороны или президента и назначается для выполнения части миссии или выполнения задач своего вышестоящего командования.

Миссия CNMF носит широкий, непрерывный, совместный и продолжительный характер, соответствующий атрибутам подчиненных объединенных команд.

Создание CNMF в качестве объединенного командования является признанием его непреходящей миссии по борьбе с иностранными злоумышленниками в киберпространстве, отражая его постоянный успех в поддержке национальных приоритетов и формализации его организационной структуры.

Повышение до подчиненного командования будет определять то, как силы будут представлены CNMF, как эти силы будут обучены и какими полномочиями будет обладать командование. Эти ключевые факторы позволят более готовым

силам выполнять операции Кибернетического командования США и Министерства обороны.

«Возвышение до суб-унифицированного командования на самом деле связано с тем, как мы будем работать со службами, чтобы гарантировать, что у нас есть нужные таланты в нужных местах», — сказал Хартман. «Речь идет о создании сил, которые могут двигаться быстрее, чем наши противники, потому что у нас есть правильный набор оборудования, правильные полномочия и правильные процедуры, которые действуют с ловкостью и скоростью».

Эволюция CNMF в киберпространстве

Создание CNMF в качестве объединенного командования также является показателем того, насколько быстро развивается киберпространство и как вместе с ним развивается Министерство обороны.

В 2010 году Киберкомандование было самым молодым объединенным командованием вооруженных сил. Теперь Киберкомандование было повышено до уровня боевого командования, а CNMF является новейшим объединенным военным командованием.

Проблемы в киберсфере постоянно растут как по количеству, так и по сложности. С момента официального выхода на полную мощность в 2018 году CNMF провела около 40 операций по поиску, тысячи удаленных кибероперациий и участвовала или реагировала почти на каждый кризис национальной безопасности, с которым сталкивались США.

«CNMF проводит операции полного спектра против противников, которые угрожают США и нашим союзникам и партнерам», — сказал Хартман. «Мы готовы защищать страну 24/7/365 в тесном сотрудничестве с нашими партнерами из США и их союзников».

Начиная с промежуточных выборов в США в 2018 году безопасность выборов стала главным приоритетом как для CNMF, так и для Агентства национальной безопасности. Это постоянное внимание в конечном итоге привело к созданию Малой группы по России, которая позже была преобразована в Группу по безопасности выборов.

«Russia Small Group была образцом будущего успеха, но также и катализатором», — сказал Хартман, который принял командование менее чем через год после промежуточных выборов 2018 года. «Это был катализатор, который стимулировал операции, которые мы проводили в течение последних нескольких лет».

С 2020 года Министерство обороны считает безопасность выборов постоянной миссией, которую возглавляет ESG.

Помимо защиты выборов в США с помощью ESG, CNMF пресек деятельность, связанную со взломом Microsoft Exchange, тесно сотрудничал с межведомственными партнерами, чтобы возложить расходы на участников, ответственных за инцидент с программой-вымогателем Colonial Pipeline, и поделился информацией об этих и других компрометациях, чтобы позволить партнерам для лучшей идентификации и защиты от киберугроз.

«В конце концов, все дело в людях, — сказал Накасоне.

«Преобразование CNMF в подчиненное командование отражает невероятную самоотверженность, профессионализм и приверженность членов подразделения, как в прошлом, так и в настоящем», — пояснил Хартман. «Мы очень гордимся вкладом всех, кто сделал это возможным»… ***(The Evolution of Cyber: Newest Subordinate Unified Command Is Nation's Joint Cyber Force // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/the-evolution-of-cyber-newest-subordinate-unified-command-is-nations-joint-cyber-force/). 03.01.2023).***

***

Кіберзахист критичної інфраструктури

«Королевская почта Великобритании обвиняет «кибер-инцидент» в нарушении обслуживания

Каждый раз, когда критическая инфраструктура выходит из строя, неизбежно возникает первый вопрос: была ли виновата кибератака?

Так было в среду, когда Федеральное авиационное управление США объявило о «наземной остановке», запретив взлет самолетов из-за отказа системы в течение ночи.

«ФАУ приказало авиакомпаниям приостановить все внутренние вылеты до 9 часов утра по восточному времени, чтобы агентство могло проверить достоверность информации о рейсах и безопасности», — сообщило в среду утром Федеральное управление гражданской авиации, входящее в состав Министерства транспорта.

Проблема заключалась в сбое в системе FAA для обмена информацией об опасностях и ограничениях в полете со всеми пилотами коммерческих авиакомпаний в режиме реального времени, называемой NOTAM, для «Уведомления о воздушных миссиях». Наземная остановка вызвала хаос в аэропортах США, поскольку пассажиры остались в затруднительном положении или задержались. Хотя самолеты в воздухе все еще могли приземлиться, сбои привели к задержке 6000 рейсов и отмене 1000, по данным отслеживающей компании FlightAware.

Белый дом быстро преуменьшил предположения о том, что сбои могли быть вызваны онлайн-атаками.

«Сегодня утром министр транспорта проинформировал президента об отключении системы FAA», — сообщила пресс-секретарь Карин Жан-Пьер в Twitter.

«На данный момент нет никаких доказательств кибератаки, но президент поручил DOT провести полное расследование причин. FAA будет предоставлять регулярные обновления», — добавила она.

Незадолго до 9 утра по восточному времени FAA прекратило наземную остановку.

«FAA определило, что система безопасности, затронутая ночным отключением, полностью восстановлена, и общенациональная наземная остановка

будет немедленно отменена», — сообщил министр транспорта Пит Буттиджич в Twitter в 8:55 утра по восточному времени.

«Я руководил процессом принятия мер, чтобы определить основные причины и рекомендовать следующие шаги», — добавил он.

Что в этом отчете о действиях указано как виновник сбоя NOTAM, еще предстоит выяснить.

Разрушение Королевской почты

Также в среду британская национальная почтовая служба Royal Mail сообщила клиентам, что «испытывает серьезные перебои в обслуживании наших международных экспортных служб после кибер-инцидента», и рекомендовала отложить попытки отправить какие-либо предметы за границу.

«Мы столкнулись с перебоями в работе наших международных экспортных служб и временно не можем отправлять товары за границу», — сообщили в Royal Mail. «Товары, которые уже были отправлены, могут быть задержаны. Мы хотели бы принести искренние извинения пострадавшим клиентам за любые сбои, вызванные этим инцидентом. Наши операции по импорту продолжают выполнять полный спектр услуг, с некоторыми незначительными задержками».

В нем добавлено: «Наши команды круглосуточно работают над устранением этого сбоя, и мы сообщим вам, как только у нас будет больше информации».

Кибератака Вопрос Дежавю

Любое необычное отключение или задержка в наши дни — не только в системах FAA, но и в британских аэропортах, перебои в энергосистеме, столкновение эсминца ВМС США с торговым танкером — кажется, немедленно вызывает вопрос: «Была ли это кибератака?» вопрос.

Как показывают эти инциденты, онлайн-атаки редко бывают виноваты.

До 2019 года ироничный веб-сайт Cyber Squirrel 1 отслеживал более 30 лет данных о 2524 глобальных отключениях электроэнергии. Только три из них могут быть приписаны людям в форме атак национального государства: отключение электроэнергии в Украине в 2015 и 2016 годах и Stuxnet, который был обнаружен в 2010 году и, по широко распространенному мнению, стал результатом проекта, проводимого Соединенными Штатами. Штаты и Израиль.

Что касается других отключений, главный виновник был ясен: белки, за которыми следовали птицы, змеи и еноты.

Между тем, для ИТ-отключений цифровая версия белки уже хорошо известна. «Это был DNS. Это всегда DNS», — написал в Твиттере эксперт по кибербезопасности Джейк Уильямс, бывший член группы атакующих хакеров Агентства национальной безопасности, о сбое системы FAA». ***(Mathew J. Schwartz. US Flights Resume After Reported Computer Glitch Resolved // Information Security Media Group, Corp. (https://www.govinfosecurity.com/blogs/us-flights-resume-after-reported-computer-glitch-resolved-p-3352). 11.01.2023).***

***

«К 2050 году солнечная генерация может обеспечить почти половину электроснабжения страны. Эти солнечные электростанции, в том числе силовые электронные устройства, которые взаимодействуют с системами управления и

автоматизации коммунальных предприятий, могут создавать серьезные проблемы с кибербезопасностью для работы энергосистемы. Пришло время полностью интегрировать солнечную энергетику в процессы планирования кибербезопасности и реагирования на инциденты в энергетическом секторе. Чтобы обеспечить эту интеграцию, Министерство энергетики США работает над повышением киберустойчивости солнечных технологий посредством исследований и разработок (НИОКР), а также путем установления стандартов и передового опыта, но солнечная промышленность также должна повысить свою осведомленность и зрелость в области кибербезопасности.

Кибербезопасность – главный приоритет

В отличие от систем корпоративных информационных технологий (ИТ), электроэнергетическая сеть представляет собой киберфизическую систему, которая подчиняется законам физики. Генерирующее, передающее и распределительное оборудование — это операционные технологии (ОТ), которые контролируют потоки электроэнергии в сети. Любые изменения в работе системы в результате преднамеренных манипуляций через ИТ и коммуникационные сети, такие как кибератаки, могут привести к повреждению оборудования ОТ и/или угрозе безопасности и здоровью. У опытных злоумышленников может быть возможность манипулировать группами физического оборудования, создавая аномальный поток энергии на большой территории и вызывая региональную нестабильность и серьезные сбои.

Коммунальные предприятия и операторы энергосистем сделали кибербезопасность одним из своих главных приоритетов. Сегодня крупномасштабные солнечные фотоэлектрические (PV) системы должны соответствовать стандартам защиты критической инфраструктуры Североамериканской корпорации по надежности электроснабжения (NERC), прежде чем они смогут работать. Тем не менее, небольшие фотоэлектрические системы и другие распределенные энергетические ресурсы (DER) — сегодня их количество исчисляется миллионами и быстро растет — в настоящее время не обязаны соответствовать стандартам кибербезопасности.

Устройства РЭР, такие как фотоэлектрические инверторы, взаимодействуют напрямую с системой управления энергоснабжения или опосредованно через агрегаторы РЭР. Обычно сообщения мониторинга и управления направляются через открытый Интернет. Также разрешен удаленный доступ к устройствам РЭР с облачных серверов. Хотя это обеспечивает удобство обслуживания оборудования и устранения неполадок, оно увеличивает уязвимость в энергосистеме. Во многих случаях солнечное фотоэлектрическое оборудование проектируется и производится за пределами Соединенных Штатов или использует коммерческие готовые компоненты, которые производятся во всем мире. Управление кибербезопасностью цепочки поставок является серьезной проблемой.

Комплексный подход

Министерство энергетики США уже много лет поддерживает исследования и разработки в области киберустойчивости для солнечных технологий. Эти усилия включают улучшение защиты и устойчивости кибербезопасности, уменьшение уязвимостей, разработку киберустойчивых технологий следующего поколения,

повышение ситуационной осведомленности, повышение зрелости кибербезопасности солнечных технологий и выявление возможностей для участия заинтересованных сторон солнечной энергии в реагировании на киберинциденты.

В этих усилиях мы использовали комплексный и совместный подход, опираясь на структуру кибербезопасности Национального института стандартов и технологий и используя Модель зрелости возможностей кибербезопасности Министерства энергетики. Во-первых, мы сотрудничали с Sandia National Laboratories (SNL) для разработки отчетов « Кибербезопасность для поставщиков DER, агрегаторов и операторов сетей » и « Дорожная карта для фотоэлектрической кибербезопасности ». Затем мы запустили несколько программ финансирования для поддержки разработки технологий, стандартов и инструментов оценки рисков для выявления, обнаружения, защиты, реагирования и восстановления после кибератак, уделяя особое внимание солнечным технологиям и технологиям DER.

Один успешный проект «Система упреждающего обнаружения и предотвращения вторжений» получил награду R&D100 в 2022 году. Эта команда под руководством SNL использует инструменты мониторинга вторжений и алгоритмы машинного обучения для выявления аномальных корреляций кибер- и физических событий, которые происходят на границе сети. В другом проекте, финансируемом Министерством энергетики, « Командование и управление прошивкой», используются передовые методы машинного обучения для создания базовой прошивки устройства DER и обнаружения необъяснимых изменений. Набор инструментов используется для анализа структурированных угроз и обмена информацией с вышестоящими операциями безопасности сети для принятия мер по предупреждению и смягчению последствий. Группу проекта возглавляют Национальная лаборатория Айдахо (INL) и Национальная лаборатория возобновляемых источников энергии (NREL).

В рамках нашего последнего сотрудничества с национальными лабораториями мы разрабатываем всеобъемлющую базу знаний и инструменты для устранения пробелов в кибербезопасности в солнечной промышленности — для проектирования оборудования, мониторинга на уровне завода и эксплуатации энергосистемы. Эти усилия уже привели к публикации Института инженеров по электротехнике и электронике (IEEE) 1547.3 проекта руководства и рекомендаций по сертификации для кибербезопасности распределенных энергетических ресурсов под руководством NREL и Underwriter Laboratories. Эти инструменты поддерживают ежегодный университетский конкурс CyberForce, который в этом году представляет собой смоделированную кибератаку на новую солнечную установку перспективного производителя электромобилей. Кроме того, управление солнечной энергетики Министерства энергетики также объединилось с Национальной ассоциацией государственных энергетических управлений, Национальной ассоциацией уполномоченных по надзору за коммунальными предприятиями и Ассоциацией производителей солнечной энергии, чтобы повысить с осведомленность о кибербезопасности и поделиться передовым опытом лицами, принимающими решения, чтобы солнечная энергетика стала одним из самое безопасное топливо в сети.

Обеспечение безопасности будущей сети

Чтобы справиться с последствиями изменения климата, электросеть США должна интегрировать большое количество возобновляемой энергии, такой как солнечная и ветровая. Эти усилия будут ускорены недавним принятием Закона об инвестициях в инфраструктуру и рабочих местах, а также Закона о снижении инфляции. Кроме того, потребители электроэнергии будут продолжать внедрять интеллектуальные энергетические устройства, включая интеллектуальное освещение и термостаты, которые смогут взаимодействовать с солнечными батареями на крыше, электромобилями и многим другим. Эти усилия имеют решающее значение для борьбы с изменением климата и обеспечения устойчивости до, во время и после крупных событий. Однако по мере того, как электросеть США претерпевает эти изменения, важно обеспечить, чтобы кибербезопасность была встроена в новые устройства, системы и инфраструктуру, а «безопасность по замыслу» была основным компонентом этих систем.

В недавно опубликованном отчете «Вопросы кибербезопасности для распределенных энергетических ресурсов в электросети США» Министерство энергетики дает обзор проблем кибербезопасности, которые следует учитывать в электроэнергетическом секторе, включая коммунальные предприятия и операторов распределенных энергетических ресурсов (DER), поставщиков, интеграторов., разработчиков и поставщиков (совместно именуемых «отрасль DER»), а также политиков, поскольку мы приступаем к этим трансформационным изменениям в электросети США. Хотя этот отчет не претендует на всесторонний обзор соображений кибербезопасности в отрасли DER, он способствует более глубокому обсуждению между отраслью DER, федеральными и местными органами власти и другими заинтересованными сторонами…» ***(Taking on solar's cybersecurity challenges // Renewable Energy World® (https://www.renewableenergyworld.com/solar/taking-on-solars-cybersecurity-challenges/). 03.01.2023).***

***

«Морская отрасль играет жизненно важную роль в мировой экономике, при этом на судоходство приходится до 90 процентов мировой торговли. К сожалению, морской сектор сталкивается с огромной проблемой: киберпреступностью, говорит Ричард Менир, генеральный директор Burning Tree.

Быстрая цифровизация основных функций принесла много преимуществ морякам и морским властям, но также создала сеть уязвимостей, которыми могут воспользоваться киберпреступники. А с нашими последними данными, указывающими на значительное увеличение еженедельных киберсобытий на 400%, цифровая безопасность, вероятно, создаст серьезные проблемы для всех основных перевозчиков в 2023 году и далее.

Итак, что стоит за постоянно растущим списком киберугроз, с которыми сталкивается морская отрасль, и каковы основные соображения по снижению киберрисков в этом секторе?

Причины морской киберпреступности

Морской сектор быстро принял цифровую трансформацию, развернув передовые технологии, такие как искусственный интеллект (ИИ) и Интернет вещей (IoT), для повышения эффективности, сокращения выбросов углерода и обеспечения безопасности судов и их грузов.

Однако чем больше морское оборудование интегрируется с технологиями, тем больше потерь в случае взлома. Хакеры хорошо знают об этой цифровой зависимости и используют ее для разрушения критически важных инфраструктур, запуская бесконечный шквал фишинговых атак и атак программ-вымогателей на уязвимые системы.

Угроза морской кибербезопасности усилилась за последний год после вторжения России в Украину. Базирующиеся в России киберпреступники и государственные деятели усердно работают над улучшением своих возможностей, обмениваясь передовым кибероружием для нарушения связи и ведения кибершпионажа по всему миру.

Что еще хуже, растущая взаимосвязанность глобальных цепочек поставок создает новые уровни риска. Если одна щель будет скомпрометирована, последствия могут быть далеко идущими. Например, кибератака на Transnet, крупнейшего портового оператора Южной Африки, привела к отключению нескольких портовых систем по всей стране. Нарушение привело к неделям простоя и стоило миллионы долларов.

Несмотря на эти угрозы, многие организации по-прежнему полагаются на устаревшие, неподдерживаемые операционные системы для выполнения критически важных функций — от управления грузами до навигации. А поскольку промышленный Интернет вещей (IIoT) связывает устройства с высокой степенью риска с бесчисленным множеством других в одной сети, хакеры получают новые шлюзы для расширения своей досягаемости.

В современном технически подкованном мире почти каждый может остановить кибероперации. Таким образом, морские и оффшорные власти не теряют времени впустую, чтобы принять превентивные меры с целостным подходом к управлению киберрисками.

Возобновление киберусилий в морском секторе

В связи с высокой инфляцией и геополитической напряженностью, сокращающей морские перевозки, многие судоходные перевозчики будут избегать инвестиций в кибербезопасность, чтобы сократить расходы, оставляя незащищенными значительное количество систем. Таким образом, в то время как индустрия кибербезопасности борется с нехваткой рабочей силы, моряки и морские организации должны оценивать динамические риски и восполнять пробелы в навыках, чтобы обеспечить безопасность и непрерывность морских операций.

Международная морская организация (IMO) и другие регулирующие органы приняли несколько законодательных актов для повышения цифровой безопасности в морской среде. Например, в январе 2021 года вступила в силу Резолюция ИМО MSC.428(98), требующая от судовладельцев и менеджеров обеспечения включения управления киберрисками в системы управления безопасностью судов.

Однако, чтобы эти политики были эффективными, моряки должны начать рассматривать кибербезопасность как коллективную ответственность. От 80 до

90% кибератак связаны с человеческими ошибками, что делает обучение и осведомленность одним из основных элементов защиты отдельных лиц, организаций и инфраструктуры от киберпреступлений.

В более широком масштабе отрасль требует действий, выходящих за рамки защиты национальных и организационных интересов. Морская отрасль нуждается в цифровой полиции в международном масштабе, чтобы перекрыть финансирование киберпреступникам и предотвратить разработку ими вредоносного программного обеспечения до того, как оно сможет представлять угрозу.

Мы рады, что многие судоходные компании сотрудничают с западными директорами по информационной безопасности (CISO), чтобы сделать эти угрозы более заметными. Тем не менее, мы надеемся, что организации будут развивать эти отношения на новых территориях, не забывая при этом о потенциальных угрозах». ***(Maritime cyber security // professional security magazine (https://www.professionalsecurity.co.uk/news/transport/maritime-cyber-security/). 16.01.2023).***

***

«Атаки кибербезопасности на критически важную инфраструктуру растут, особенно учитывая значительные потенциальные негативные последствия, которые такие атаки могут вызвать как для внутренней, так и для мировой экономики страны. Одной из самых известных угроз кибербезопасности, с которыми в настоящее время сталкиваются организации, является программа-вымогатель, представляющая собой тип вредоносного программного обеспечения, которое угрожает опубликовать активы данных жертвы или заблокировать доступ к ключевым сетям жертвы или связанной с ней инфраструктуре, если не будет заплачена существенная сумма денег. В первой половине 2021 года глобальные атаки программ-вымогателей увеличились на ошеломляющие 151%. Инциденты с программами-вымогателями могут разрушить организации, нарушив их критически важные операции в той мере, в какой они зависят от сетевого и системного подключения.

В Канаде горнодобывающая промышленность уже давно вносит основной вклад и поддерживает критически важную инфраструктуру за счет производства сырья, используемого для создания необходимого оборудования и товаров. В результате риск кибератак на предприятия, работающие в горнодобывающей отрасли, высок. Угроза для предприятий, работающих в горнодобывающей промышленности, часто усугубляется из-за их высокой степени зависимости от технологий в их бизнес-операциях, их потребности в постоянной и надежной связи с удаленными местами, а также того факта, что полезные ископаемые, добываемые в сами по себе, но они часто являются ключевыми полезными ископаемыми в производстве ключевых технологий во всем мире. Недавно было несколько громких атак программ-вымогателей, в том числе широко разрекламированные атаки на Nvidia, Kaseya и Colonial Pipeline. Затем, 27 декабря 2022 года, компания Copper Mountain Mining стала объектом атаки программы-вымогателя, которая

привела к остановке шахты на юге Британской Колумбии почти на неделю и немедленному падению цены их акций на 5,5%.

Воздействие атак на кибербезопасность

Атаки программ-вымогателей часто приводят к полной остановке бизнес-операций, что делает такие атаки одной из самых разрушительных форм киберпреступности для горнодобывающих организаций. Отключение ключевых операционных систем, систем безопасности и обработки может нанести значительный экономический ущерб горнодобывающему бизнесу, который, в сочетании с тем фактом, что такие атаки могут также нанести ущерб, уничтожить или привести к раскрытию конфиденциальных данных (включая личную информацию), последствия являются серьезными для бизнеса, пострадавшего от атаки программ-вымогателей. В дополнение к этим немедленным последствиям атаки программ-вымогателей могут иметь долгосрочные последствия для бизнеса, включая потерю доверия, негативное общественное восприятие, повышенные риски для бренда и беспокойство инвесторов.

На высоком уровне инциденты кибербезопасности, такие как атаки программ-вымогателей, могут привести к серьезным финансовым, нормативным и операционным проблемам для бизнеса, в том числе:

Компрометация ключевых информационных активов, включая конфиденциальную информацию, личную информацию, коммерческую тайну и ключевую интеллектуальную собственность;

Операционные сбои, вызванные блокировкой важных информационных систем;

Регуляторный контроль, включая жалобы и расследования;

Возможная гражданско-правовая ответственность; и

Требование вымогательства со стороны злоумышленников.

Поскольку эти воздействия настолько серьезны для организации, многие предприятия, которые подвергаются атаке программ-вымогателей, готовы заплатить выкуп, чтобы восстановить работу как можно быстрее. Однако выплата выкупа не обязательно предотвращает эти последствия. Недавний опрос канадских предприятий показал, что только 42% организаций, заплативших выкуп, полностью восстановили свои данные. В свете этих рисков горнодобывающим организациям требуются надежные средства защиты и процессы кибербезопасности, а также надежные программы соблюдения конфиденциальности, чтобы снизить риск любых инцидентов кибербезопасности.

Реагирование на инциденты кибербезопасности

Горнодобывающие компании должны проявлять инициативу в разработке планов и процессов как для защиты от кибератаки, так и для четкого определения шагов, которые необходимо предпринять в ответ на кибератаку. Хотя невозможно устранить риск кибератаки, организации могут свести к минимуму свою уязвимость и влияние, которое такие атаки могут оказать на них, расставив приоритеты при планировании реагирования на инциденты. Например, каждая организация должна, как минимум:

Определите ключевых членов своей группы реагирования на инциденты и то, как и когда они будут общаться в случае кризиса;

Проведите инвентаризацию конфиденциальных и закрытых данных в системах организации (или которые могут находиться у сторонних поставщиков услуг) и связанных с ними юридических обязательств, которые могут применяться в случае компрометации таких данных;

Обеспечьте наличие важных политик и процедур, которые помогут ограничить воздействие в случае кризиса (например, надлежащая политика хранения и уничтожения документов); и

Рассмотрите возможность внедрения страхового покрытия кибер-рисков.

Реагирование на инциденты кибератаки должно быть сосредоточено как на немедленной, так и на долгосрочной защите вашей организации. Соответствующие функции плана реагирования на инциденты будут варьироваться в зависимости от уникальных потребностей и обстоятельств каждой организации. Ответы могут быть сосредоточены на:

Предоставление своевременных и эффективных услуг по реагированию на инциденты, связанные с инцидентами кибербезопасности, включая атаки программ-вымогателей, отслеживание сотрудников, неверные электронные письма и другие инциденты;

Рекомендация и внедрение стратегии отчетности и уведомления для соблюдения юридических обязательств и снижения риска судебных разбирательств; и

Подготовка внутренних заявлений, публичных ответов и часто задаваемых вопросов для снижения риска судебных разбирательств и проблем с репутацией.

Заключение

По мере того, как атаки программ-вымогателей развиваются и становятся все более изощренными с развитием новых технологий, атаки будут оставаться вездесущей угрозой для всех предприятий, особенно для тех, кто работает в горнодобывающей отрасли. Макмиллан может помочь горнодобывающим компаниям в разработке стратегий предотвращения инцидентов кибербезопасности и подготовки к ним, а также оказать поддержку в реагировании на инциденты». ***(Robert Piasentin, Mitch Koczerginski, Kristen Shaw, Gemma Walsh. Cybersecurity Threats to the Canadian Mining Industry: Is your Business Ready? // McMillan LLP (https://mcmillan.ca/insights/cybersecurity-threats-to-the-canadian-mining-industry-is-your-business-ready/). 10.01.2023).***

***

Кіберзахист закладів охорони здоров'я

«Совокупный законопроект о расходах на сумму 1,7 триллиона долларов, подписанный на прошлой неделе президентом Джо Байденом, содержит новые требования к кибербезопасности для медицинских устройств, которые меняют правила игры для укрепления безопасности в экосистеме здравоохранения, говорит доктор Сюзанна Шварц из Управления по санитарному надзору за качеством пищевых продуктов и медикаментов США.

«После многих лет информирования экосистемы о том, насколько важна кибербезопасность для безопасности пациентов и безопасности критической инфраструктуры здравоохранения и общественного здравоохранения, мы теперь получили подтверждение и признание ее критичности, приняв закон», — говорит Шварц, директор. из Управления стратегического партнерства и технологических инноваций в Центре устройств и радиологического здоровья FDA.

Многие положения, включенные в новый закон — Закон о сводных ассигнованиях от 2023 года — в целом отражают действия, к которым FDA уже призывало производителей медицинского оборудования для обеспечения кибербезопасности своей продукции.

Подобные предложения также содержались в нескольких предыдущих законопроектах, направленных на повышение кибербезопасности медицинских устройств, таких как закон PATCH в прошлом году, которые не получили поддержки в качестве отдельных законопроектов…

Но теперь, в соответствии с новым законом, производители в своих продуктах, подаваемых в FDA, должны включать достаточные доказательства способности устройства обновляться и устанавливать исправления, а также средства контроля и тестирования его безопасности, а также предоставлять спецификацию программного обеспечения для коммерческого использования. компоненты с открытым исходным кодом и готовые программные компоненты.

«Это необходимо заранее», — говорит Шварц в интервью Information Security Media Group.

Безопасность жизненного цикла

Хотя закон относится к новым продуктам, «эти меры, принятые на ранних стадиях, позволят нам иметь гораздо более безопасные устройства на протяжении всего жизненного цикла, поскольку эти устройства остаются на рынке и находятся в клиническом использовании — в отличие от того, что мы в настоящее время face, которые, честно говоря, было очень сложно обновить или исправить безопасным способом», — говорит она.

«Несмотря на то, что мы снова и снова говорили, что кибербезопасность медицинских устройств не является факультативной и не добровольной, до сих пор у нас никогда не было силы закона, действующего законодательства, требующего от производителей заниматься кибербезопасностью медицинских устройств», — говорит она.

«Установление этой связи между разумными гарантиями безопасности и эффективности медицинских устройств и кибербезопасностью медицинских устройств — это очень важно для нас», — говорит она.

По словам Шварца, в прошлом FDA использовало свои «неявные полномочия» посредством регулирования системы качества, чтобы помочь улучшить состояние экосистемы для кибербезопасности.

«Теперь у нас есть явные полномочия и надзор за этим. Это масштабный сдвиг, и мы очень рады тому, что нас ждет в будущем».

Законодательство также предоставляет FDA финансирование в размере 5 миллионов долларов для поддержки его расширенных усилий по регулированию кибербезопасности медицинских устройств.

В этом аудиоинтервью с Information Security Media Group Шварц также обсуждает:

Ключевые выводы для производителей медицинского оборудования и организаций, предоставляющих медицинские услуги, относительно потенциального воздействия недавно принятого закона и соблюдения FDA новых требований кибербезопасности медицинских устройств;

Будущее обновленного проекта руководства FDA по кибербезопасности предпродажных медицинских устройств, выпущенного в апреле прошлого года;

Как новый закон согласуется с указом президента Байдена от 2021 года об укреплении кибербезопасности в федеральном правительстве, а также с последствиями других важных положений о безопасности, содержащихся в законодательстве.

Шварц поддерживает программу FDA по кибербезопасности медицинских устройств, которая включает в себя повышение осведомленности, обучение и проведение разъяснительной работы, партнерство и создание коалиций в секторе здравоохранения и общественного здравоохранения, а также содействие сотрудничеству между другими государственными учреждениями и частным сектором. Она также возглавляет рабочую группу CDRH по кибербезопасности, которой поручено сформулировать политику FDA в отношении кибербезопасности медицинских устройств, и была сопредседателем правительственного координационного совета по сектору здравоохранения и критической инфраструктуры общественного здравоохранения». ***(Marianne Kolbasuk McGee. Exclusive: FDA Leader on Impact of New Medical Device Law // Information Security Media Group, Corp. (https://www.govinfosecurity.com/interviews/exclusive-fda-leader-on-impact-new-medical-device-law-i-5216). 04.01.2023).***

***

Захист персональних даних та соціальні мережі

«…В 2022 году организации США выпустили 1802 уведомления об утечке данных, сообщая о раскрытии записей или личной информации, затрагивающих более 400 миллионов человек, сообщает Ресурсный центр по краже личных данных.

Эта цифра всего на 60 нарушений меньше, чем 1862 нарушения в США, которые ITRC насчитал в 2021 году.

«Хотя в прошлом году мы не установили рекорд по количеству скомпрометированных данных в США, мы приблизились к этому», — говорит Ева Веласкес, президент и главный исполнительный директор ITRC.

Этот промах произошел, несмотря на заметное снижение объемов утечки данных в первой половине 2022 года. Веласкес говорит, что российские преступники, вероятно, были слишком отвлечены или озабочены вторжением их страны в Украину, а также волатильностью на рынке криптовалют. Во второй половине года объем нарушений снова начал расти.

В число организаций, совершивших самые крупные известные взломы в 2022 году, вошли Twitter, где было раскрыто 222 миллиона записей; Neopets с 69 миллионами жертв; AT&T Data с 23 миллионами жертв; и Cash App Investing с 8,2 миллионами жертв.

Судя по сообщениям о взломах, наиболее часто раскрываемыми атрибутами были имена жертв, за которыми следовали номера социального страхования, даты рождения, текущие домашние адреса, водительские права или идентификационные номера штата, медицинские данные и номера банковских счетов.

Ведущий вектор взлома: онлайн-атаки

Организации, подвергшиеся взлому, сообщили, что универсальная категория «онлайн-атак» была основной причиной утечки данных в 2022 году, за ней следовали фишинг или компрометация деловой электронной почты, а затем программы-вымогатели и вредоносные программы. Все это далеко от 2005 года, когда ITRC сообщил, что главными виновниками были утерянные бумажные записи или ленты с резервными копиями, а также утерянные или украденные ноутбуки.

Прозрачность и занижение отчетности продолжают оставаться серьезными проблемами для оценки истинного масштаба эпидемии утечки данных. В прошлом году организации в совокупности насчитали 422 миллиона человек, пострадавших от взлома. Но 68% всех уведомлений о нарушениях не включали подсчет того, сколько людей пострадало или как они были затронуты. Кроме того, 42% не указали подробности атаки.

«Если вы объедините эти две статистические данные вместе, у нас будет только 34% уведомлений об утечке данных, которые содержат информацию, по которой можно действовать», — говорит Джеймс Ли, главный операционный директор ITRC.

«Это привело к тому, что данные стали менее надежными, что мешает потребителям, предприятиям и государственным учреждениям принимать обоснованные решения о риске компрометации данных и действиях, которые необходимо предпринять в случае их воздействия», — говорит Веласкес.

Другие организации, особенно в тех же секторах, что и организация-жертва, или с аналогичной ИТ-инфраструктурой, часто используют отчеты о взломе, чтобы собрать самую свежую информацию об угрозах, чтобы лучше защитить себя.

Недостаток информации также мешает жертвам-потребителям узнать, с каким риском они сталкиваются. Это одна из целей законов штатов об уведомлении об утечке данных: предоставить потребителям полезную информацию, которую они могут использовать для защиты себя, после того как организации, хранящие их личные данные, в конечном итоге раскроют их личную информацию.

По словам Ли, особенно в эпоху, когда усталость от взлома данных стала обычным явлением, неспособность расширить возможности потребителей подвергает их большему риску.

Предоставление им таких подробностей позволяет им понять, «это что-то, что им нужно принять немедленно, чтобы защитить себя, или это что-то, что может подождать день или два, или, может быть, им вообще не нужно ничего делать», —

говорит он. «Без такого рода информации, сообщаемой в этих уведомлениях об утечке данных, никто не знает, что делать, и это увеличивает риск, и это очень, очень тревожная тенденция». ***(Mathew J. Schwartz. Reported Data Breaches in US Reach Near-Record Highs // Information Security Media Group, Corp. (https://www.govinfosecurity.com/reported-data-breaches-in-us-reach-near-record-highs-a-21018). 25.01.2023).***

***

«…Более 4 миллиардов человек имеют аккаунты в Facebook и Instagram, что делает их самыми популярными социальными сетями на планете. Участники делятся фотографиями, жизненными событиями и мнениями, чтобы привлечь подписчиков, построить бизнес и оставаться на связи с друзьями и семьей. Но у этих социальных платформ есть и более темная сторона.

Жалобы на захват учетных записей в социальных сетях в Ресурсный центр по краже личных данных подскочили более чем на 1000% в прошлом году. Кража, выдача себя за другое лицо и поддельные учетные записи в Facebook и Instagram — социальных свойствах Meta — подпитывают массовый рост мошенничества и незаконной деятельности. Фактически, федеральные власти говорят, что около 50% случаев захвата учетных записей сегодня происходят из социальных сетей.

«У нас есть все эти платформы, но кто позаботится о вашей безопасности? Кто позаботится о вашей конфиденциальности? – Крис Ингрэм, писатель, бывший радиоведущий и жертва кражи личных данных Facebook.

«Эти мошенничества в социальных сетях являются большей частью основных мошенничеств, которые мы наблюдаем», — говорит Стивен Догерти, следователь по финансовому мошенничеству из Секретной службы США. «Мы наблюдаем, как многие выдают себя за других в социальных сетях и дезинформируют в социальных сетях, которые используются для совершения мошеннических действий, таких как мошенничество с романтическими отношениями, которые, как мы все знаем, очень и очень сказываются на вовлеченных жертвах, потому что они не только обычно несут финансовые потери, но и часто их можно подставить и использовать в качестве денежных мулов для совершения более крупных кибер- и даже финансовых преступлений, таких как компрометация деловой электронной почты».

Инвестиции в криптовалюту в наши дни являются обычным мошенничеством в социальных сетях, что приводит к новому повороту в разделке свиней, который обычно начинается с контакта в социальных сетях и часто включает элементы романтического мошенничества. Власти США в ноябре конфисковали семь поддельных доменов веб-сайтов, которые использовались для того, чтобы обманом заставить пять жертв инвестировать 10 миллионов долларов в криптоактивы, которые просто исчезли.

Растущие угрозы банкам

Личные данные о клиентах, находящиеся в свободном доступе на Facebook и Instagram, уже давно используются для «заполнения границ» о жертвах, чтобы облегчить захват банковских счетов, но растущая тенденция заключается в

использовании этой информации для открытия новых учетных записей для банковского мошенничества и кражи правительства. Преимущества, говорит Джеймс Ли, главный операционный директор Ресурсного центра по краже личных данных. По его словам, переход к цифровому банкингу и открытию онлайн-счетов усугубил проблему.

«Никто никогда не посмотрит на вас. Вы не будете находиться в физическом присутствии человека, когда будете открывать эти счета», — говорит Ли в Information Security Media Group. «Итак, эта учетная запись теперь настроена, и вы, человек, чья информация была использована, совершенно не подозреваете, что кто-то открыл учетную запись на ваше имя. В первый раз вы узнаете, когда, месяцы спустя, в зависимости от о типе счета, который они открывают, когда вы получаете какое-либо уведомление от финансового учреждения, то есть документ, который вы должны подать в свои налоги».

Каждый крупный банк США тратит не менее 1 миллиарда долларов в год на кибербезопасность и обнаружение мошенничества, но Американская ассоциация банкиров признает, что мошенничество в социальных сетях приносит отрасли значительные убытки.

«Я думаю, что это проблема для всех», — говорит Пол Бенда, старший вице-президент по операционным рискам и кибербезопасности Американской ассоциации банкиров. «Когда вы смотрите на это, очевидно, что это человек, чья личность украдена. Это ужасная вещь. Они стали жертвой мошенников. сделать вас целым, так что банк также является жертвой, потому что им приходится платить много из этих вещей. И поэтому у нас есть проблема: это должен быть совместный ответ. Потребители должны попытаться обучить себя на «Каковы красные флажки?» И банки ежегодно тратят миллиарды долларов, пытаясь идентифицировать эти вещи в фоновом режиме с помощью предупреждений о мошенничестве,

Кража учетных данных Facebook поразила 500 миллионов пользователей

Автоматизированные инструменты позволяют злоумышленникам компрометировать огромное количество учетных записей в социальных сетях. Исследователи из фирмы по кибербезопасности PIXM отслеживают единственную кампанию, активную в Facebook с 2021 года, в ходе которой были украдены учетные данные полумиллиарда пользователей, и их число продолжает расти. Мошенник из Колумбии хвастался, что заработал 60 миллионов долларов на кликах по рекламе.

Кража учетных данных начинается с фишингового электронного письма через Facebook Messenger, которое приходит от «друга» и спрашивает: «Это ты на этом видео? Тебе лучше удалить его». По словам Ника Асколи, вице-президента по исследованию угроз в PIXM, большинство пользователей Facebook нажимают на ссылку, и это запускает атаку «человек посередине» с поддельной страницей входа в Facebook для кражи учетных данных.

«Что они будут делать с вашими учетными данными Facebook, так это программно с помощью своих собственных ботов войти в вашу учетную запись Facebook, а затем сделать то же самое — распространить одну и ту же ссылку на все ваши контакты Facebook Messenger», — говорит Асколи.

В то время как основной мотивацией колумбийского злоумышленника является получение дохода от рекламы путем подключения к законным рекламным и вредоносным сервисам, этот процесс показывает, насколько легко обмануть защиту электронной почты Facebook Messenger и украсть учетные данные. Асколи отслеживает переходы из Messenger на ряд поддельных веб-сайтов, используемых хакером. Сайты являются поддоменами Hubspotpagebuilder.eu, законной службы веб-хостинга.

Как только пользователь нажимает на фишинговую ссылку, он перенаправляется на страницу, которая отображает страницу с ошибкой «404» менее 1 секунды. Затем он перенаправляет пользователей на поддельную страницу входа в Facebook, требуя от них предоставить свои учетные данные. После захвата учетных данных пользователь перенаправляется на пустую страницу видео с другими ссылками на поддельный контент. По словам Асколи, за кулисами хакер обслуживает от 10 до 15 рекламных страниц и получает около 15 центов за клик.

«Когда защитная технология загружает эту страницу, она не видит ничего подозрительного: она видит страницу 404, не предлагающую ничего — ничего необычного на ней, никакого подозрительного JavaScript, никаких подозрительных встроенных элементов — и она разрешает сеанс для пользователя. продолжайте», — говорит Асколи.

Процесс восстановления учетной записи «смехотворен»

Одна из самых больших проблем с захватом учетных записей на Facebook заключается в том, что жертвам трудно, если вообще возможно, восстановить свои учетные записи. Возьмем, к примеру, Криса Ингрэма, писателя и бывшего радиоведущего. Он не был активным пользователем Facebook, но однажды он получил электронное письмо от своей бывшей жены, которая хотела знать, почему он пытался продать ей криптовалюту.

«Я пошел и проверил свою учетную запись Facebook и не смог войти в нее», — говорит Ингрэм. «Он сказал, что мой пароль был ложным. Он сказал, что это не моя учетная запись Facebook. И даже когда я попытался пройти через резервную копию — мой номер телефона и тому подобное, он не позволил мне войти».

Ингрэм сообщил о краже учетных данных онлайн в Meta, и примерно через 10 дней он получил уведомление от системы, в котором говорилось, что человек, выдающий себя за него, не «нарушал стандарты сообщества». Не сумев с Метой связаться с реальным человеком, он сообщил о краже еще несколько раз — с тем же результатом.

«На самом деле это смехотворно, — говорит он. «Тем временем мои друзья получают электронные письма с попытками продать им все, от биткойнов до отпуска на Арубе».

Ли из Ресурсного центра по краже личных данных говорит, что кража учетных данных — обычная проблема для пользователей Facebook и Instagram. В большинстве случаев, по его словам, пользователи просто отказываются от попыток восстановить свою учетную запись.

«Они не могут пройти через системы, созданные платформами для решения этих проблем, которые, по большому счету, не связаны с настоящим человеком, что расстраивает людей и отталкивает их», — говорит Ли. «Ответы, которые вы

получаете от организаций по такого рода проблемам, в основном таковы: «Если бы нам потребовалась дополнительная проверка на внешнем интерфейсе, если бы нам потребовалась универсальная многофакторная аутентификация, если бы нам потребовались другие виды процессов, которые упростили бы доказательство того, что фактического владельца учетной записи выгнали, что это каким-то образом сделает систему либо менее безопасной, либо более обременительной, либо это будет невыполнимо с точки зрения затрат ». Это отговорки, это не законные причины».

Но за каждым захватом аккаунта стоят человеческие жертвы, которые невозможно измерить. Например, пока Ингрэм пытался восстановить свой аккаунт, умер его 32-летний сын, и он не смог поговорить с многочисленными друзьями о своей утрате.

«Я пытался связаться с друзьями, которые любили его и которые могли бы захотеть узнать об этом, и, честно говоря, которые могли бы утешить меня в то время, но я не мог связаться с ними», — говорит Ингрэм. «Я не мог установить те связи, которые, честно говоря, теперь стали через Интернет, которые раньше были более плотскими и личными. Очевидно, по большому счету, невозможность связаться с людьми на Facebook — это не конец мир. Но это был всего лишь один дополнительный мучительный удар в живот, который, честно говоря, только сделал это еще более раздражающим».

Meta, материнская компания Facebook и Instagram, не ответила на запросы об интервью с Information Security Media Group. В декабре Натаниэль Глейхер, глава отдела политики безопасности Meta, заявил, что социальная платформа улучшила средства контроля безопасности для предотвращения фишинга и запустила новую функцию онлайн-чата, которая помогла более чем 1 миллиону человек в девяти странах восстановить свои учетные записи.

Meta говорит, что пользователи обычно сталкиваются с проблемами при восстановлении учетной записи, когда у них есть неполная или устаревшая контактная информация, а гигант социальных сетей говорит, что 1 из 4 поглощений учетной записи происходит, когда контактная информация скомпрометирована. Ранее в этом месяце Meta подала в суд на поставщика услуг парсинга по найму и закрыла 60 000 поддельных учетных записей.

Однако такие пользователи, как Ingram, говорят, что Meta обязана делать больше перед участниками.

«Приоритетом должна быть безопасность», — говорит он. «Если вы собираетесь открыть компанию, которая будет предоставлять такого рода услуги, вашим приоритетом номер один должны быть в первую очередь конфиденциальность и безопасность, а затем все остальное. К сожалению, я думаю, что у нас определенно стоит телега впереди лошади. У нас есть все эти платформы, но кто позаботится о вашей безопасности? Кто позаботится о вашей конфиденциальности?

Эксперты предупреждают пользователей быть еще более бдительными, но некоторые говорят, что федеральное правительство может помочь переломить ситуацию. По словам Ли, одним из важных шагов в правильном направлении может стать национальный закон об утечке данных, который требует от

организаций сообщать о том, что произошло, и о том, какие действия предпринимаются для устранения проблемы.

«Личная конфиденциальность, кибербезопасность, конфиденциальность бизнеса, безопасность бизнеса — все эти вещи теперь переплетены таким образом, которого мы никогда не видели в истории, — говорит Ли. — Это один из лучших способов справиться с этим и начать процесс добиться реального прогресса в сокращении числа жертв преступлений против личности». ***(Anna Delaney. Facebook, Instagram Blasted for 'Lame' Security Practices // Information Security Media Group, Corp. (https://www.govinfosecurity.com/facebook-instagram-blasted-for-lame-security-practices-a-21022). 26.01.2023).***

***

«Неавторизованная сторона получила доступ к API компании примерно на 6 недель

Третий по величине оператор беспроводной связи в США сообщил в четверг федеральным регулирующим органам, что обнаружил злоумышленника, который перекачивал идентифицирующую информацию 37 миллионов клиентов.

T-Mobile, название, принятое компанией, появившейся после слияния телекоммуникационных компаний Sprint и T-Mobile US в 2020 году, минимизировало влияние нарушения при подаче заявки в Комиссию по ценным бумагам и биржам. По словам компании, взлом не связан ни с платежными картами, ни с правительственными идентификаторами, ни с паролями. У телекоммуникационной компании Bellevue, штат Вашингтон, более 110 миллионов клиентов.

Он обнаружил интерфейс прикладного программирования, который раскрывал данные, включая имена, адреса электронной почты, номера телефонов и даты рождения, как источник взлома. Хакеры не получили полный набор данных о каждом из 37 миллионов пострадавших, добавил он. Затронуты клиенты с предоплатой и подпиской; хакеры также получили данные, включая количество линий на счете и особенности тарифного плана.

Хакеры имели доступ к API в течение примерно шести недель, пока сотрудники компании не обнаружили и не закрыли доступ к интерфейсу извне 5 января. В отдельном пресс-релизе говорится, что время от обнаружения инцидента до его разрешения составило менее 24 часов.

Хотя утечка данных, таких как номера телефонов и адреса электронной почты, не так опасна, как утечка финансовых счетов, они все же могут представлять угрозу для потребителей, особенно если злоумышленники знают, что информация является свежей и, следовательно, может быть достоверной. Риск попыток фишинга и кражи личных данных обычно возрастает после утечки данных, даже если у киберворов нет такой информации, как пароли.

Всего несколько месяцев назад перевозчик заключил мировое соглашение на сумму 350 миллионов долларов в связи с утечкой личных данных в 2021 году, затронувшей 77 миллионов клиентов. В рамках мирового соглашения компания обязалась потратить не менее 150 миллионов долларов на улучшение своей кибербезопасности.

В нормативной документации, поданной в четверг, говорится, что в 2021 году компания начала «существенные многолетние инвестиции» в кибербезопасность, и утверждается, что на сегодняшний день компания «добилась существенного прогресса».

Тем не менее, инцидент может в конечном итоге стоить компании значительных расходов, заявили в T-Mobile». ***(David Perera. T-Mobile Says Hackers Stole Data of 37 Million Customers // Information Security Media Group, Corp. (https://www.govinfosecurity.com/t-mobile-says-hackers-stole-data-37-million-customers-a-20984). 19.01.2023).***

***

«…Французское агентство по защите данных наложило штраф в размере 5 миллионов евро на платформу коротких видео социальных сетей TikTok, заявив, что китайская компания нарушила национальный закон о конфиденциальности, ограничивающий мониторинг активности веб-браузера.

Расследование, проведенное Национальной комиссией по информатике и свободе, известной как CNIL, показало, что веб-приложение TikTok побуждает пользователей включать отслеживающие файлы cookie.

Проверка веб-платформы в середине 2021 года показала, что TikTok позволял французским пользователям принимать все файлы cookie одним щелчком мыши, но заставлял их нажимать несколько раз при отклонении дополнительных файлов cookie.

Большинству веб-сайтов для работы требуются текстовые файлы, известные как файлы cookie, поскольку в противном случае они не могут поддерживать непрерывность пользователя от одного клика до другого — результат решений в области интернет-дизайна, принятых десятилетия назад, которые рассматривают каждое соединение от пользователя к серверу, как если бы это было совершенно новый.

Европейские правительства стремились разрешить потребителям отказываться от файлов cookie, которые отслеживают действия пользователей исключительно в целях онлайн-рекламы. TikTok, у которого в среднем около 1 миллиарда пользователей в месяц по всему миру, стал новым рекламным гигантом в Интернете благодаря отслеживанию файлов cookie на своем собственном веб-сайте и сторонних веб-сайтах.

В феврале 2022 года TikTok представил кнопку «отклонить все», дающую пользователям возможность либо полностью отклонить, либо принять файлы cookie TikTok.

Компания не сразу ответила на запрос о комментарии.

CNIL оштрафовала Google на 150 миллионов евро и Facebook на 60 миллионов евро за аналогичные нарушения французского законодательства, призванного облегчить потребителям отказ от файлов cookie.

TikTok находится в центре ряда споров о конфиденциальности по всему миру, в том числе в Соединенных Штатах, где его собственность китайской компании ByteDance привела к обвинениям в том, что приложение представляет угрозу национальной безопасности. Федеральное правительство и примерно 20

штатов США запретили его использование на правительственных устройствах. В ноябре директор ФБР Кристофер Рэй заявил в Конгрессе, что у бюро есть ряд проблем с TikTok.

«Они включают в себя возможность того, что китайское правительство может использовать его для контроля сбора данных о миллионах пользователей или управления алгоритмом рекомендаций, который может быть использован для операций влияния, если они того захотят, или для управления программным обеспечением на миллионах устройств, что дает ему возможность потенциально технически скомпрометировать персональные устройства», — сказал Рэй». ***(Akshaya Asokan. French CNIL Fines TikTok 5 Million Euros for Cookie Policies // Information Security Media Group, Corp. (https://www.govinfosecurity.com/french-cnil-fines-tiktok-5-million-euros-for-cookie-policies-a-20928). 13.01.2023).***

***

«Федеральная торговая комиссия (FTC) обратилась в федеральный суд с просьбой отклонить «превентивный» иск, который брокер данных подал против FTC прошлым летом, всего за несколько недель до того, как регулирующее агентство возбудило принудительный иск против компании за незаконную продажу конфиденциальных данных о местоположении, собранных с сотен миллионов мобильных устройств.

В понедельник Федеральная торговая комиссия в судебном заседании раскритиковала «упреждающий» иск компании Kochava Inc. из Айдахо, поданный против Федеральной торговой комиссии в августе, и последующий запрос аналитической фирмы в октябре об отклонении судом гражданского исполнительного иска Федеральной торговой комиссии.

FTC в своем августовском правоприменительном иске против Kochava утверждает, что компания незаконно собирает и продает данные о местоположении, полученные с мобильных устройств потребителей, включая данные, которые могут быть использованы для идентификации лиц, которые посещали клиники для абортов, поставщиков психиатрических услуг и другие конфиденциальные места. таких как места отправления культа и приюты для бездомных и домашнего насилия (см.: FTC подает в суд на фирму, которая собирает и продает конфиденциальные данные о местонахождении).

Принудительные действия FTC против Kochava направлены на то, чтобы остановить продажу фирмой конфиденциальных данных о геолокации и потребовать от компании удалить собранные ею данные о местоположении.

Kochava в своем иске, поданном за несколько недель до этого против FTC - в ожидании принудительных действий этого агентства - утверждает, что FTC превышает свои полномочия и ошибочно утверждает, что Kochava не предлагает никаких технических средств контроля, чтобы запретить клиентам идентифицировать потребителей или отслеживать их в важных местах.

На самом деле, как утверждает Кочава в судебных документах, 10 августа 2022 года компания объявила о новой возможности, блокировке конфиденциальности, которая позволяет клиентам фирмы, таким как разработчики мобильных приложений, отключать сбор конфиденциальных данных о

местоположении медицинских служб из так называемый Кочавский коллективный рынок.

Кочава в своем иске против FTC просит суд постановить, среди прочего, что FTC не уполномочена добиваться судебного запрета на «прошлое поведение, которое прекратилось, при отсутствии доказательств того, что оно может повториться».

«Гонка к зданию суда»

FTC в своем последнем судебном документе на этой неделе утверждает, что Кочава «поспешил в суд», чтобы подать в суд на FTC в августе 2022 года, вскоре после того, как агентство сообщило фирме, занимающейся анализом данных и маркетингом, что оно стало целью потенциального гражданского правоприменения.

«Компания в спешке подала жалобу, не удовлетворяющую пороговым юрисдикционным и состязательным требованиям», — говорится в ходатайстве КДК с просьбой отклонить иск Кочавы к КДК.

Спор между Кочавой и FTC также возник после исполнительного распоряжения президента Байдена в июле прошлого года после решения Верховного суда по делу Роу против Уэйда. Среди прочих действий исполнительный приказ предписывал Федеральной торговой комиссии рассмотреть варианты «противодействия обманным или мошенническим действиям, в том числе в Интернете, и защиты доступа к точной информации».

Растущие опасения

Судебный процесс между Кочавой и FTC также является одним из ряда других споров о конфиденциальности, связанных со сбором конфиденциальных данных о состоянии здоровья, которые возникли в течение нескольких месяцев после решения Верховного суда США об отмене решения «Роу против Уэйда».

Это включает в себя объединенный коллективный иск, поданный в федеральный суд Калифорнии против материнской компании Facebook Meta, в котором утверждается, что компания с помощью своих инструментов отслеживания Pixel собирает конфиденциальные данные о здоровье миллионов людей с веб-сайтов поставщиков медицинских услуг и порталов пациентов без ведома или согласия пациентов.

Федеральная торговая комиссия (FTC) отклонила просьбу Information Security Media Group прокомментировать судебный процесс. Адвокат, представляющий Кочаву, не сразу ответил на запрос ISMG о комментариях.

Еще не все

Дэниел Кауфман, бывший исполняющий обязанности директора Бюро по защите прав потребителей FTC, который в настоящее время является юристом по регулированию в юридической фирме BakerHostetler, говорит, что решение Кочавы подать превентивный иск против FTC — это юридический маневр, который несколько других фирм попытались получить о принудительных действиях Федеральной торговой комиссии по обвинениям в недобросовестной или вводящей в заблуждение деловой практике.

«Я не видел, чтобы эта [правовая стратегия] была успешной, — говорит он. По его словам, суды, как правило, выносили решения против упреждающих исков

этих компаний в пользу того, чтобы позволить правительству добиться соблюдения нормативных требований.

«Что делает дело Кочавы — и многие из этих вопросов — очень интересными, так это то, что Федеральная торговая комиссия использует свои «полномочия по недобросовестности» [для правоприменения], которым уже несколько десятков лет… и они довольно широки… но не предназначены для решения передовых технологий. вопросы конфиденциальности», — говорит он. «Все это может измениться, если Конгресс в конечном итоге примет широкий закон о конфиденциальности».

Между тем, FTC в этом году, вероятно, продолжит усиливать правоприменение в других подобных спорных случаях, связанных с проблемами конфиденциальности и безопасности данных, прогнозирует Кауфман.

«Я думаю, что мы увидим больше случаев, основанных на несправедливости, когда FTC пытается решить проблемы конфиденциальности, расширяя границы несправедливости». ***(Marianne Kolbasuk McGee. FTC Wants Data Broker's Lawsuit Dismissed in Privacy Dispute // Information Security Media Group, Corp. (https://www.govinfosecurity.com/ftc-wants-data-brokers-lawsuit-dismissed-in-privacy-dispute-a-20866). 05.01.2023).***

***

«Ирландская комиссия по защите данных наложила на Meta Ireland штраф в размере 390 миллионов евро за нарушение Общего регламента по защите данных, связанного с обработкой пользовательских данных. Meta подтвердила, что будет оспаривать штраф, направленный на персонализацию рекламы в Facebook и Instagram.

Последний штраф является частью двух отдельных расследований, начатых комиссией против платформ социальных сетей Meta, Facebook и Instagram, относительно использования компанией данных пользователей для персонализации рекламы.

Запросы, которые были начаты после того, как в 2018 году австрийская группа по защите прав на неприкосновенность частной жизни NYOB и один австралиец подали две отдельные жалобы, изучали, как Meta Ireland могла нарушить положение о согласии пользователя, предусмотренное статьей 6 GDPR.

В 2018 году Meta Ireland представила «договорную необходимость» — свои обновленные, ориентированные на конфиденциальность условия обслуживания для Instagram и Facebook, которые стремились узаконить обработку пользовательских данных сразу после вступления в силу европейского GDPR.

В то время как ранее компания требовала согласия пользователей для доступа к службам Facebook и Instagram, в соответствии с пересмотренными изменениями пользователи должны были принять обновленные условия обслуживания компании, чтобы продолжить доступ к службам.

В жалобах утверждалось, что обновленные условия обслуживания Meta Ireland фактически вынуждали пользователей давать согласие и принимать условия обслуживания компании для обработки пользовательских данных для поведенческих данных и других персонализированных услуг. Они также

утверждали, что, вводя обновленные условия, Meta Ireland «обошла» требование о согласии в соответствии с GDPR, добавив в условия пункт о включении рекламы.

Завершая свои расследования в среду, ирландский DPC объявил, что программа Meta Ireland нарушила несколько положений GDPR, не предоставив пользователям информацию о том, как будут обрабатываться их данные. В результате компания Meta Ireland была оштрафована на 210 миллионов евро за нарушения, связанные с услугами Facebook, и на 180 миллионов евро за услуги Instagram.

Комиссия также дала Meta Ireland срок в три месяца для соблюдения GDPR.

В отдельном заявлении, также опубликованном в среду, Meta заявила, что «категорически не согласна» с окончательным решением комиссии и обжалует это решение.

«Учитывая, что сами регуляторы не соглашались друг с другом по этому вопросу вплоть до финальной стадии этих процессов в декабре, трудно понять, как нас могут критиковать за подход, который мы заняли до сих пор, и поэтому мы также планируем оспорить размер наложенных штрафов», — сказал Мета». ***(Akshaya Asokan. Irish Privacy Watchdog Fines Meta 390 Million Euros for Ads // Information Security Media Group, Corp. (https://www.govinfosecurity.com/irish-privacy-watchdog-fines-meta-390-million-euros-for-ads-a-20857). 04.01.2023).***

***

«Министр связи и цифровых технологий Малайзии Фахми Фадзил приказал провести расследование предполагаемой массовой утечки данных, затронувшей около 13 миллионов граждан. Сообщается, что утечки касаются данных Maybank, спутникового вещателя Astro и Избирательной комиссии.

Фадзил приказал национальному агентству по кибербезопасности CyberSecurity Malaysia и Департаменту защиты персональных данных Малайзии расследовать, есть ли утечка данных с участием заинтересованных сторон, и принять юридические меры в случае нарушения.

В субботу крупнейшая финансовая группа Малайзии Maybank опровергла предполагаемое обвинение в утечке данных клиентов. В Twitter говорится : «После расследования подтверждается, что эти обвинения являются ложными».

В нем также говорится: «Мы хотели бы заверить вас, что ваши данные остаются в безопасности [и] конфиденциальными и что никакие данные клиентов не были скомпрометированы. Мы будем продолжать уделять приоритетное внимание нашим мерам кибербезопасности, поскольку защита данных клиентов имеет для нас первостепенное значение. "

Утечка стала известна после того, как пользователь Facebook под ником Pendakwah Teknologi отметил Фадзила и поделился подробностями об утечке данных.

Пользователь поделился скриншотами данных, доступных на форуме взлома, включая такую информацию, как имя пользователя, дата рождения, адрес и идентификационные номера.

Предполагаемый пост на форуме о взломе был сделан 25 декабря 2022 г., и в нем говорилось:

3,5 миллиона информации Astro просочились;

1,8 миллиона информации о MAYBANK просочились;

Утекла информация о 7,2 миллиона SPR.

В ответ на сообщение Pendakwah Teknologi Фадзил сказал: «Это серьезная предполагаемая утечка, связанная с большим объемом данных. Я попрошу CyberSecurity Malaysia, Департамент защиты персональных данных Малайзии, расследовать, есть ли утечка данных с участием заинтересованных сторон, и подать в суд».

Утечка была впервые обнаружена платформой анализа киберугроз ThreatMon 26 декабря 2022 года.

Расследование раскрыто

В пятницу Фадзил сообщил в Facebook, что Министерство связи и цифровых технологий через Департамент защиты личных данных в сотрудничестве с CyberSecurity Malaysia запрашивает отзывы у Maybank и Astro, чтобы обеспечить законность владения данными.

Расследование показало, что информация о номере счета Maybank на рассматриваемом веб-сайте была недействительной или отсутствовала. Министр заявил, что предполагаемая утечка данных может быть связана с инцидентом, произошедшим в 2018 году.

«Официальное подтверждение от соответствующих сторон требуется для проведения подробного расследования в соответствии с Законом о защите персональных данных 2010 года (Закон 709)», — сказал Фадзил.

Что касается данных, касающихся Избирательной комиссии, Фадзил сказал, что результаты расследования будут переданы Национальному агентству кибербезопасности для дальнейших действий, поскольку они не подпадают под юрисдикцию Закона 709.

Министр также объявил, что он направил уведомление об ограничении в Комиссию по связи и мультимедиа Малайзии, чтобы предотвратить доступ общественности к предполагаемому веб-сайту, на котором были размещены данные». ***(Prajeet Nair. Malaysian Agencies Investigate Alleged Breach Affecting 13M // Information Security Media Group, Corp. (https://www.govinfosecurity.com/malaysian-agencies-investigate-alleged-breach-affecting-13m-a-20839). 02.01.2023).***

***

«Недавно просочившаяся база данных, содержащая более 200 миллионов записей Twitter, станет постоянным ресурсом для хакеров, мошенников и других преступников, действующих в Интернете, предупреждает эксперт по безопасности.

Утечка базы данных объемом 93 ГБ «к сожалению, приведет к множеству хакерских атак, целенаправленного фишинга и доксинга» как со стороны преступников, так и со стороны правительств, говорит Алон Гал, технический директор израильской разведывательной компании Hudson Rock, в сообщении для LinkedIn. «Это одна из самых значительных утечек, которые я видел».

Утечка включает 211 524 284 записи, включая имена, имена пользователей, адреса электронной почты и количество подписчиков, согласно бесплатной службе уведомлений об утечке данных Have I Been Pwned.

Информация была публично выставлена на продажу в прошлом месяце генеральному директору Twitter Илону Маску в виде базы данных из 400 миллионов записей, которую впервые обнаружил Гал.

В среду владелец бесплатно опубликовал урезанную версию — вероятно, для устранения дубликатов — через популярный форум по киберпреступности. Личность человека, который контролирует или собирает информацию, остается неизвестной.

Хотя утечка данных Twitter не включает пароли, многие другие утечки данных включали такую информацию, которую, по словам экспертов, можно легко собрать и объединить со многими из этих записей.

Гэл говорит, что записи предоставляют преступникам полезную информацию, например, информацию о том, какие владельцы учетных записей Twitter заинтересованы в криптовалюте и, возможно, являются ее владельцами, на основе учетных записей, содержащих .ethих имя или другой текст на крипто-тематику. Список также можно использовать для таргетинга на высококлассные учетные записи на основе количества подписчиков, выявления учетных записей «OG» с желаемыми именами пользователей, таргетинга на «политические учетные записи» и разоблачения «анонимных» учетных записей, которые не использовали уникальный адрес электронной почты для Twitter., а скорее адрес, который может быть проиндексирован другими утечками данных, чтобы идентифицировать владельца, говорит он.

Преступники злоупотребили Twitter API

Адреса электронной почты, похоже, не были украдены из Twitter. Скорее, «данные были получены где-то в 2021 году путем злоупотребления API, который позволял преобразовывать адреса электронной почты в профили Twitter», согласно HIBP. Соответственно, информация была собрана задолго до того, как Маск купил Twitter за 44 миллиарда долларов в октябре 2022 года.

Это не единственный набор данных, который был скомпилирован людьми, воспользовавшимися недостатком API. В ноябре прошлого года злоумышленник удалил базу данных, содержащую 5,4 миллиона имен пользователей, отображаемых имен, биографий, местоположений, адресов электронной почты и номеров телефонов.

В августе прошлого года Twitter подтвердил, что данные были украдены из функции «разрешить другим находить вас по вашему телефону», которая была добавлена в июне 2021 года, а затем заблокирована в январе 2022 года после получения отчета об ошибке о риске, связанном с новой функцией. Пока это не было исправлено, Twitter заявил, что «если кто-то отправит адрес электронной почты или номер телефона в системы Twitter, системы Twitter сообщат человеку, с какой учетной записью Twitter были связаны отправленные адреса электронной почты или номер телефона, если таковые имеются».

Жизненный цикл взломанных данных

Основываясь на выборке первых 10 000 записей, содержащихся в данных Twitter, сброшенных в среду, почти каждый адрес электронной почты фигурировал в предыдущих утечках данных, сообщает эксперт по утечкам данных Трой Хант, который создал и запускает Have I Been Pwned.

Бесплатная служба уведомления о нарушениях отправляет электронное письмо любому, кто регистрирует адрес электронной почты, всякий раз, когда этот адрес появляется в общедоступной утечке данных или дампе данных. На сегодняшний день он отследил 12,4 миллиарда заблокированных учетных записей, а некоторые адреса электронной почты фигурировали в нескольких взломах.

Что касается недавней утечки более 200 миллионов записей в Твиттере, «уровень 98% «разблокированных до» ясно указывает на то, что адреса электронной почты были взяты из других утечек данных, а затем использовались для запроса уязвимого API», — говорит Хант через Twitter. Эти запросы позволяли тому, кто составлял набор данных, добавлять имя пользователя, имя пользователя Twitter и количество подписчиков, связанных с каждым из проверенных адресов электронной почты, которые были привязаны к учетной записи Twitter.

Многие электронные письма, содержащиеся в образце утекших записей Twitter, фигурируют в трех из 10 крупнейших утечек или наборов утечек данных на сегодняшний день, как отслеживается Have I Been Pwned:

62% появляются в наборе данных Collection1 — всего 773 миллиона записей;

58% появляются в наборе данных ExploitIn — всего 593 миллиона записей;

26% появляются в наборе данных AntiPublic — всего 458 миллионов записей.

«Никаких разоблачений, ИМХО, просто подтверждение того, что как только данные появляются, они снова и снова циркулируют и злоупотребляют», — говорит Хант. «Эти адреса есть только в скопированных данных Twitter, потому что они уже были скомпрометированы где-то еще, поэтому цикл продолжается». ***(Mathew J. Schwartz. Expect Hacking, Phishing After Leak of 200M Twitter Records // Information Security Media Group, Corp. (https://www.govinfosecurity.com/expect-hacking-phishing-after-leak-200m-twitter-records-a-20872). 06.01.2023).***

***

«Федеральная комиссия по связи изучает, как определить ключевую терминологию, которая регулирует требования к представлению данных для телекоммуникационных компаний, в рамках предстоящего обновления требований к утечке данных.

Обновленные правила, которые разрабатывались с прошлого года, направлены на своевременное уведомление об утечке данных в телекоммуникационном секторе для лучшей защиты потребителей. Изменения, предложенные в текущих правилах FCC, касающихся отчетности об инцидентах утечки данных, включают расширение определения «нарушения».

«Мы предлагаем пересмотреть наше определение, чтобы определить нарушение как любой случай, когда лицо без авторизации или превышения авторизации получило доступ, использовало или раскрыло [собственную сетевую информацию клиента]», — говорится в уведомлении. «Мы просим прокомментировать это предложение и другие возможные определения».

Текущее определение нарушения FCC основано на намерении получить доступ к такому CPNI, за исключением случаев случайного доступа и раскрытия информации. Предлагаемое определение теперь будет включать такие случаи.

FCC отмечает, что законы нескольких штатов исключают «добросовестное» получение конфиденциальных данных от авторизованного пользователя из их определения «нарушения», в основном на основании использования раскрытых данных. Чиновники FCC рассматривают возможность включения этой детали в свое обновленное определение.

Агентство также призвало прокомментировать, должно ли его новое определение «нарушения» включать сценарии, когда телекоммуникационная компания или третья сторона раскрывают поведение, которое могло «обоснованно» привести к раскрытию конфиденциальных данных потребителей, даже до того, как утечка данных была обнаружена. было доказано.

В этом ключе большая часть отзывов, которые агентство хочет получить, сосредоточено на требовании от телекоммуникационных компаний принять стандарт уведомления, который требует, чтобы сообщалось об утечке данных на основе того, были ли затронуты потребители.

Это уведомление, называемое триггером на основе вреда, используется в протоколах утечки данных в некоторых штатах, которые FCC привела в качестве примера при разработке своей новой системы отчетности. Триггеры, основанные на причинении вреда, как правило, не требуют, чтобы организации сообщали о нарушениях потребителям, если доказано, что их собственные данные не пострадали в результате атаки.

«Мы просим прокомментировать, следует ли отказаться от требования уведомления клиентов или правоохранительных органов о нарушении в тех случаях, когда оператор связи может обоснованно определить, что в результате нарушения нет причинения вреда клиентам», — поясняется в уведомлении.

Одним из ключевых компонентов принятия правила срабатывания на основе ущерба является то, как именно FCC и телекоммуникационные организации определяют, был ли нанесен какой-либо ущерб после утечки данных.

«Мы [FCC] предварительно считаем, что ни один фактор сам по себе (например, базовое шифрование) не является достаточным для принятия решения о причинении вреда клиентам», — говорится в уведомлении. И это определение вреда может иметь иное влияние на потребителей, чем на правоохранительные органы.

«Хотя есть законные причины рассмотреть вопрос об исключении уведомлений для клиентов в тех случаях, когда нарушение разумно не может причинить вред, включая снижение путаницы, стресса, финансовых трудностей и усталости от уведомлений, можно ли то же самое сказать об уведомлениях правоохранительных органов?»

Агентство также изучает, как точно определить «ущерб» в контексте утечки данных, потенциально дополняя определение, чтобы охватить эмоциональный и репутационный ущерб.

Другие агентства, в том числе Национальный институт стандартов и технологий, использовали столь же широкий подход к определению ключевых

терминов кибербезопасности. Нынешнее значение «вреда» в официальном глоссарии NIST учитывает «неблагоприятные последствия, которые могут возникнуть у человека (т. е. могут быть социально, физически или финансово опасны) или организации» в случае утечки данных.

Само слово «взлом» также включает в себя более случайные случаи раскрытия данных, которые в настоящее время рассматривает Федеральная комиссия по связи США. NIST определяет «нарушение» как любую потерю контроля над данными, когда «лицо, отличное от авторизованного пользователя, получает или потенциально может получить доступ к информации, позволяющей установить личность; или авторизованный пользователь получает доступ к информации, позволяющей установить личность, для иной, чем авторизованная, цели».

Между тем Агентство по кибербезопасности и безопасности инфраструктуры не обязательно включает «ущерб» в тот же контекст, однако оно определяет «утечку данных» как «несанкционированное перемещение или раскрытие конфиденциальной информации стороне», отмечая, что несанкционированный доступ обычно организуется лицом, не входящим в организацию.

Другой предлагаемый уровень протокола сообщения об инцидентах потребует от операторов уведомлять правоохранительные органы о нарушении, а именно Секретную службу и Федеральное бюро расследований, в дополнение к FCC.

Поскольку кибератаки на цифровые сети критической инфраструктуры только усугубляются, федеральным агентствам все чаще поручают возглавить работу по повышению национальной кибербезопасности.

Председатель FCC Джессика Розенворсель в январе 2023 г. и в 2022 г. выступала за ужесточение требований к отчетности об утечке данных.

«Закон требует от операторов защищать конфиденциальную информацию о потребителях, но, учитывая увеличение частоты, сложности и масштабов утечек данных, мы должны обновить наши правила, чтобы защитить потребителей и ужесточить требования к отчетности», — сказала она в более раннем заявлении о предлагаемом изменении отчетности.

После публикации предлагаемого правила период комментариев открыт до конца дня 22 февраля 2023 г., а ответы на комментарии должны быть представлены до 24 марта». ***(Alexandra Kelley. What's in a Word? FCC's Proposed Data Breach Rule Redefines Key Terms // Nextgov (https://www.nextgov.com/cybersecurity/2023/01/whats-word-fccs-proposed-data-breach-rule-redefines-key-terms/382088/). 23.01.2023).***

***

«Личные электронные письма, связанные с 235 миллионами учетных записей Twitter, которые были взломаны некоторое время назад, были раскрыты, по словам израильского исследователя безопасности Алона Гала, что сделало миллионы уязвимыми для компрометации их учетных записей или раскрытия личности, если они использовали сайт анонимно для критики репрессивных правительств, для экземпляр.

Гэл, который является соучредителем и главным техническим директором фирмы по кибербезопасности Hudson Rock, написал на этой неделе в сообщении LinkedIn, что утечка «к сожалению, приведет к большому количеству взломов, целевого фишинга и доксинга».

Хотя пароли учетных записей не были раскрыты, злоумышленники могли использовать адреса электронной почты, чтобы попытаться сбросить пароли людей или угадать их, если они обычно используются или повторно используются с другими учетными записями. Это особенно опасно, если учетные записи не защищены двухфакторной аутентификацией, которая добавляет второй уровень безопасности к учетным записям, защищенным паролем, заставляя пользователей вводить автоматически сгенерированный код для входа в систему.

По словам экспертов, люди, которые используют Twitter анонимно, должны иметь адрес электронной почты, выделенный для Twitter, который не раскрывает их личность и используется исключительно для Twitter.

Хотя взлом, похоже, произошел до того, как Илон Маск захватил Twitter, новости об утечке электронных писем добавляют еще одну головную боль миллиардеру, чьи первые пару месяцев на посту главы Twitter были, мягко говоря, хаотичными.

Twitter не сразу ответил на сообщение с комментариями о взломе.

Известие о взломе может вызвать у компании проблемы с Федеральной торговой комиссией. Компания из Сан-Франциско подписала с агентством соглашение о согласии в 2011 году, которое требовало устранения серьезных недостатков в безопасности данных.

В мае прошлого года, за несколько месяцев до прихода Маска, Twitter заплатил штраф в размере 150 миллионов долларов за нарушение приказа о согласии. В обновленной версии установлены новые процедуры, требующие от компании реализации расширенной программы защиты конфиденциальности, а также усиления информационной безопасности.

В ноябре группа законодателей-демократов обратилась к федеральным регулирующим органам с просьбой расследовать любые возможные нарушения платформой законов о защите прав потребителей или ее обязательств по безопасности данных.

В то время FTC заявила, что «с глубокой обеспокоенностью отслеживает последние события в Twitter», хотя об официальном расследовании не было объявлено. Но эксперты, а также нынешние и бывшие сотрудники Twitter предупреждают о серьезных рисках для безопасности, связанных с резким сокращением штата и углублением беспорядков в компании.

В августе бывший глава службы безопасности Twitter подал жалобу осведомителя, утверждая, что компания ввела в заблуждение регулирующие органы относительно своей слабой защиты от кибербезопасности и небрежности в попытках искоренить поддельные учетные записи, распространяющие дезинформацию.

Одним из самых серьезных обвинений Пейтера Затко является то, что Twitter нарушил условия соглашения FTC 2011 года, ложно заявив, что он принял более строгие меры для защиты безопасности и конфиденциальности своих

пользователей». ***(Barbara Ortutay. Israeli researcher reports leak of 235m email addresses linked to Twitter accounts // The Times of Israel (https://www.timesofisrael.com/israeli-researcher-reports-leak-of-235m-email-addresses-linked-to-twitter-accounts/). 07.01.2023).***

***

«…Сегодня исследователи из компании Avanan, входящей в состав Check Point Software Technologies Ltd., подробно рассказали, что хакеры используют уведомления Facebook о нарушении авторских прав для кражи учетных данных. Атака начинается с того, что хакеры рассылают поддельные уведомления о нарушении авторских прав Facebook, в которых утверждается, что учетная запись жертвы была заблокирована из-за загрузки фотографии на страницу учетной записи, что нарушает политику Facebook в отношении нарушения авторских прав.

В электронном письме потенциальным жертвам сообщается, что для обжалования приостановки у них есть 24 часа на подачу апелляции, в противном случае их учетная запись будет заблокирована навсегда. Ссылка в электронном письме ведет не на страницу, контролируемую Meta Platforms Inc., а на страницу сбора учетных данных.

Несмотря на то, что отправитель электронного письма и ссылка явно исходят не от Facebook, исследователи отмечают, что в остальном это вполне правдоподобно, включая ссылку в электронном письме, в которой упоминается страница жертвы в Facebook.

Тогда возникает вопрос, как люди попадают на такие аферы, особенно с учетом того, что ссылки незаконны. По мнению исследователей, лучшие фишинговые электронные письма играют на срочности, в данном случае на угрозе потери доступа к учетной записи Facebook.

«Подумайте об этом: если ваша организация полагается на свою страницу в Facebook для рекламы, повышения осведомленности и другой деловой активности, ее постоянное приостановление будет довольно сложно преодолеть», — объясняют исследователи. «Подача быстрой апелляции кажется разумной».

Хотя неясно, насколько успешными были электронные письма, исследователи добавляют, что они имеют успех, о чем свидетельствуют волны рассылаемых электронных писем, поскольку хакеры продолжают рассылать фишинговые электронные письма только в том случае, если некоторые из них успешны.

Пользователям всегда рекомендуется наводить курсор мыши на URL-адреса, прежде чем щелкнуть, чтобы убедиться, что они законны. Отправитель любого электронного письма должен быть перепроверен, и в случае заявленного нарушения авторских прав со стороны Facebook пользователи должны войти в свою учетную запись напрямую, чтобы увидеть статус учетной записи, вместо того, чтобы щелкать URL-адрес в электронном письме…» ***(Duncan Riley. Facebook users targeted with fake copyright notices in credential stealing campaign // SiliconANGLE Media Inc. (https://siliconangle.com/2023/01/09/facebook-users-targeted-fake-copyright-notices-credential-stealing-campaign/). 09.01.2023).***

***

«14 января один из его почти 90 000 подписчиков в Твиттере купил украденный у NFT God яхт-клуб Mutant Ape Yacht Club NFT и предложил вернуть все свои цифровые активы в результате взлома. это по себестоимости — свыше $25000.

Ранее в тот же день NFT God, настоящее имя которого Алекс, загрузил сервис потокового видео OBS. Однако он использовал рекламную ссылку в Google, которая содержала программное обеспечение, зараженное вредоносным ПО. Две недели назад эксперт по кибербезопасности Джон Хаммонд предостерег людей от поддельного программного обеспечения OBS.

Пару часов спустя подписчик предупредил Алекса, что его аккаунт в Твиттере был взломан. Через несколько минут Алекс восстановил контроль над своей учетной записью в Твиттере и удалил мошеннические твиты, опубликованные хакерами.

Через несколько часов Алекс понял, что взлом Twitter — это только начало череды атак. Все его кошельки были опустошены в криптовалютах и NFT, что, по словам Алекса, «сумма, которая меняет жизнь».

Через несколько часов Алекс узнал, что хакеры также получили контроль над его Gmail, Discord и Substack. Злоумышленники также разослали два электронных письма с фишинговыми ссылками его 16 000 подписчиков.

Дорогостоящая ошибка

Создавая свою учетную запись в Ledger, Алекс «облажался», написал он в твиттере. Несмотря на то, что Алекс был «высокотехничным», он допустил ошибку и ввел свою сид-фразу таким образом, что «больше не держал ее в холоде», как он написал.

Поскольку он не покупал новых NFT в течение нескольких месяцев и не собирался делать это в ближайшее время, Алекс отложил покупку еще одного холодного кошелька Ledger.

Эта ошибка позволила хакерам получить контроль над криптографией и NFT Алекса посредством атаки вредоносного ПО на его рабочий стол. Алекс написал:

«Не купить сразу новый холодный кошелек было смертельной ошибкой. Но даже с холодным кошельком весь мой цифровой мир все равно будет уничтожен. Цифровая безопасность — это не просто покупка холодного кошелька. Это также осторожность со ВСЕМ, что вы делаете в Интернете. Все.» ***(Monika Ghosh. Wallets of NFT influencer drained in OBS malware attack // CryptoSlate (https://cryptoslate.com/wallets-of-nft-influencer-gets-drained-in-obs-malware-attack/?amp=1). 15.01.2023).***

***

«В 2022 году ставки на утечку данных выросли во многих отношениях. IBM сообщила, что средняя стоимость утечки данных составляет до 4,35 миллиона долларов. Однако, что еще более важно, регулирующие органы сосредоточили свое внимание на руководителях и советах директоров более высокого уровня как в отношении их управления киберрисками, так и в отношении

их участия в реагировании на нарушения. Все это вытекает из растущего числа уведомлений о нарушениях, связанных с множеством новых требований и ожиданий в отношении уведомлений о нарушениях.

Вот топ-5 изменений в области киберправа в 2022 году…

1. Федеральная торговая комиссия США и Министерство юстиции пресекают действия руководителей в киберпространстве.

Во-первых, в октябре Федеральная торговая комиссия (FTC) приняла решение о принудительном иске, связанном с утечкой данных, против Дризли, который впервые в деле о кибербезопасности назначил генерального директора индивидуально. FTC утверждала, что он не внедрил или не делегировал внедрение разумных методов безопасности. В жалобе особо упоминалось об отсутствии директора по информационной безопасности. В результате урегулирования генеральный директор связан обязательствами по обеспечению безопасности в соглашении о разрешении, даже если он покинет Drizly, а это означает, что если он покинет Drizly и будет нанят в новую компанию, утвердительные обязательства последуют за ним в эту компанию. Это также создает возможность индивидуальных штрафов за нарушение порядка, в настоящее время 46 517 долларов за нарушение.

Во-вторых, также в октябре Министерство юстиции добилось осуждения бывшего CSO Uber за сокрытие утечки данных в ходе продолжающегося расследования FTC. Сокрытие включало обмен сообщениями, чтобы скрыть инцидент, выплату 100 000 долларов хакеру для получения возврата украденных данных и соглашение о неразглашении с ложными заявлениями. Первоначальные заявления Министерства юстиции по этому поводу предполагали, что Министерство юстиции может более агрессивно стремиться использовать уголовные законы в вопросах кибербезопасности. Однако совсем недавно высокопоставленный чиновник Министерства юстиции пояснил, что «преследование ОГО Uber было связано с чрезмерным набором действий, которые представляют собой резкое отклонение от обычной практики соблюдения». Он добавил: «Никто не должен отнимать у этого в случае, если добросовестные решения о соблюдении требований будут подлежать уголовному преследованию». При этом само осуждение означает, что компании должны тщательно оценивать текущие обязательства по раскрытию информации о проблемах безопасности перед регулирующими органами во время расследования.

2. SEC предлагает расширенные новые правила киберотчетности и раскрытия информации

В феврале SEC предложила новые правила управления киберрисками для инвестиционных фондов и консультантов. Правила включают требование о предоставлении отчетов в течение 48 часов об определенных киберинцидентах (это очень много):

Инциденты, которые значительно подрывают или ухудшают способность консультанта или его фонда, или способность клиента частного фонда консультанта поддерживать критически важные операции, или которые приводят к несанкционированному доступу или использованию информации консультанта или его фонда, когда несанкционированный доступ или использование такой

информации приводит к (а) существенному ущербу консультанту или его фонду, или (б) существенному ущербу клиенту или инвестору, чья информация была доступна.

Правила также требуют принятия комплексной программы управления рисками кибербезопасности, которая включает оценку рисков, безопасный доступ пользователей, защиту системы, управление уязвимостями, готовность к инцидентам и проверку советом директоров. Предлагаемое правило обновляет формы раскрытия информации консультантами и фондами, чтобы включить отчетные киберинциденты за предыдущие два года, а также риски кибербезопасности и меры по их устранению на месте.

В марте SEC предложила новые правила раскрытия информации о кибербезопасности, которые включают:

Требование о раскрытии существенных инцидентов кибербезопасности в форме 8-K в течение четырех рабочих дней с момента определения события как существенного.

Периодическое раскрытие информации об управлении рисками кибербезопасности, стратегии и управлении, в том числе

Политики и процедуры, используемые для выявления и управления рисками кибербезопасности, включая сведения о надзоре совета директоров.

Роль кибербезопасности в стратегии компании, финансовом планировании и распределении капитала.

Контроль и опыт руководства и директора в области кибербезопасности.

Правила находятся на повестке дня и, как ожидается, будут окончательно утверждены в апреле 2023 года.

3. FTC и EC ожидают уведомления о расширении

В мае FTC объявила, что «независимо от того, применяется ли закон об уведомлении о нарушениях, нарушенная организация, которая не раскрывает информацию, чтобы помочь сторонам смягчить разумно предсказуемый ущерб, может нарушить раздел 5 Закона о FTC». Похоже, что цель состоит в том, чтобы подтолкнуть компании к тому, чтобы уведомлять отдельных лиц, когда нарушение увеличивает риск финансового мошенничества, хотя оно также может быть направлено и на другие формы вреда. В объявлении также подчеркивается важность своевременных уведомлений, которые точно передают затронутую информацию и меры реагирования.

Этот шаг добавляет новый и аморфный анализ в процесс уведомления о нарушениях для многих американских компаний. Тем не менее, это приближает FTC к соответствию правилу уведомления о нарушениях HIPAA, GDPR и требованиям к уведомлению о нарушениях по всему миру, что может упростить анализ уведомлений о нарушениях и принятие решений для некоторых предприятий.

Говоря о GDPR, Европейский совет по защите данных опубликовал Руководство по уведомлению о нарушениях, в котором разъясняется, что подпадающие под действие компаний, которые имеют утечку персональных данных и не зарегистрированы в ЕС, должны уведомить органы по защите данных всех государств-членов, где проживают затронутые лица. В худшем случае это 42

авторитета. На практике это может потребовать обширной координации для подачи или подачи уведомлений в соответствии с различными местными требованиями или ожиданиями, на местных языках и, конечно же, в течение 72 часов. Это также означает, что предприятия с большей вероятностью столкнутся с более тщательным контролем со стороны большего числа регулирующих органов после утечки данных. Ключевым моментом здесь является подготовка, и некоторые стратегии, которые следует учитывать, приведены здесь.

4. Предотвращайте, обнаруживайте, реагируйте и уведомляйте об ожиданиях в отношении заполнения учетных данных (и захвата учетных записей)

Генеральный прокурор Нью-Йорка (NY AG) начал насыщенный 2022 год выпуском Business Guide for Credential Stuffing Attacks. Вброс учетных данных — это тип кибератаки, которая обычно включает в себя попытку получить доступ к приложению или войти в него с использованием учетных данных, украденных из других онлайн-сервисов, в том числе путем грубого форсирования функций аутентификации приложения. Атаки такого рода могут привести к тому, что скомпрометированный доступ к учетной записи будет использоваться для мошеннических транзакций или для сбора информации, которая может быть использована для мошенничества или фишинга.

Для предотвращения и обнаружения подмены учетных данных и последующего мошенничества в Руководстве рекомендуется реализовать обнаружение ботов, брандмауэр веб-приложений, а также многофакторную или беспарольную аутентификацию, повторную аутентификацию для покупок в приложении и использование программного обеспечения для обнаружения мошенничества.

Руководство включает в себя блокировку доступа, сброс пароля и расследование любой подозрительной активности учетной записи.

Что касается уведомлений, руководство, в частности, ожидает индивидуальных уведомлений для владельцев скомпрометированных учетных записей, даже если уведомление может не требоваться в соответствии с законами штата об уведомлениях о нарушениях. Это важно для многих предприятий, чья стратегия снижения такого рода рисков включала маскировку или запутывание информации, раскрытие которой может повлечь за собой требование об уведомлении в соответствии с законодательством штата. Руководство и предыдущая история правоприменения NY AG указывают на то, что этого может быть недостаточно.

5. NYDFS предлагает существенные поправки к своему регламенту кибербезопасности

В ноябре Департамент финансовых услуг Нью-Йорка (NYDFS) опубликовал предлагаемые поправки к своему и без того обременительному Регламенту о кибербезопасности, часть 500. В случае принятия поправки установят существенные новые требования к организациям, на которые распространяется действие страховки, в том числе:

Дополнительные обязательства по отчетности. Поправки значительно расширяют обстоятельства, при которых застрахованная организация должна уведомлять NYDFS о событии кибербезопасности, включая события, когда: (1)

неавторизованный пользователь получил доступ к привилегированной учетной записи; (2) событие кибербезопасности привело к развертыванию программы-вымогателя в существенной части информационной системы обслуживаемой организации; или (3) застрахованная организация затронута инцидентом кибербезопасности у стороннего поставщика услуг. Примечательно, что подпадающие под действие организации также должны уведомить NYDFS в течение 24 часов после совершения платежа за вымогательство в связи с событием кибербезопасности.

Управление. Поправки требуют, чтобы подпадающие под действие организаций обеспечивали, чтобы их CISO могли надлежащим образом управлять рисками кибербезопасности, в том числе имея возможность «направлять достаточные ресурсы для внедрения и поддержания программы кибербезопасности». Совет директоров также должен обладать достаточным опытом или знаниями, чтобы осуществлять эффективный надзор за рисками кибербезопасности или получать консультации от лиц, которые это делают.

Контроль доступа. Поправки уточняют, что многофакторная аутентификация должна использоваться для удаленного доступа как к информационным системам субъекта, на которого распространяется действие, так и к сторонним приложениям, включая облачные приложения, а также к привилегированным учетным записям. Подпадающие под действие организации должны периодически проверять права доступа пользователей, и существуют дополнительные ограничения на использование привилегированных учетных записей.

Политики и процедуры. Поправки вводят множество новых обязательных политик и процедур, в том числе письменные политики, касающиеся инвентаризации активов, планов обеспечения непрерывности бизнеса и аварийного восстановления (BCDR), а также политик паролей и шифрования.

Период комментариев завершится 9 января 2023 года. Если поправки будут приняты после 60-дневного периода комментариев, большинство новых положений вступят в силу через 180 дней с даты принятия». ***(Aravind Swaminathan, Joseph C Santiesteban, Alyssa Wolfington. Takeaways From Top 5 Cyber Law Developments in 2022 // Orrick Herrington & Sutcliffe LLP (https://www.orrick.com/en/Insights/2023/01/Takeaways-From-Top-5-Cyber-Law-Developments-in-2022). 10.01.2023).***

***

«…согласно новому отчету ISACA, профессиональной ассоциации управления ИТ, когда организации ищут внутри себя меры по снижению рисков и соблюдению законов о конфиденциальности данных, для этого не хватает квалифицированных специалистов. Команды по технической конфиденциальности и юридическим вопросам/соответствию недоукомплектованы, бюджеты предприятий на конфиденциальность недофинансированы, и есть пробелы в навыках. Выводы основаны на глобальном опросе 1890 специалистов по обеспечению конфиденциальности данных, занимающих, например, должности в сфере ИТ, аудита, нормативно-правового соответствия и управления рисками.

Несоблюдение законов и нормативных актов о конфиденциальности, таких как Общее положение о защите данных в Европе или даже законов штатов, включая Калифорнийский закон о конфиденциальности потребителей (CCPA), дорого обходится, говорит мне Сафия Кази, руководитель профессиональной практики ISACA в области конфиденциальности. 1 января в CCPA вступили в силу обновления соответствия, касающиеся уведомления сотрудников и соискателей о правилах конфиденциальности компании.

Так что это вопрос, который может попасть в компетенцию финансового директора. «Опыт финансовых директоров в области управления рисками бесценен, — говорит Кази. «Особенно это касается закупок». По словам Кази, не только третьи лица могут быть источником серьезного нарушения конфиденциальности, но и выбор неквалифицированных третьих лиц может привести к «серьезному нарушению конфиденциальности и штрафу». Около четверти респондентов заявили, что всегда или часто сотрудничают с финансовым отделом своей организации. Но этот процент, возможно, придется увеличить.

«Инциденты с безопасностью и инциденты с конфиденциальностью — это не одно и то же»

Но большой риск означает большую награду — по крайней мере, для венчурных капиталистов, инвестирующих в это новое поколение продуктов кибербезопасности. Ожидается, что к 2027 году глобальный рынок кибербезопасности достигнет 403 миллиардов долларов, как подробно описывает в своем новом отчете моя коллега Люси Брюстер: «Кибербезопасность накалена докрасна. Вот 13 лучших венчурных капиталистов, которых нужно знать». Среди венчурных капиталистов, которых она представляет, Ченкси Ван, который инвестировал в платформу кибербезопасности «программное обеспечение как услуга» (SaaS) Claroty, и Ариэль Цейтлин, который инвестировал в платформу безопасности SaaS AppOmni — продукты, которые однажды могут стать стандартом в безопасной организации.

Что касается наличия специальной программы конфиденциальности данных, опрос ISACA показал, что 42% респондентов заявили, что их бюджет на конфиденциальность недофинансирован, и только 34% указали, что их бюджеты на конфиденциальность будут увеличены в 2023 году. Между тем, 40% заявили, что нет ясности в мандате, роли и обязанности, а 39% указали на отсутствие поддержки руководства или бизнеса.

«В прошлом году программы-вымогатели вызывали серьезную озабоченность, и многие организации предприняли шаги, чтобы подготовиться к атаке программ-вымогателей, — объясняет Кази. «Но возможно, что они рассматривают инциденты с безопасностью и инциденты с конфиденциальностью как одно и то же, что на самом деле не так. Вкладывать значительные средства в безопасность, не думая при этом о конфиденциальности, — это серьезная ошибка: такая, казалось бы, мелочь, как неправильное уведомление клиентов о конфиденциальности (которое не будет решено с помощью каких-либо инвестиций в безопасность), может стоить предприятию миллионы долларов и нанести ущерб репутации».

Она продолжает: «Члены правления некоторых организаций могут не до конца понимать разницу между безопасностью и конфиденциальностью и, следовательно, не уделять должного внимания конфиденциальности».

По словам Кази, важны как кибербезопасность, так и конфиденциальность. Но указывает на одну оговорку: «Конфиденциальность невозможна без безопасности, но возможна безопасность без конфиденциальности».

Она добавила: «Цифровое доверие все чаще становится приоритетом для совета директоров и высшего руководства, а конфиденциальность является ключевым компонентом цифрового доверия». ***(Sheryl Estrada. Despite cybersecurity being top of mind for the C-suite, data privacy is lagging, a new report finds // Fortune Media IP Limited (https://fortune.com/2023/01/24/cybersecurity-top-of-mind-c-suite-data-privacy-lagging-a-new-report-finds/). 24.01.2023).***

***

Кібербезпека та хмарні технології

«…Microsoft обвинила изменение конфигурации внутренней сети в серии сбоев, которые нарушили глобальный доступ к ее облачным службам Azure, включая Outlook и Microsoft Teams.

«Любой пользователь, обслуживаемый уязвимой инфраструктурой, может не иметь доступа к нескольким службам Microsoft 365», — предупредила Microsoft в среду утром в предупреждении о деградации службы Microsoft 365.

Отключение затронуло широкий спектр служб, включая SharePoint Online и OneDrive для бизнеса. Другие затронутые службы включают портал администрирования Microsoft 365 и управление конечными точками Microsoft Intune, а также Microsoft Defender для облачных приложений, удостоверений и конечных точек. Microsoft заявила, что проблема не только повлияла на прямой доступ к ее услугам, но и на то, как информация передается между ее центрами обработки данных.

Веб-сайт Downdetector, который собирает сообщения о перебоях в обслуживании, сообщил, что сообщения о сбоях начали расти около 7:00 утра по всемирному координированному времени. Также пострадали сервисы, ориентированные на потребителя, такие как Minecraft и Xbox Live.

Microsoft около 08:00 UTC впервые подтвердила сообщения об отключении и заявила, что, по-видимому, выявила проблему, которую описала как «изменение маршрутизации глобальной сети». Это описание предполагает, что изменение сети вызвало сбои в работе системы доменных имен.

В то же время пользователи по всему миру сообщали о сбоях в обслуживании. «В настоящее время мы наблюдаем отброшенные пакеты и высокую задержку для ресурсов в Azure», — написал в Mastodon один британский системный инженер.

Microsoft примерно в 09:00 UTC выпустила это обновление: «Мы откатили изменение сети, которое, по нашему мнению, оказывает влияние. Мы следим за службой, пока откат вступает в силу».

Microsoft заявила, что после изменения доступ к своим службам Microsoft 365 восстановили больше пользователей. «Мы также подключаем сервис к дополнительной инфраструктуре, чтобы ускорить процесс восстановления», — написала Microsoft в Твиттере.

Глобальное разрушение

На странице состояния Microsoft Azure в среду утром были показаны сбои в работе в Африке, Америке, Азиатско-Тихоокеанском регионе, Европе и на Ближнем Востоке. Единственным незатронутым регионом был Китай, включая Azure Government для Китая. Облачные сервисы Microsoft используются многими крупнейшими компаниями мира, а это означает, что сбой, вероятно, затронул миллионы людей.

Многие пользователи обратились в Twitter, чтобы сообщить о сбоях, в некоторых случаях через хэштег #Outlookdown.

«Думаю, сбой Teams и Outlook означает, что я наконец-то могу отдохнуть от людей, связывающихся со мной», — написал один из пользователей в Твиттере. «Нет, серьезно, неработающие Teams и Outlook действительно портят мой день».

В последний раз в Microsoft произошел серьезный сбой в июне 2022 года, когда был прерван доступ к Microsoft 365. Так же как и доступ к своей среде облачных вычислений Azure, которая уступает только Amazon Web Services с точки зрения размера своей пользовательской базы.

Другие крупные провайдеры не застрахованы от серьезных сбоев. Также в июне 2022 года Google сообщил, что серьезное отключение, которое нарушило доступ для пользователей на Ближнем Востоке и привело к увеличению задержки для пользователей в Европе и Азии, связано с проблемой физической инфраструктуры.

«Отключение было вызвано двумя одновременными обрывами оптоволокна в нашей ближневосточной сети. Это затронуло сквозной путь для нескольких подводных кабелей, уменьшив пропускную способность многих телекоммуникационных и технологических компаний, включая Google», — говорится в сообщении…». ***(Mathew J. Schwartz. Microsoft 365 Cloud Service Outage Disrupts Users Worldwide // Information Security Media Group, Corp. (https://www.govinfosecurity.com/microsoft-365-cloud-service-outage-disrupts-users-worldwide-a-21017). 25.01.2023).***

***

Кібербезпека Інтернету речей. Штучний інтелект

«З моменту запуску ШІ-бота ChatGPT ентузіасти встигли випробувати вирішення широкого кола завдань: бот не тільки відповідає на запитання, але й пише технічні статті, есе, вірші та комп'ютерний код. Як виявилося, на

останнє слід звернути увагу, тому що цей код може бути шкідливим, якщо таке завдання ставить перед штучним інтелектом користувач.

Експерти з кібербезпеки компанії Check Point Research опублікували дослідження, де розповіли, що учасники хакерських форумів використовують ChatGPT для написання шкідливого коду та фішингових електронних листів — деякі з цих людей мають невеликий досвід у програмуванні або взагалі його не мають.

В одному з наведених прикладів описується скрипт мовою Python, який при деякому доопрацюванні можна перетворити на програму-вимагач, здатну шифрувати дані на комп'ютері користувача. Ще один створений ChatGPT скрипт на Python здійснює пошук файлів заданого типу, наприклад, PDF на локальній машині, здійснює їх стиснення та відправку на сервер потенційного зловмисника — це стандартний сценарій крадіжки інформації.

В іншому прикладі написаний ChatGPT скрипт призначався для запуску торгового онлайн-майданчика, на якому здійснюється купівля або обмін скомпрометованих облікових записів, даних банківських карток, шкідливих програм та інших віртуальних товарів, що продаються в даркнеті. Скрипт підключався до стороннього інтерфейсу для отримання актуальних даних про котирування найпопулярніших криптовалют для спрощення розрахунків.

Дослідники Check Point Research і самі спробували використати нейромережу для моделювання хакерської атаки. Робот люб'язно написав їм переконливий фішинговий лист, в якому повідомлялося про блокування облікового запису в одному з хостерів і пропонувалося відкрити вкладений файл Excel. З кількох спроб ChatGPT написав і вбудований у цей файл шкідливий VBA-макрос». ***(Хакери початківці стали використовувати штучний інтелект ChatGPT для створення вірусів // No worries! (https://noworries.news/hakery-pochatkivczi-staly-vykorystovuvaty-shtuchnyj-intelekt-chatgpt-dlya-stvorennya-virusiv/). 07.01.2023).***

***

«Чат-бот ChatGPT може на запит користувачів писати програми-шкідники. Для цього не треба бути хакером — чат-бот зробить все самостійно і напише код.

Як повідомляє Arstechnica, дослідники компанії Check Point Research заявляють, що для кіберзлочинців відкрилася безліч можливостей при використанні штучного інтелекту. На форумах для хакерів знайшлися повідомлення про перші вдалі спроби створити за допомогою ChatGPT хакерські інструменти.

Наприклад, одна з програм була написана мовою Python і при належній обкатці її швидко можна перетворити на «вимагача». Програма може зашифрувати усі файли на комп'ютері жертви та вимагати плату за розшифровку.

В іншому прикладі більш розвинений хакер виклав на форумі в даркнеті приклад коду, написаного ChatGPT, який робить приховане завантаження на сервер клієнта. Непомітно підключившись до сервера, кіберзлочинець отримує повний доступ до даних жертви.

Також спеціалістам із Check Point вдалося за допомогою ChatGPT отримати цілий розсип інструментів: скрипти для сканування портів, доступ до Reverse Shell і навіть можливість скомпілювати код у файл Windows, що виконується». ***(Руслан Сорока. Хакери використовують ChatGPT для написання вірусних програм // Speka.Media (https://speka.media/xakeri-vikoristovuyut-chatgpt-dlya-napisannya-virusnix-program-9w45np). 10.01.2023).***

***

«Вновь представленный законопроект просит Федеральную торговую комиссию установить правила раскрытия информации для интеллектуальных устройств и бытовой техники, от которых потребители не ожидают, что они будут их записывать.

Двухпартийная группа сенаторов и представителей повторно представила Закон об информировании потребителей об интеллектуальных устройствах в обеих палатах Конгресса в среду, стремясь защитить потребителей от непреднамеренной записи с домашних интеллектуальных устройств, которые, как можно подумать, не имеют таких компонентов, как холодильники и кондиционеры.

Законопроект, внесенный в Сенат председателем Комитета по торговле, науке и транспорту Марией Кантуэлл, штат Вашингтон, и новым членом рейтинга Тедом Крузом, штат Техас, требует от Федеральной торговой комиссии разработки разумных руководящих принципов раскрытия информации о продуктах, которые неожиданно компоненты аудио- или видеозаписи, такие как микрофоны или камеры. К таким устройствам могут относиться холодильники, посудомоечные машины и тостеры, а также стиральные машины и сушилки.

«По оценкам, к 2026 году более 84 миллионов домохозяйств будут иметь интеллектуальные устройства, обеспечивающие связь и контроль над всем, от кондиционера до фритюрницы. Тем не менее, большинство потребителей ожидают, что их холодильники сохранят молоко холодным, а не оснащены камерой или микрофоном для записи их личных и частных семейных разговоров», — сказал Кантуэлл в пресс-релизе.

Законодатели отметили, что потребители могут не знать или не осознавать, что все большее число бытовых интеллектуальных устройств и бытовой техники содержат микрофоны или камеры, которые могут записывать людей и могут иметь возможность передавать эти данные по Wi-Fi.

«Поскольку количество интеллектуальных устройств в домах неуклонно растет, потребители заслуживают большей прозрачности в отношении того, как эти устройства работают и как они влияют на конфиденциальность. Американцы должны знать, записывает ли холодильник слова и движения членов их семей, и они должны знать, передает ли их виртуальный помощник аудиозаписи частных семейных разговоров», — сказал Круз.

Законодательство не будет применяться к технологиям, которые потребители ожидают записывать, например к смартфонам и ноутбукам.

Представители Джон Кертис, штат Юта, и Сет Моултон, штат Массачусетс, представили версию закона Палаты представителей.

Кертис отметил, что законопроект направлен на защиту потребителей, «а также уравновешивает гибкость для компаний, разрабатывающих интеллектуальные технологии», добавив, что закон получил поддержку широкой коалиции компаний, занимающихся защитой интересов потребителей и технологических компаний.

«Нам должно быть позволено принимать обоснованные решения в отношении электронных подслушивающих устройств, которых мы приглашаем в наши дома. Но мы не сможем этого сделать, если большие технологии спрячут микрофоны и камеры, которые всегда подслушивают, в холодильниках, тостерах и других бытовых гаджетах. Давайте примем этот законопроект, чтобы потребители знали, когда к ним прислушиваются крупные технологические компании», — сказал Моултон.

Сенаторы ранее представили законопроект в ноябре 2022 года, но у них не хватило времени, чтобы провести его через комитет. Закон был принят Палатой единогласно, когда он был представлен на последнем Конгрессе». ***(Kirsten Errick. Legislators Renew Efforts to Protect Consumers from an Eavesdropping Fridge // Nextgov (https://www.nextgov.com/emerging-tech/2023/01/legislators-renew-efforts-protect-consumers-eavesdropping-fridge/382255/). 26.01.2023).***

***

«С запуском AI RMF 1.0 федеральные исследователи сосредоточились на четырех основных функциях, чтобы структурировать то, как все организации оценивают и внедряют более надежные системы искусственного интеллекта.

В четверг утром Национальный институт стандартов и технологий представил свою долгожданную концепцию управления рисками искусственного интеллекта, представляющую собой кульминацию 18-месячного проекта, целью которого является универсальное применение к любой технологии искусственного интеллекта во всех секторах.

Повышение надежности и снижение рисков — две основные темы концепции, которую директор NIST Лори Локасио представила в качестве руководства, помогающего организациям разрабатывать системы искусственного интеллекта с низким уровнем риска. В документе описываются типы рисков, обычно встречающиеся в технологиях искусственного интеллекта и машинного обучения, а также то, как организации могут создавать этичные и надежные системы.

«Технологии искусственного интеллекта обладают значительным потенциалом для преобразования жизни отдельных людей и даже нашего общества. Они могут принести положительные изменения в нашу торговлю и наше здоровье, наш транспорт и нашу кибербезопасность», — сказал Локасио на мероприятии по запуску фреймворка. «AI RMF поможет многочисленным организациям, которые разработали принципы ИИ и придерживаются их, воплотить эти принципы на практике».

Эта структура предлагает четыре взаимосвязанные функции в качестве метода снижения рисков: управление, картирование, измерение и управление.

«Управление» лежит в основе стратегии смягчения последствий RMF и призвано служить основополагающей культурой предотвращения рисков и управления ими, лежащей в основе любой организации, использующей RMF.

Построенная на фундаменте «Управление», «Карта» является следующей в плане игры RMF. Этот шаг работает, чтобы контекстуализировать потенциальные риски в технологии ИИ и в целом определить положительную миссию и использование любой данной системы ИИ, одновременно принимая во внимание ее ограничения.

Затем этот контекст должен позволить пользователям фреймворка «измерять», как на самом деле функционирует система ИИ. Решающее значение для компонента «Измерение» имеет использование достаточного количества показателей, которые представляют собой универсальные научные и этические нормы. Затем строгие измерения применяются посредством «тщательного» тестирования программного обеспечения, которое дополнительно анализируется внешними экспертами и отзывами пользователей.

«Потенциальные ловушки при попытке измерить негативный риск или ущерб включают в себя тот факт, что разработка показателей часто является институциональной задачей и может непреднамеренно отражать факторы, не связанные с лежащим в основе воздействием», — предупреждает отчет. «Измерение рисков ИИ включает в себя отслеживание метрик для достоверных характеристик, социального воздействия и конфигураций человека и ИИ».

Последним шагом в стратегии смягчения последствий RMF ИИ является «Управление», основная функция которого заключается в распределении ресурсов для снижения рисков и обеспечении непрерывного внедрения ранее установленных механизмов.

«Пользователи Framework расширят свои возможности для всесторонней оценки надежности системы, выявления и отслеживания существующих и возникающих рисков и проверки эффективности показателей», — говорится в отчете.

Владельцы бизнеса, участвующие в AI RMF, также выразили оптимизм по поводу рекомендаций этой структуры. Наврина Сингх, генеральный директор ИИ-стартапа Credo.AI и член Национального консультативного комитета по искусственному интеллекту Министерства торговли США, сказала, что клиенты, которым нужны решения ИИ, хотят иметь более целостные планы для смягчения предвзятости.

«Большинство наших клиентов… действительно ищут механизм для наращивания потенциала по внедрению ответственного ИИ, который очень хорошо зарекомендовал себя в функции «Управление» NIST AI RMF», — сказала она на панели после выпуска RMF. «Компоненты «Карта, измерение, управление» и то, как они могут быть реализованы в контексте, во всех этих конкретных случаях использования в этих организациях, — это следующий шаг, который хотят сделать большинство наших клиентов».

Новое руководство было встречено широкой двухпартийной поддержкой: член палаты представителей Зои Лофгрен, штат Калифорния, и член палаты

представителей Фрэнк Лукас, штат Оклахома, оба отправили поздравительные сообщения по случаю запуска.

«Используя подход, подтверждающий права, структура может максимизировать выгоды и снизить вероятность любой степени вреда, который могут принести эти технологии», — сказал Лофгрен на брифинге для прессы.

Участие сообщества из различных групп секторов имело решающее значение для разработки структуры. Алондра Нельсон, заместитель директора по науке и обществу в Управлении науки и технической политики Белого дома, сказала, что ее офис был одним из организаций, которые внесли значительный вклад NIST в AI RMF 1.0. Она добавила, что эта структура, как и Билль о правах ИИ Белого дома, ставит на первое место человеческий опыт и влияние алгоритмов ИИ.

«AI RMF признает, что, когда речь идет об ИИ и алгоритмах машинного обучения, мы никогда не можем рассматривать технологию вне контекста ее воздействия на людей», — сказала она. «Соединенные Штаты применяют принципиальный и изощренный подход к ИИ, который продвигает американские ценности и решает сложные задачи этой технологии, и мы должны гордиться этим».

Подобно Биллю о правах ИИ, AI RMF NIST является добровольной структурой, не предусматривающей никаких наказаний или вознаграждений, связанных с ее принятием. Несмотря на это, Locascio надеется, что фреймворк будет широко использоваться, и просит продолжать отзывы сообщества, поскольку агентство планирует выпустить обновление этой весной…» ***(Alexandra Kelley. NIST Debuts Long-Anticipated AI Risk Management Framework // Nextgov (https://www.nextgov.com/emerging-tech/2023/01/nist-debuts-long-anticipated-ai-risk-management-framework/382251/). 26.01.2023).***

***

«ChatGPT — это горячее приложение для искусственного интеллекта (ИИ) на данный момент. Если вы один из немногих, кто еще не сталкивался с этим, то это очень сложный чат-бот с генеративным искусственным интеллектом, работающий на большой языковой модели OpenAI GPT-3 (LLM). По сути, это означает, что это компьютерная программа, которая может понимать и «разговаривать» с нами способом, очень близким к разговору с реальным человеком. При этом очень умный и знающий человек, который знает около 175 миллиардов единиц информации и способен почти мгновенно вспомнить любую из них…

Правда в том, что ChatGPT — и, что более важно, будущие итерации технологии — могут применяться как для кибератак, так и для киберзащиты. Это связано с тем, что базовая технология, известная как обработка естественного языка или генерация естественного языка (NLP/NLG), может легко имитировать письменный или устный человеческий язык, а также может использоваться для создания компьютерного кода.

Во-первых, мы должны охватить одну важную оговорку. OpenAI, создатели GPT-3 и ChatGPT, включили некоторые довольно строгие меры безопасности, которые теоретически предотвращают его использование в злонамеренных целях.

Это делается путем фильтрации контента для поиска фраз, которые предполагают, что кто-то пытается использовать его таким образом.

Например, попросите его создать приложение-вымогатель (программное обеспечение, которое шифрует данные цели и требует денег, чтобы сделать его снова доступным), и он вежливо откажет.

«Извините, я не могу писать код для программы-вымогателя… моя цель — предоставлять информацию и помогать пользователям… а не поощрять вредоносные действия», — сказал он мне, когда я спросил его в качестве эксперимента.

Однако некоторые исследователи говорят, что им уже удалось найти обходной путь для этих ограничений. Кроме того, нет никакой гарантии, что будущие версии технологии LLM/NLG/NLP вообще будут включать такие меры безопасности.

Некоторые из возможностей, которые может иметь в своем распоряжении злонамеренная сторона, включают следующее:

Написание более официальных или правильно звучащих мошеннических и фишинговых электронных писем — например, поощрение пользователей делиться паролями или конфиденциальными личными данными, такими как информация о банковском счете. Это также может автоматизировать создание многих таких электронных писем, персонализированных для разных групп или даже отдельных лиц.

Автоматизация общения с жертвами мошенничества. Если кибер-вор пытается использовать программу-вымогатель для вымогательства денег у жертв, то можно использовать сложный чат-бот, чтобы увеличить их способность общаться с жертвами и обсуждать с ними процесс выплаты выкупа.

Создание вредоносного ПО. Поскольку ChatGPT демонстрирует, что алгоритмы NLG/NLP теперь можно использовать для профессионального создания компьютерного кода, это может быть использовано для того, чтобы позволить практически любому создавать свои собственные вредоносные программы, предназначенные для слежки за действиями пользователей и кражи данных для заражения систем. с программами-вымогателями или создать любое другое вредоносное программное обеспечение.

Встраивание языковых возможностей в саму вредоносную программу. Это потенциально позволит создать совершенно новое поколение вредоносных программ, которые могут, например, читать и понимать все содержимое компьютерной системы цели или учетной записи электронной почты, чтобы определить, что является ценным, а что нет. должны быть украдены. Вредоносное ПО может даже «подслушивать» попытки жертвы противостоять ему — например, разговор с персоналом службы поддержки — и соответствующим образом адаптировать свою собственную защиту.

Как можно использовать ChatGPT и последующие технологии в киберзащите?

У ИИ в целом есть потенциальные приложения как для атаки, так и для защиты, и, к счастью, это не исключение для ИИ на основе естественного языка.

Выявление фишинговых атак. Анализируя содержимое электронных и текстовых сообщений, можно предсказать, могут ли они быть попытками обманом заставить пользователя предоставить личную информацию или информацию, которую можно использовать.

Написание программного обеспечения для защиты от вредоносных программ. Поскольку он может писать компьютерный код на ряде популярных языков, включая Python, Javascript и C, его потенциально можно использовать для помощи в создании программного обеспечения, используемого для обнаружения и уничтожения вирусов и других вредоносных программ.

Обнаружение уязвимостей в существующем коде. Хакеры часто используют плохо написанный код для поиска эксплойтов, таких как возможность переполнения буфера, что может привести к сбою системы и возможной утечке данных. Алгоритмы NLP/NLG потенциально могут обнаруживать эти уязвимые места и генерировать предупреждения.

Аутентификация. Этот тип ИИ потенциально может использоваться для аутентификации пользователей путем анализа того, как они говорят, пишут и печатают.

Создание автоматических отчетов и сводок. Его можно использовать для автоматического создания простым языком сводок об атаках и угрозах, которые были обнаружены или отражены, или тех, от которых организация, скорее всего, станет жертвой. Эти отчеты можно настроить для разных аудиторий, таких как ИТ-отделы или руководители, с конкретными рекомендациями для разных людей.

Я работаю в сфере кибербезопасности – представляет ли это угрозу для моей работы?

В настоящее время ведутся споры о том, может ли ИИ привести к массовым потерям рабочих мест и избыточности среди людей. Мое мнение таково, что хотя некоторые рабочие места неизбежно исчезнут, вполне вероятно, что вместо них будут созданы новые. Что еще более важно, скорее всего, будут потеряны те работы, которые требуют в основном рутинной, повторяющейся работы, такой как установка и обновление фильтров электронной почты и программного обеспечения для защиты от вредоносных программ.

С другой стороны, те, которые останутся или будут вновь созданы, будут требовать более творческих, творческих и человеческих навыков. Это будет включать в себя развитие опыта в области инженерии машинного обучения для создания новых решений, а также развитие и формирование культуры осведомленности о кибербезопасности в организациях, наставничество сотрудников в отношении угроз, которые не может быть остановлен ИИ (например, опасности написания данных для входа в систему на почте). — отмечается в нем) и разработка стратегических подходов к кибербезопасности.

Понятно, что благодаря ИИ мы вступаем в мир, в котором машины заменят часть более рутинной «мыслительной» работы, которую необходимо выполнять. Подобно тому, как предыдущие технологические революции привели к замене рутинной ручной работы машинами, квалифицированная ручная работа, такая как столярное или слесарное дело, по-прежнему выполняется людьми. На мой взгляд, революция ИИ, вероятно, окажет такое же влияние. Это означает, что

информационные и умственные работники в областях, которые могут быть затронуты, таких как кибербезопасность, должны развивать способность использовать ИИ для расширения своих навыков, продолжая развивать «мягкие» наборы человеческих навыков, которые вряд ли будут заменены в ближайшее время». ***(Bernard Marr. How Dangerous Are ChatGPT And Natural Language Technology For Cybersecurity? // Forbes (https://www.forbes.com/sites/bernardmarr/2023/01/25/how-dangerous-are-chatgpt-and-natural-language-technology-for-cybersecurity/?sh=60c2cad04aa6). 25.01.2023).***

***

Кіберзлочинність та кібертерроризм

«Скандально відомий ексголова збанкрутілої біржі FTX Сем Бенкман-Фрід опублікував нову заяву, в якій він представив свою версію причин краху його платформи. На думку шахрая, головним винуватцем банкрутства FTX є не Бенкман-Фрід та його махінації з клієнтськими коштами, а керівник найбільшої біржі Binance Чанпен Чжао.

За словами SBF, керівник Binance скористався рецесією ринку криптовалют і спровокував крах Alameda Research, що в результаті призвело до банкрутства FTX, оскільки компанія мала велику позицію на криптобіржі. Бенкман-Фрід переконаний, якби Binance не втрутилась, Alameda втрималася б на плаву навіть після падіння ринку на 80%.

При цьому колишній CEO FTX запевнив, що навіть зараз біржа здатна майже повністю повернути всі кошти своїм клієнтам. Бенкман-Фрід заявив, що біржа віддала б кошти ще раніше, втім на неї «спчинили тиск», щоб змусити заявити про своє банкрутство…». ***(Найбільший криптовалютний шахрай звинуватив голову Binance у своїх проблемах // No worries! (https://noworries.news/najbilshyj-kryptovalyutnyj-shahraj-zvynuvatyv-golovu-binance-u-svoyih-problemah/). 13.01.2023).***

***

«Іспанська фірма з кібербезпеки та ПЗ Panda Security передбачає «сплеск шахрайств та спроб масового викрадення віртуальних активів» у 2023 році. Фірма заявила, що хакери з Північної Кореї намагатимуться «використати відновлений суспільний інтерес до криптовалюти», коли ринок оговтається після криптозими. Аналітики впевнені що Пхеньян «дедалі більше зосереджуватиметься на незаконній кібердіяльності для крадіжок криптовалют».

Цифрові активи стали важливим джерелом фінансування для північнокорейських ядерних програм і розробки зброї масового ураження. Аналітики неодноразово стверджували, що саме через крадіжку та відмивання криптовалюти Північна Корея змогла запустити 70 балістичних ракет у 2022 році - і це попри санкції цивілізованого світу. Південнокорейські ЗМІ зазначають, що для фінансування ядерних розробок Пхеньяну знадобиться «іноземна валюта», а це означає, що «зростання незаконної кібердіяльності буде неминучим». Мова йде, перш за все, за найвідоміше хакерське угруповування Lazarus Group.

Претензії іспанських експертів з кібербезпеки з'явилися після заяв Національної розвідувальної служби Південної Кореї (NIS). Відомство нещодавно повідомило, що за останні п'ять років північнокорейські хакери вкрали криптоактиви на суму приблизно 1,2 мільярда доларів, причому більшу частину цієї суми поцупили у 2022 році. NIS погоджується з іспанськими колегами і також припускає зростання кількості хакерських атак на замовлення Пхеньяна цього року.

Panda Security вважає, що на перспективні криптовалютні злочини ООН, швидше за все, відповість черговими санкціями. Провайдери безпеки підкреслюють, що зараз Пхеньян використовує фіктивні криптогаманці та клони-додатки криптобірж, які при інсталяції поширюють вірус «троян». Шкідливе ПЗ компрометує комп'ютери своїх жертв, дозволяючи хакерам проникнути туди та згодом викрасти монети». ***(Крадіжки криптовалют зростатимуть через хакерські атаки // No worries! (https://noworries.news/kradizhky-kryptovalyut-zrostatymut-cherez-hakerski-ataky/). 09.01.2023).***

***

«Гері Хармон — брат засновника криптовалютного міксера Helix Ларрі Хармона — визнав себе винним у крадіжці понад 712 BTC. На цей час криптовалюту конфіскували. Згідно з пресрелізом Міністерства юстиції, 31-річному зловмиснику з Клівленда загрожує 40 років в'язниці. Судове засідання щодо винесення вироку призначено на 17 березня.

У лютому 2020 Ларрі Хармона заарештували у США за підозрою у відмиванні понад $ 300 млн через даркнет-ринки. Окрім коштів у BTC, ETH та

DOGE, правоохоронці вилучили у хакера й фізичний біткоїн-гаманець Trezor. Щоправда, тоді поліція так і не змогла отримати доступу до криптовалюти.

Гері Хармон скористався обліковими записами брата і таємно переслав понад 712 BTC з його рахунків на свій біткоїн гаманець, чим перешкодив конфіскації коштів. Частину вкрадених криптовалют Хармон витратив на покупки предметів розкоші та задоволення власних потреб.

Вже у серпні 2021 року Ларрі Хармон визнав себе винним у відмиванні понад $ 300 млн через криптоміксер Helix. Тож його брату не залишилося нічого, як повернути владі 712 BTC ($ 12,3 млн за курсом на момент написання новини)…». ***(Американський хакер вкрав 712 біткоїнів в уряду // No worries! (https://noworries.news/amerykanskyj-haker-vkrav-712-bitkoyiniv-v-uryadu/). 09.01.2023).***

***

«Люк Дашир, один з основних розробників Bitcoin Core, втратив 200 BTC внаслідок злому, що відбувся 31 грудня. Криптоентузіаст запевняє, що ця сума — майже всі його заощадження у цифрових активах.

За словами потерпілого, він підозрює, що хакер якимось чином отримав доступ до його PGP-ключа. Деякі користувачі пов'язують цю подію з більш ранньою атакою хакерів, що відбулася 17 листопада. Тоді, у своїх соціальних мережах, відомий розробник поділився інформацією про компрометацію його сервера зловмисниками та закликав усіх бути обережнішими.

Дашир заявив, що не має жодного уявлення про те, яким чином злочинці отримали доступ до його гаманця. За його словами, він би навіть не помітив факту злому, якби не отримав сповіщення про спроби входу в систему у листах від Coinbase та Kraken.

Інцидент привернув увагу спільноти. У тому числі і її відомих представників. Серед них був голова Binance Чанпен Чжао. Підприємець висловив розробнику свої співчуття та пообіцяв заморозити вкрадені кошти, якщо вони раптом опиняться на Binance:

«Шкода, що ти так багато втратив. Повідомив нашу службу безпеки для це. Якщо ми побачимо шахрая, ми його заморозимо. Якщо є ще щось, з чим ми можемо допомогти, будь ласка, дай нам знати. Ми часто стикаємося з хакерами та підтримуємо відносини з правоохоронними органами по всьому світу».

У той же час деякі з криптоентузіастів вважають, що злому насправді не було. Зникнення коштів вони пов'язують з тим, що можливо, хтось із користувачів, які займаються підбором приватних ключів для отримання доступу до загублених BTC, випадково підібрав сід-фразу і авторизувався в гаманці розробника. Але і це ще далеко не найдивніша з версій — частина користувачів прямим текстом звинувачують Дашира у брехні. Вони впевнені, що розробник просто інсценував злом для того, щоб уникнути необхідності сплати податків». ***(В ніч на 1 січня одного з головних розробників біткоїна зламали хакери // No worries! (https://noworries.news/v-nich-na-1-sichnya-odnogo-z-golovnyh-rozrobnykiv-bitkoyina-zlamaly-hakery/). 02.01.2023).***

***

«С тех пор, как полиция закрыла рынок Hydra, российские конкуренты борются за долю рынка

Конкуренция между русскоязычными рынками даркнета остается жесткой после ликвидации лидера рынка Hydra в апреле прошлого года многонациональной правоохранительной операцией.

На карту поставлена доля рынка, которая может составить до миллиардов долларов для любой платформы, способной облегчить поток всего, от незаконных наркотиков и вредоносных программ до поддельных удостоверений личности и украденных данных платежных карт. Только Hydra заработала более 1,3 миллиарда долларов в 2020 году, отчасти благодаря услугам по отмыванию денег, которые она предлагала.

Соперничество обещает быть интенсивным — если судить по последнему развитию рынка даркнета Solaris, который, по оценкам, контролировал 25% торговли наркотиками в даркнете. На прошлой неделе он пережил темный веб-эквивалент враждебного поглощения: его взломали.

Относительный новичок Kraken — не связанный с законной одноименной криптовалютной биржей — утверждает, что плохая «операционная безопасность» Solaris позволила легко взломать его всего за 72 часа, сообщает исследовательская компания Elliptic.

13 января пользователи Solaris, пытавшиеся получить доступ к рынку, «были встречены перенаправлением на Kraken с уведомлением об успешном захвате киберинфраструктуры Solaris, репозитория GitLab и исходных кодов проекта», — сообщает Эрай Арда Акартуна, старший Аналитик криптоугроз в Elliptic. «Многие группы продавцов, связанные с Kraken, на форуме WayAway» — связанные с Kraken — «соперничают за найм бывших продавцов незаконных товаров и услуг Solaris».

Оглядываясь назад, можно сказать, что для «Соляриса» написанное было на стене на нескольких фронтах.

В конце прошлого года Solaris попыталась исключить конкуренцию, сообщив своим 3480 владельцам виртуальных магазинов, что внесет в черный список всех, кто также продает на WayAway и Kraken, сообщила фирма по кибербезопасности Resecurity. В последующий список «врагов Solaris» были добавлены конкурирующие рынки OMG!OMG! и Рутор в черный список, что предвещает какие-то разборки.

Связи с KillNet

Проблемы Solaris также косвенно связаны с его связью с группой хактивистов KillNet, которая была запущена в начале 2022 года и была связана с прокремлевскими распределенными атаками типа «отказ в обслуживании».

KillNet была связана с 84 известными атаками, сообщает CyberPeace Institute, независимая и нейтральная неправительственная организация. Целями были Европарламент, веб-сайты аэропортов США, Украина и ее союзники и даже конкурс песни «Евровидение».

Но KillNet также, похоже, преследовала рынок наркотиков Rutor от имени Solaris, сообщила ZeroFox Intelligence в октябре прошлого года.

«KillNet атакует конкурентов Solaris, и Solaris, скорее всего, платит KillNet за предоставляемые услуги», — сказал ZeroFox. Пытаясь сфальсифицировать свои действия, KillNet в разное время заявляла, что Rutor находится в ведении Службы безопасности Украины, СБУ (абсолютно необоснованное утверждение), а также что она преследовала Rutor за продажу запрещенных наркотиков россиянам. «KillNet также заявила, что 50% доходов, полученных от администратора Rutor, были направлены на помощь детским домам в Российской Федерации», — сообщил ZeroFox. Доказательства в поддержку этого утверждения не были опубликованы.

Есть более чем неподтвержденные свидетельства связи между двумя группами. Elliptic сообщает, что биткойн-средства на сумму более 44 000 долларов были переведены из Solaris на кошельки KillNet, по всей видимости, для DDoS-атак.

В октябре прошлого года KillNet публично поблагодарил Solaris за «огромную поддержку». Это замечание прозвучало, когда российское правительственное пропагандистское издание RT взяло интервью у основателя KillNet, известного под псевдонимом Killmilk.

Киллмилк сказал о Solaris: «Я не знаю, откуда они, но я давно знаю этих профессионалов. Спасибо за их внимание к нам, KillNet движется вперед полным ходом».

KillNet страдает от проникновения

Связи между KillNet и Solaris побудили эксперта по кибербезопасности из Висконсина Алекса Холдена, украинца, уехавшего из Киева в подростковом возрасте, попытаться разрушить рынок даркнета. Холден говорит, что прошлым летом он успешно внедрился в Solaris и начал искать слабые места, чтобы получить доступ к частям его инфраструктуры, предназначенным только для администраторов.

В прошлом месяце Холден сделал свой первый публичный шаг против Solaris, когда он использовал свой доступ для перенаправления 1,6 биткойнов — тогда это стоило около 25 000 долларов — из кошелька, принадлежащего операторам рынка даркнета. Он отправил биткойны в украинскую благотворительную организацию по оказанию гуманитарной помощи Enjoying Life вместе с 8000 долларов из собственных денег, как впервые сообщил Forbes.

«Мы гордимся еще одним важным шагом в нашей борьбе с киберпреступностью и KillNet», — написала Hold Security в твиттере в прошлом месяце. «Благодаря инсайдерскому доступу к российской наркоплатформе Solaris мы смогли получить большую часть их данных. Мы также смогли перенаправить деньги от продажи наркотиков на благотворительность в Украине».

В ответ администраторы Solaris «демонтировали большую часть его инфраструктуры» для того, что, как они утверждали, будет «крупным обновлением», сообщает Hold Security. «Они изо всех сил старались опровергнуть историю Forbes — за исключением денежного перевода — уверяя своих клиентов, что их новая версия будет больше и лучше. Все это было ложью».

Чтобы еще больше подчеркнуть связи между KillNet и его партнером по рынку наркотиков в даркнете, а также «привлечь внимание к его все еще уязвимой

платформе», 12 января Холден выложил обширные объемы данных, которые он собрал, проникнув в Solaris.

Выгруженные данные включают в себя сценарии развертывания серверов и ключи SSH, скрытые сервисные ключи Onion для своих сайтов на основе Tor, исходный код для «системы AntiDDoS Solaris Guard», базы данных SQL для ряда магазинов с удаленной информацией о криптовалютных кошельках и данные MongoDB. дамп, содержащий общедоступные и частные сообщения от рынка, говорит он.

Затем Solaris перешел к Kraken, который заявил, что его трехдневная хакерская атака, завершившаяся всего через 22 дня после выхода отчета Forbes, прошла незамеченной администраторами Solaris, сообщает Elliptic.

По словам Акартуна из Elliptic, раскрытие в декабре 2022 года того, что системы Kraken были взломаны исследователем кибербезопасности, несомненно, побудило конкурентов исследовать системы рынка на наличие уязвимостей, которые можно использовать, чтобы лучше захватить свою долю рынка.

Исчезновение Соляриса является напоминанием о том, что все, кажется, остается справедливым не только в любви и войне, но и в соперничестве на русскоязычном рынке даркнета». ***(Mathew J. Schwartz. Hostile Takeover: Kraken Hacks Rival Darknet Market Solaris // Information Security Media Group, Corp. (https://www.govinfosecurity.com/hostile-takeover-kraken-hacks-rival-darknet-market-solaris-a-20986). 20.01.2023).***

***

«Сотни округов США продолжают работать с ручкой и бумагой после того, как на прошлой неделе кибератака на их поставщика управления цифровыми записями нарушила методы просмотра, добавления и редактирования государственных записей.

Сторонний поставщик Cott Systems, поставщик облачных решений, проинформировал своих клиентов о том, что 26 декабря на системы компании была нанесена «организованная кибератака», которая привела к «необычной активности» на ее серверах. Компания ответила отключением от сети. свои серверы, чтобы изолировать вторжение, сказал Котт в уведомлении, переданном округу Рокленд в Нью-Йорке.

Cott Systems помогает управлять государственными данными, в том числе публичными записями, земельными записями и судебными делами. Согласно ее веб-сайту, компания обслуживает более 400 местных органов власти в 21 штате и имеет давние связи с несколькими национальными и международными организациями.

Приостановка работы серверов вынудила сотни местных органов власти прибегнуть к ручным процессам, что замедлило обработку свидетельств о рождении, разрешений на брак и операций с недвижимостью.

Компания уведомила ФБР и Министерство внутренней безопасности об инциденте, но заявляет, что нет «абсолютных» сроков возобновления обслуживания всей линейки продуктов, которая включает в себя пять систем,

используемых местными клерками и регистраторами для управления государственными и земельными записями, собственностью. дела и судебные дела.

Компания не раскрыла подробностей об исполнителе угрозы, ответственном за нападение, но заявила, что «и ФБР, и DHS указали, что они знают об этой конкретной группе преступников, действующих по всему миру, и проводят расследование». Котт не ответил на запрос Information Security Media Group о дополнительной информации о группе угроз или ее индикаторах компрометации, но сказал, что дополнительная информация будет предоставлена по мере продолжения расследования.

Признаки замедления

Волновой эффект кибератаки в настоящее время наблюдается в различных округах по всей стране, поскольку темп их работы замедляется.

По крайней мере шесть округов в Северной Каролине были заблокированы в своих системах записи актов гражданского состояния и вернулись к обновлению записей вручную. «Все происходит гораздо медленнее», — сказал WRAL-TV Скотт Роджерс, помощник менеджера округа Нэш. Он добавил, что после нападения округ не смог выдать новые лицензии на брак или провести новые сделки с недвижимостью.

Сотрудник прихода Ливингстон, штат Луизиана, где Котт предоставляет электронные услуги, сообщил информационному агентству WAFB9, что «обходной путь заключался в использовании ручек для временных меток новых документов и поиске ценных записей в грудах физических копий».

Клерки округа из Коннектикута и Миссисипи также сообщили об аналогичных замедлениях на прошлой неделе, поскольку службы не работали.

Данные не потеряны

В уведомлении округа Рокленд в понедельник генеральный директор Cott Systems Дебора Болл подтвердила, что базы данных компании «находятся в хорошем состоянии» и что 93% ее инфраструктуры исправлено. Она добавила, что ни одна из данных компании не была потеряна или повреждена». ***(Mihir Bagwe. Cyberattack on Records Vendor Affects Scores of US Counties // Information Security Media Group, Corp. (https://www.govinfosecurity.com/cyberattack-on-records-vendor-affects-scores-us-counties-a-20856). 04.01.2023).***

***

«…Согласно анализу Cybersecurity Venture, глобальные ежегодные убытки от киберпреступлений могут превысить 8 триллионов долларов в 2023 году.

Это число может даже занижать проблему, согласно данным Security Intelligence, которые подсчитали, что только американские финансовые учреждения потеряли около 1,2 миллиарда долларов в результате атак программ-вымогателей в 2021 году, что почти на 200% больше, чем в предыдущем году. Если этот показатель будет расти такими же темпами, глобальные убытки от киберпреступности могут достичь 16 триллионов долларов в 2023 году.

Однако финансовые учреждения — не единственная мишень для киберпреступников, которые использовали новые технологии и слабые места в системах для нападения на всех, от малого бизнеса до отдельных людей.

В связи с тем, что в 2023 году ожидается всплеск этих преступлений, вот пять киберпреступлений, которых следует опасаться в этом году.

Сканирование QR-кодов может скомпрометировать ваши личные данные

QR-коды стали обычным явлением для пользователей смартфонов в последние годы, они используются для быстрой передачи данных, таких как информация о доставке или меню ресторана.

Тем не менее, эксперты предупреждают, что количество вредоносных QR-кодов растет, потенциально подвергая людей опасным веб-сайтам, которые могут загружать их личные данные или позволять хакерам отслеживать каждое их движение через приложения с поддержкой геолокации.

«Киберпреступники вмешиваются как в цифровые, так и в физические QR-коды, чтобы заменить законные коды вредоносными кодами», — говорится в предупреждении ФБР о растущей угрозе.

По данным ФБР, вредоносные коды могут предлагать пользователям поддельный веб-сайт или приложение ввести логин или финансовую информацию, что позволит злоумышленнику легко украсть деньги.

«Вредоносные QR-коды также могут содержать встроенное вредоносное ПО, позволяющее преступнику получить доступ к мобильному устройству жертвы и украсть ее местоположение, а также личную и финансовую информацию», — говорится в предупреждении. «Киберпреступник может использовать украденную финансовую информацию для вывода средств со счетов жертв».

Чтобы не стать жертвой, ФБР советует пользователям смартфонов никогда не загружать приложение, когда будет предложено сделать это после сканирования QR-кода. Агентство также предлагает сохранять бдительность в отношении того, какие ссылки предлагает вам открыть сканирование QR-кода, и никогда не использовать сторонние приложения для сканирования кодов, вместо этого придерживаясь встроенной функции сканирования QR-кода, встроенной в ваш смартфон.

Ожидается, что угроза программ-вымогателей продолжит расти

Атаки программ-вымогателей, которые угрожают скомпрометировать личные данные пользователя или заблокировать доступ к ним до тех пор, пока не будет выплачен выкуп, почти так же стары, как и сам Интернет. Тем не менее, эксперты предупреждают, что в 2023 году ожидается, что старая тактика станет более серьезной угрозой, поскольку киберпреступники адаптируются к инструментам, от которых люди зависели, чтобы обеспечить их безопасность.

«Программы-вымогатели ухудшаются, даже больше, чем мы прогнозировали», — предупредила швейцарская компания по кибербезопасности Acronis в своем отчете о киберугрозах за 2022 год.

В отчете нарисована мрачная картина на 2023 год, согласно которой глобальный ущерб от программ-вымогателей превысит 30 миллиардов долларов. Между тем, отчет Cybereason за этот год показал, что примерно 73% организаций

подверглись хотя бы одной атаке программ-вымогателей в 2022 году, по сравнению с 55% в 2021 году.

«Усложнение ИТ продолжает приводить к взломам и компрометации, что подчеркивает необходимость более целостных подходов к киберзащите», — говорится в отчете Acronis. «Существующая картина угроз кибербезопасности требует многоуровневого решения, которое сочетает в себе функции защиты от вредоносных программ, EDR, DLP, защиты электронной почты, оценки уязвимостей, управления исправлениями, RMM и резервного копирования».

Хакеры могут атаковать уязвимые цепочки поставок

Глобальные цепочки поставок, которые серьезно пострадали во время пандемии COVID-19, постепенно восстанавливаются, но 2023 год станет для них еще одним испытанием, поскольку киберпреступники попытаются воспользоваться их уязвимостью.

Согласно анализу BlackBerry, за последний год четыре из пяти организаций столкнулись с угрозами в своей цепочке поставок программного обеспечения. По словам BlackBerry, результаты этих уязвимостей привели к огромным затратам: 58% этих организаций столкнулись с операционными сбоями и потерей данных, 55% - с потерей интеллектуальной собственности и 49% - с финансовыми потерями.

Эта проблема не исчезнет в ближайшее время, заявила вице-президент BlackBerry по безопасности продуктов Кристин Гэдсби, предупредив организации, чтобы они тщательно следили за собственной кибербезопасностью.

«Неизвестные компоненты и отсутствие прозрачности в цепочке поставок программного обеспечения создают слепые зоны, содержащие потенциальные уязвимости, которые могут нанести ущерб не только одному предприятию, но и нескольким из-за потери данных и интеллектуальной собственности, операционного простоя, а также финансового и репутационного ущерба. воздействия», — сказал Гэдсби. «То, как компании отслеживают и управляют кибербезопасностью в своей цепочке поставок программного обеспечения, должно основываться не только на доверии».

Киберпреступники усилят атаки на электромобили

Стремление защитников окружающей среды сократить выбросы за счет перехода на электромобили вызвало бум в индустрии электромобилей, и за последние несколько лет электромобили стали более популярными.

Однако многие автомобили содержат технологии, уязвимые для атак киберпреступников, которые могут атаковать дисплей автомобиля, навигацию, климат-контроль и даже функции автономного вождения.

«Поскольку новые автомобили и электромобили стали более подключенными и автоматизированными, чем когда-либо прежде, они также подвергаются более высокому риску кибератак», — сказал Wards Auto ранее в этом году Стив МакЭвой, вице-президент автомобильного подразделения Expleo. «Электромобили не обязательно должны подвергаться большему риску, чем современные автомобили с ДВС — просто электромобили для максимизации своих характеристик, естественно, будут использовать самую современную

электрическую архитектуру, включая все виды подключения, которые по своей природе могут создать более высокий уровень риска».

Электросеть может стать новой линией фронта кибертерроризма

Атаки на уязвимую электрическую сеть страны могут вскоре привести к перебоям в подаче электроэнергии, нехватке топлива и препятствовать производству энергии.

Продолжающееся вторжение России в Украину послужило примером того, насколько опасными могут быть нападения на энергетическую инфраструктуру страны, погружающие гражданское население Украины во тьму и холод, когда жестокие зимние температуры охватывают всю страну.

Эксперты годами предупреждали, что электросеть США становится все более уязвимой для атак, будь то киберугроза со стороны государственного субъекта, такого как Россия, или международной террористической группировки.

«Я удивлюсь, если в какой-то момент электроэнергетическая компания перестанет работать из-за кибератаки? Нет. Если этого не произойдет в течение следующих пяти лет, я буду очень удивлен», — Дэнни Дженкинс, генеральный директор компании ThreatLocker, специализирующейся на кибербезопасности., сказал в интервью Forbes в прошлом году.

Агентство передовых оборонных исследовательских проектов Пентагона готовилось к такой возможности с 2015 года, инвестировав 118 миллионов долларов в проект под названием Системы быстрого обнаружения, изоляции и характеристики атак (RADICS).

Программа, которая продлилась до 2020 года, предложила 15 коммунальным компаниям возможность протестировать уязвимости и изучить случай атаки в реальных сценариях, что эксперты назвали поучительным опытом для компаний.

Однако другие эксперты утверждают, что США еще недостаточно сделали для предотвращения того, что может перерасти в разрушительную атаку.

«Насколько подвержена риску эта страна? Может быть, лучше спросить: сколько мы сделали, чтобы предотвратить что-то подобное тем сценариям, которые произошли в RADICS?» Об этом ранее в этом году заявил основатель Red Balloon Security Анг Цуй. «Я думаю, совершенно очевидно, что мы сделали недостаточно». ***(Michael Lee. Top 5 cybercrimes to watch out for in 2023 // FOX News Network, LLC (https://www.foxnews.com/us/top-five-cybercrimes-watch-out-for-2023). 05.01.2023).***

***

Діяльність хакерів та хакерські угруповування

«Прошлым летом российская хакерская группа, известная как Cold River, напала на три ядерные исследовательские лаборатории в США, согласно интернет-записям, просмотренным агентством Reuters и пятью экспертами по кибербезопасности.

В период с августа по сентябрь, когда президент Владимир Путин дал понять, что Россия будет готова использовать ядерное оружие для защиты своей территории, Cold River нацелился на Брукхейвенскую (BNL), Аргоннскую (ANL) и

Ливерморскую национальные лаборатории имени Лоуренса (LLNL), показав хакеров, создающих фальшивые страницы входа для каждого учреждения и отправляющих электронные письма ученым-ядерщикам, чтобы заставить их раскрыть свои пароли.

Агентство Reuters не смогло определить, почему лаборатории были атакованы, и была ли попытка вторжения успешной. Представитель BNL отказался от комментариев. LLNL не ответила на запрос о комментарии. Представитель ANL направил вопросы в Министерство энергетики США, которое отказалось от комментариев.

По словам исследователей кибербезопасности и западных правительственных чиновников, Cold River активизировала свою хакерскую кампанию против союзников Киева после вторжения в Украину. Цифровой блиц против американских лабораторий произошел, когда эксперты ООН вошли на территорию Украины, контролируемую Россией, чтобы осмотреть крупнейшую в Европе атомную электростанцию и оценить риск того, что, по словам обеих сторон, может стать разрушительной радиационной катастрофой на фоне сильных обстрелов поблизости.

Согласно интервью, проведенным девятью фирмами, занимающимися кибербезопасностью, Cold River впервые попала в поле зрения специалистов по разведке после атаки на министерство иностранных дел Великобритании в 2016 году. Агентство Reuters отследило учетные записи электронной почты, использованные в его хакерских операциях в период с 2015 по 2020 год, до ИТ-специалиста в российском городе Сыктывкар.

«Это одна из самых важных хакерских групп, о которых вы никогда не слышали», — сказал Адам Мейерс, старший вице-президент по разведке американской компании по кибербезопасности CrowdStrike. «Они участвуют в прямой поддержке информационных операций Кремля».

Федеральная служба безопасности России (ФСБ), агентство внутренней безопасности, которое также проводит шпионские кампании в пользу Москвы, и посольство России в Вашингтоне не ответили на запросы о комментариях по электронной почте.

Западные чиновники заявляют, что российское правительство является мировым лидером в области хакерских атак и использует кибершпионаж, чтобы шпионить за иностранными правительствами и отраслями, чтобы получить конкурентное преимущество. Однако Москва последовательно отрицает, что проводит хакерские операции.

Агентство Reuters представило свои выводы пяти отраслевым экспертам, которые подтвердили причастность Cold River к попыткам взлома ядерных лабораторий на основе общих цифровых отпечатков пальцев, которые исследователи исторически связывали с группой.

Агентство национальной безопасности США (АНБ) отказалось комментировать деятельность Cold River. Штаб-квартира глобальных коммуникаций Великобритании (GCHQ), ее аналог АНБ, не прокомментировала ситуацию. Министерство иностранных дел отказалось от комментариев.

'СБОР ИНФОРМАЦИИ'

В мае Cold River взломал и слил электронные письма, принадлежащие бывшему главе британской разведывательной службы МИ-6. По словам экспертов по кибербезопасности и сотрудников службы безопасности Восточной Европы, это была лишь одна из нескольких операций «взлома и утечки», проведенных в прошлом году хакерами, связанными с Россией, в ходе которых конфиденциальные сообщения были обнародованы в Великобритании, Польше и Латвии.

По данным французской фирмы по кибербезопасности SEKOIA.IO, в рамках другой недавней шпионской операции, направленной против критиков Москвы, компания Cold River зарегистрировала доменные имена, имитирующие как минимум три европейские НПО, расследующие военные преступления.

Попытки взлома, связанные с НПО, имели место непосредственно перед и после опубликования 18 октября доклада независимой следственной комиссии ООН, в котором было установлено, что российские силы несут ответственность за «подавляющее большинство» нарушений прав человека в первые недели войны на Украине, которую Россия назвала специальной военной операцией.

В сообщении в блоге SEKOIA.IO говорится, что, основываясь на своем нацеливании на неправительственные организации, Cold River стремилась внести свой вклад в «сбор российской разведывательной информации о выявленных доказательствах, связанных с военными преступлениями, и / или международных судебных процедурах». Агентство Reuters не смогло независимо подтвердить, почему Cold River нацелилась на НПО.

Комиссия по международному правосудию и подотчетности (CIJA), некоммерческая организация, основанная опытным следователем по военным преступлениям, заявила, что за последние восемь лет она неоднократно безуспешно подвергалась атакам поддерживаемых Россией хакеров. Две другие НПО, Международный центр ненасильственных конфликтов и Центр гуманитарного диалога, не ответили на запросы о комментариях.

Посольство России в Вашингтоне не ответило на запрос с просьбой прокомментировать попытку взлома CIJA.

Как сообщили Reuters исследователи в области безопасности, Cold River использовала такую тактику, как обманом заставляя людей вводить свои имена пользователей и пароли на поддельных веб-сайтах, чтобы получить доступ к своим компьютерным системам. Для этого Cold River использовала различные учетные записи электронной почты для регистрации доменных имен, таких как «goo-link.online» и «online365-office.com», которые на первый взгляд похожи на законные службы, управляемые такими фирмами, как Google и Microsoft, — заявили исследователи безопасности.

ГЛУБОКИЕ СВЯЗИ С РОССИЕЙ

В последние годы Cold River допустила несколько ошибок, которые позволили аналитикам по кибербезопасности установить точное местонахождение и личность одного из ее членов, что дает наиболее четкое указание на российское происхождение группы, по мнению экспертов из интернет-гиганта Google, британского оборонного подрядчика BAE и Американская разведывательная фирма Nisos.

Несколько личных адресов электронной почты, использованных для создания миссий Cold River, принадлежат Андрею Коринцу, 35-летнему ИТ-специалисту и культуристу из Сыктывкара, примерно в 1600 км (1000 миль) к северо-востоку от Москвы. Использование этих учетных записей оставило след цифровых доказательств от различных взломов до онлайн-жизни Коринца, включая учетные записи в социальных сетях и личные веб-сайты.

Билли Леонард, инженер по безопасности из группы анализа угроз Google, который расследует хакерские атаки в национальных государствах, сказал, что Коринец был замешан. «Google связал этого человека с российской хакерской группой Cold River и их ранними операциями», — сказал он.

Винцас Чизиунас, исследователь безопасности в Nisos, который также связал адреса электронной почты Коринца с деятельностью Cold River, сказал, что ИТ-специалист исторически был «центральной фигурой» в сыктывкарском хакерском сообществе. Чизиунас обнаружил ряд русскоязычных интернет-форумов, в том числе электронный журнал, где Коринец обсуждал хакерские атаки, и поделился этими сообщениями с Reuters.

Коринец подтвердил, что ему принадлежат соответствующие учетные записи электронной почты в интервью Reuters, но отрицал какие-либо сведения о Cold River. Он сказал, что его единственный опыт хакерства появился много лет назад, когда он был оштрафован российским судом за компьютерное преступление, совершенное во время делового спора с бывшим клиентом.

Агентство Reuters смогло отдельно подтвердить связи Коринца с Cold River, используя данные, собранные с помощью платформ исследования кибербезопасности Constella Intelligence и DomainTools, которые помогают идентифицировать владельцев веб-сайтов: данные показали, что адреса электронной почты Коринца зарегистрированы на многочисленных веб-сайтах, используемых в хакерских кампаниях Cold River. в период с 2015 по 2020 год.

Неясно, участвовал ли Коринец в хакерских операциях с 2020 года. Он не объяснил, почему использовались эти адреса электронной почты, и не ответил на дальнейшие телефонные звонки и вопросы по электронной почте». ***(James Pearson, Christopher Bing. Exclusive: Russian hackers targeted U.S. nuclear scientists // Reuters (https://www.reuters.com/world/europe/russian-hackers-targeted-us-nuclear-scientists-2023-01-06/). 07.01.2023).***

***

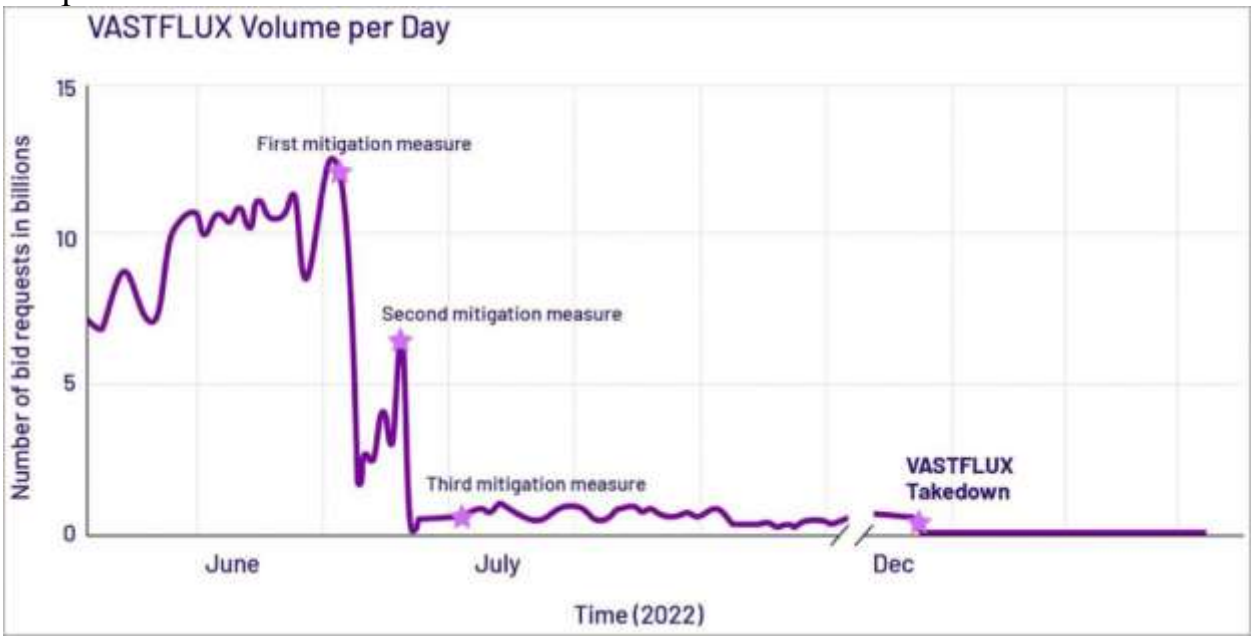
«Дослідники з безпеки підрозділу Satori, що працюють у компанії HUMAN, виявили масштабну хакерську схему, що отримала назву «Vastflux». Кіберзлочинці підробили понад 1700 відомих додатків для iOS — все для отримання прибутків з реклами.

Експерти з’ясували, що хакери впроваджували шкідливий JavaScript-код у рекламні оголошення, а потім «нашаровували» відеоплеєри з рекламою один на одний. Так, що жодного з них не було видно користувачеві — всі вони відображалися за активним вікном. Однак із кожного запущеного відео шахраї отримували прибуток від монетизації. «Нашаровувати» таким чином у зловмисників виходило до 25 відеоплеєрів одночасно.

```
[
  {
    "mvr": 5,
    "acap": "1",
    "id": "438952273",
    "group": "1",
    "freqCap": "0",
    "callbacks": {
    },
    "dmid": "377911121-463584956-644957944-438952273",
    "moat": {
      "rate": 0.01
    },
    "domainId": "466",
    "url": "https://ads.          .com/www/delivery/swfIndex.php?reqType=AdsSetup&protocolVersion=2.0&zoneId=13811951&appName=Differen
    600&deviceIfa=029cbc16-3fa7-4c6e-b25a-bda798e34e83&_fw_did_idfv=336F28C0-2458-4242-8029-83762AB47815&_fw_atts=3&loc=US&cb=[CB]&ip=
    "gtag": false,
    "timers": {},
    "type": "vast"
  },
  {
    "mvr": 5,
    "acap": "1",
    "id": "1419198560",
    "group": "1",
    "freqCap": "0",
    "callbacks": {
    },
    "dmid": "377911121-2027495463-1101989314-1419198560",
    "moat": {
      "rate": 0.01
    },
    "domainId": "466",
    "url": "https://ads.          .com/www/delivery/swfIndex.php?reqType=AdsSetup&protocolVersion=2.0&zoneId=23103426&schain=1.0,1!so
    &appName=Differences%20-%20Find%20&%20Spot%20them&appBundle=1445691600&loc=1445691600&appStoreUrl=https://apps.apple.com/us/app/di
    id1445691600&playerSize=480x320&_fw_us_privacy=&_fw_gdpr=0&_fw_gdpr_consent=&_fw_did_idfv=[APP_IDDF]&_fw_atts=",
    "gtag": false,
    "timers": {},
    "type": "vast"
```


Такий спосіб шахрайства назвали «Vastflux» — все через шаблон показу відеореклами «VAST» і метод ухилення «fast flux», який використовується кіберзлочинцями, щоб приховати фішингові сайти за мережею скомпрометованих хостів, шляхом швидкої зміни великої кількості IP-адрес і записів DNS, пов'язаних з одним доменом.

Хоча шахрайство з рекламою не є негативним для користувачів додатків, воно викликає зниження продуктивності пристроїв, збільшує витрату заряду батареї та трафіку, а також може призвести до перегріву пристрою. Відеореклама споживає набагато більше енергії, ніж статична реклама, а декілька прихованих відеоплеєрів — тим більше.



Щоб зупинити діяльність хакерів, спеціалісти з безпеки компанії HUMAN склали карту інфраструктури Vastflux і запустили три хвилі цільових дій у період з червня до липня 2022 року. Врешті-решт Vastflux на деякий час відключив свої

сервери C2 і скоротив свої операції, а 6 грудня рекламні операції зупинилися повністю…». ***(Хакери підробили понад 1700 додатків для iOS для заробітку на рекламі // No worries! (https://noworries.news/hakery-pidrobyly-ponad-1700-dodatkiv-dlya-ios-dlya-zarobitku-na-reklami/). 24.01.2023).***

***

«Історія зі зламом збанкрутілої криптовалютної біржі FTX, внаслідок якого фірма втратила майже $ 400 мільйонів, триває. Як стало відомо, невідомий хакер опублікував поради для свого «колеги» з відмивання викрадених $ 400 мільйонів.

Про ситуацію розповів директор Coinbase Конор Гроган, який помітив на Etherscan незвичний переказ ETH з одного гаманця на інший. Транзакція містила повідомлення, у якому хакер розповів викрадачеві коштів FTX як краще відмити величезну суму.

Відправник запропонував зловмиснику використовувати сервіси крипто-мікшування, що орієнтовані на конфіденційність, а не популярні рішення, такі як ChipMixer. Міксери дозволяють користувачам приховувати свої транзакції при переміщенні активів і є поширеним інструментом серед криптошахраїв. Користувач наголосив, що готовий поділитися з хакером додатковою інформацією про міксери та інші способи відмивання коштів та вказав своє ім'я в Telegram для подальшого зв’язку.

Наразі невідомо з якою метою ймовірний хакер надав власні поради викрадачу $ 400 мільйонів та чи не є це пасткою для зловмисника. Голова Coinbase порівняв таку спробу допомоги з холодними дзвінками у продажах, коли продавці телефонують до потенційних клієнтів, нав’язливо пропонуючи власний товар та послуги…». ***(Невідомий хакер публічно дав поради з відмивання криптовалюти іншому хакеру, який викрав $ 400 мільйонів // No worries! (https://noworries.news/nevidomyj-haker-publichno-dav-porady-z-vidmyvannya-kryptovalyuty-inshomu-hakeru-yakyj-vykrav-400-miljoniv/). 17.01.2023).***

***

«Lazarus Group украла 100 миллионов долларов у Blockchain Bridge в июне

ФБР США в понедельник подтвердило то, что уже давно говорят эксперты по безопасности Web3: спонсируемые государством северокорейские хакеры несут ответственность за кражу 100 миллионов долларов с блокчейн-моста Harmony Horizon.

На прошлой неделе Lazarus Group попыталась вывести из ограбления Horizon трофеи на сумму 63,5 миллиона долларов, используя криптомиксеры, платформу конфиденциальности смарт-контрактов Railgun и централизованные биржи, сообщил популярный исследователь безопасности Web3 ZackXBT. Криптовалютные биржи Binance и Huobi вмешались, чтобы заморозить небольшую часть средств, проходящих через их соответствующие платформы, сказал генеральный директор Binance Чанпэн Чжао, хотя ZackXBT добавил, что компании не смогли полностью помешать северокорейским хакерам обналичить деньги.

ФБР подтвердило в своем заявлении, что 13 января хакеры использовали Railgun для отмывания украденных монет Эфириума. Агентство также заморозило часть средств, сотрудничая с некоторыми поставщиками услуг виртуальных активов, где хакеры пытались конвертировать Эфириум в монеты. биткойн, говорится в сообщении. Сумма заблокированных средств не уточняется.

Федеральное агентство заявило, что «продолжит разоблачать и бороться с использованием Северной Кореей незаконной деятельности, включая киберпреступность и кражу виртуальной валюты, для получения доходов для режима», включая ее программы баллистических ракет и оружия массового уничтожения.

В июне аналитическая компания Elliptic заявила, что контрольные признаки взлома и последующего отмывания денег соответствуют действиям, предпринятым хакерами из Пхеньяна. Хотя в то время не было неопровержимых доказательств, Elliptic заявила, что Lazarus Group уже была замешана в нескольких крупных кражах криптовалюты и недавно обратила свое внимание на децентрализованные финансовые операции, включая мосты, которые позволяют передавать криптовалюты по сетям.

Северную Корею также сильно подозревают в том, что она стоит за взломом моста Ронина на сумму более 600 миллионов долларов в марте (см.: Северная Корея стоит за хищением Гармонии на 100 миллионов долларов, говорят исследователи).

Кампания TraderTraitor

По словам ФБР, Lazarus Group использовала кампанию вредоносного ПО под названием TraderTraitor для атаки на мост Harmony.

Хакеры обычно отправляют «большое» количество целевых фишинговых сообщений руководителям DevOps или системным администраторам криптовалютных компаний, предлагая им фальшивую высокооплачиваемую работу, которая может соблазнить сотрудников загрузить криптографическое приложение с вредоносным ПО. ФБР, Агентство по кибербезопасности и безопасности инфраструктуры и Министерство финансов. Хакеры используют проекты с открытым исходным кодом для разработки вредоносных приложений, которые, по-видимому, имеют инструменты для торговли криптовалютой или прогнозирования цен. Когда его пользователи «обновляют» свои приложения (предварительно разработанная вредоносная функция), вредоносное ПО загружает и выполняет вредоносную полезную нагрузку в системе для кражи данных, которые дадут им доступ к криптографии жертвы.

В случае с Horizon хакеры скомпрометировали закрытые ключи и выполнили транзакции, в результате которых были извлечены токены, хранящиеся в мосте, заявил в то время основатель Harmony Стивен Це. По сути, мост представлял собой контракт с несколькими подписями, который требовал одобрения от 2 из 5 адресов для подтверждения передачи, сообщил Information Security Media Group Уильям Каллахан, директор по правительственным и стратегическим вопросам Blockchain Intelligence Group. «Если какие-либо 2 из 5 адресов сообщали в контракте о переводе средств кому-то, то он это делал. В этом случае хакер, вероятно, скомпрометировал два адреса и заставил их перевести криптовалюту на свой

кошелек», — говорит Каллахан...» ***(Rashmi Ramesh. North Korean Hackers Attacked Horizon, Confirms FBI // Information Security Media Group, Corp. (https://www.govinfosecurity.com/north-korean-hackers-attacked-horizon-confirms-fbi-a-21008). 24.01.2023).***

***

«…Во вторник хакерская группа NoName057(16) атаковала несколько датских банков в ходе распределенной атаки типа «отказ в обслуживании», вызвав операционные задержки во многих пострадавших банках.

Очевидные цели включали некоторые из крупнейших финансовых учреждений, в том числе Jyske Bank и Sydbank. Arbejdernes Landsbank заявил, что пострадала его система онлайн-банкинга.

NoName057(16) в своем Telegram-канале заявил об атаках на Sydbank, Sparekassen Sjælland-Fyn, Bankinvest, Jyskebank.

Агентство Reuters сообщило, что хакеры также атаковали Bankdata, частную компанию, предоставляющую финансовые технологии. Хакеры также нацелились на Национальный банк Дании, который восстановил доступ после того, как атака на короткое время отключила его веб-сайт, сообщает Reuters.

NoName057(16) вместе с KillNet входит в число нескольких киберпреступных группировок, запускающих DDoS-атаки в предполагаемую поддержку российского правительства, которое продолжает свое вторжение в Украину.

NoName057(16) координирует свои действия с несколькими подгруппами для проведения атак на свои цели. Одной из таких групп является DDosia, через которую NoName предоставляет инструкции по использованию пользовательского инструмента, доступного на GitHub под тем же именем. В сентябре 2022 года NoName057(16) учредил финансовое вознаграждение для высокопоставленных участников, успешно проведших DDoS-атаки». ***(Akshaya Asokan. Danish Banks Are Targets of Pro-Russian DDoS Hacking Group // Information Security Media Group, Corp. (https://www.govinfosecurity.com/danish-banks-are-targets-pro-russian-ddos-hacking-group-a-20902). 10.01.2023).***

***

«Польская разведка в конце года выпустила предупреждение о российских хакерах, действующих в национальном киберпространстве, заявив, что они намерены дестабилизировать жизненно важного союзника Украины.

Польша является плацдармом для военной помощи Киеву и пунктом назначения для более чем 1,4 миллиона беженцев, бежавших от захватнической войны Москвы, которая идет уже 11-й месяц. Страна заявляет, что предоставила своему восточному соседу помощь в размере 9 миллиардов долларов.

Российские хакеры в Польше предшествовали вторжению в феврале 2022 года, но с тех пор враждебная активность усилилась, говорится в пятничном предупреждении Управления правительственного полномочного представителя по кибербезопасности.

Хакерские группы, «связанные с Кремлем», используют программы-вымогатели и распространяют атаки типа «отказ в обслуживании» и фишинговые атаки с целью «дестабилизации, запугивания и сеяния хаоса», пишет польское правительственное агентство.

«Россия хочет оказать давление на Польшу как на прифронтовую страну и ключевого союзника Украины на восточном фланге НАТО», — говорится в сообщении.

Предупреждение соответствует другим предупреждениям, в том числе декабрьскому официальному заявлению Microsoft, в котором говорится, что Россия может активизировать цифровые операции в Европе, включая дезинформацию (см.: Microsoft предупреждает о растущих российских цифровых угрозах Европе).

Исследователи безопасности из Microsoft ранее приписывали новую кампанию вымогателей, активную в Украине и Польше, тому же кремлевскому хакеру, ответственному за вредоносное ПО NotPetya. Злоумышленник связан с российской военной разведкой ГРУ и чаще всего известен под псевдонимом Sandworm, хотя Microsoft отслеживает его как Iridium.

Международные наблюдатели сомневаются в эффективности российских хакерских атак на территории Украины и приходят к выводу, что российские ракеты гораздо эффективнее уничтожают украинскую инфраструктуру, чем очистители данных. Сбор разведданных, а не уничтожение, вероятно, является главной киберугрозой для Киева, говорится в недавней статье, опубликованной Фондом Карнеги за международный мир.

Польская разведка ссылается на деятельность кампании, известной как GhostWriter, как на свидетельство российского шпионажа и дезинформации. Среди прочего, он использовал подставных лиц для распространения нарративов о том, что украинские беженцы являются обузой для экономики и системы здравоохранения Польши, а также разжигал опасения, что «неонацисты» будут использовать поток беженцев в Польшу для совершения терактов, угрожает разведывательная фирма Mandiant. сообщалось ранее в этом году. GhostWriter также пытался убедить украинцев в том, что польская криминальная группировка занимается извлечением органов у беженцев. Mandiant оценивает с «умеренной уверенностью», что близкий союзник России Беларусь как минимум частично несет ответственность за кампанию GhostWriter.

По словам Польши, помимо распространения дезинформации операторы GhostWriter атакуют учетные записи социальных сетей и адреса электронной почты польских общественных деятелей.

В предупреждении также говорится, что национальная группа реагирования на инциденты в области компьютерной безопасности обнаружила веб-сайт, выдающий себя за официальный правительственный сайт. Поддельный сайт собирал данные платежных карт, ложно утверждая, что жители Польши имеют право на получение гранта, финансируемого Европейским союзом. «Это типичная операция, направленная на сеяние хаоса, подрыв государства, а также сбор личных данных и вымогательство денег», — написал польский полпред по безопасности информационного пространства.

В нем также упоминается октябрьский инцидент, в результате которого сайт Сената Польши был нарушен через день после того, как палата единогласно проголосовала за признание России «террористическим режимом». Польша приписывает инцидент группе, обозначенной как NoName057(16)». ***(Prajeet Nair. Poland Sounds Alarm on Russian Hacking // Information Security Media Group, Corp. (https://www.govinfosecurity.com/poland-sounds-alarm-on-russian-hacking-a-20841). 03.01.2023).***

***

«Хакерская группа Blind Eagle вернулась из своего перерыва и проводит постоянную кампанию, направленную на испаноязычные цели в Колумбии и Эквадоре.

Конечная цель продвинутого субъекта постоянной угрозы — перехватить и получить доступ к банковским счетам жертв, для чего развертывается обновленный троян с открытым исходным кодом под названием QuasarRAT, сообщает компания Check Point, занимающаяся кибербезопасностью.

Список банков и других организаций, на которые нацелена эта кампания, включает: Banco AV Villas, Banco Caja Social, Banco de Bogotá, Banco Popular, Bancoomeva, BBVA Net Cash, Colpatria, Davivienda и TransUnion.

Trend Micro в сентябре 2021 года раскрыла методы работы Blind Eagle, которые в первую очередь ориентированы на атаки на государственные учреждения Колумбии.

Согласно отчету Trend Micro, APT традиционно использует общедоступные инструменты удаленного доступа и трояны, такие как njRAT, imminent monitor, ProyectoRAT, Warzone RAT, Async RAT, Lime RAT, Remcos RAT и BitRAT. Со временем APT переключается с одной RAT на другую. Продолжая эту тенденцию, Blind Eagle теперь использует модифицированную версию QuasarRAT, говорят исследователи Check Point.

Атака начинается с фишинговых писем, содержащих заминированную ссылку, которая запускает троянца Quasar RAT.

APT использовала сервер геофильтрации в одной кампании, которая перенаправляет запросы, сделанные за пределами Эквадора и Колумбии, на веб-сайт Налоговой службы Эквадора, что указывает на направленность APT.

Кампания не только сбрасывает RAT, но и использует более сложную цепочку заражения. Он использует законный mshta.exедвоичный файл для выполнения VBScript, встроенного в HTML-файл, чтобы в конечном итоге загрузить два скрипта Python, что добавляет новый этап в цепочку заражения.

Первый из двух ByAV2.py— это загрузчик в памяти, который запускает полезную нагрузку Meterpreter в формате DLL. Mp.py— еще один образец Meterpreter, полностью написанный на Python. Исследователи говорят, что цель этих двух сценариев может заключаться в том, что если один из образцов будет обнаружен антивирусным решением и удален, другой все еще может быть выполнен.

«В течение последних нескольких месяцев мы наблюдали за текущими кампаниями, организованными Blind Eagle, которые в основном придерживались

описанных выше TTP», — говорят исследователи. Сюда входят фишинговые электронные письма якобы от Министерства иностранных дел Колумбии, которые угрожают получателю проблемами, связанными с выездом из страны без решения бюрократических вопросов.

Вредоносные сценарии Blind Eagle APT позволяют злоумышленнику поддерживать постоянный бэкдор в системах жертв. Но «судя по набору его инструментов и обычным операциям, он явно больше заинтересован в киберпреступности и денежной наживе, чем в шпионаже», — говорят исследователи». ***(Mihir Bagwe. Blind Eagle APT Hunts Banking Victims in Colombia, Ecuador // Information Security Media Group, Corp. (https://www.govinfosecurity.com/blind-eagle-apt-hunts-banking-victims-in-colombia-ecuador-a-20879). 06.01.2023).***

***

«Российская группировка Killnet взломала совместно с белорусской Infinity Hackers BY серверы Налоговой службы США. Об этом стало известно от хакера Killmilk, возглавляющего российскую группировку.

Согласно данным «Лента.ру» со взломом серверов российским хакерам помогли их белорусские партнеры из Infinity Hackers BY. Данная группировка была создана из участников хакерского форума Infinity.

Инициаторы атаки анонсировали публикацию 188 млн строк из похищенной у Налоговой службы США базы данных, если Вашингтон сделает в сторону границ РФ и Беларуси еще один шаг. База данных содержит логины и пароли.

Из опубликованного Killmilk сообщения следует, что взломать серверы удалось через корпоративную сеть. Работник логистической службы государственного органа перешел по фишинговой ссылке во время просмотра порнографических роликов…» ***(Российские хакеры использовали порно для взлома Налоговой службы США // ProstoMOB (https://prostomob.com/130313-rossijskie-hakery-ispolzovali-porno-dlya-vzloma-nalogovoj-sluzhby-ssha). 17.01.2023).***

***

Вірусне та інше шкідливе програмне забезпечення

«Федеральне управління фінансового нагляду Німеччини (BaFin) опублікувало офіційне попередження про нове шкідливе ПЗ «Хрещений батько». Програма збирає дані користувачів у банківських та криптовалютних додатках. Правоохоронці BaFin заявили, що вірус орієнтований на понад 400 застосунків, що працюють не лише у самій Німеччині, а й у всьому світі.

Принцип роботи «Хрещеного батька» можна назвати класичним — ПЗ імітує сайти банківських чи криптовалютних програм та краде дані користувачів у момент залогінення. Більш того, вірус може надсилати push-повідомлення, щоб отримати коди двофакторної автентифікації.

На цей час фахівці BaFin намагаються розібратися, яким чином шкідлива програма потрапляє на пристрої користувачів. Експерти фіксували «троян» ще у 2021 році, проте тоді зловмисне програмне забезпечення було малоефективним.

Вперше вдосконалений та повністю готовий білд «Хрещеного батька» виявили у грудні 2022 на пристроях з ОС Android. На той момент програма була націлена на користувачів із 16 країн. Зараз «троян» в основному орієнтується на банківські додатки зі США, 110 платформ обміну криптовалютами, а також 94 криптогаманці.

Криптовалютні експерти підкреслюють, що крадіжки цифрових активів у 2023 році лише зростатимуть. Іспанська фірма з кібербезпеки та ПЗ Panda Security передбачає «сплеск шахрайств та спроб масового викрадення віртуальних активів» через зростання лояльності до криптовалют. Фірма заявила, що найбільше у зломах зацікавлена Північна Корея, тож слід очікувати нових експлойтів від найвідомішого злочинного кіберугруповування Lazarus Group». ***(Новий вірус для криптовалютних додатків краде дані про власників криптовалют // No worries! (https://noworries.news/novyj-virus-dlya-kryptovalyutnyh-dodatkiv-krade-dani-pro-vlasnykiv-kryptovalyut/). 10.01.2023).***

***

«Исследователи Proofpoint говорят, что TA444 адаптируется...

Поток спама, выпущенный в декабре прошлого года в попытке собрать учетные данные американских и канадских финансовых работников, был попыткой северокорейской коммерческой хакерской группы диверсифицировать поток своих доходов.

Исследователи из Proofpoint говорят, что группа, которую они отслеживают как TA444 в этом месяце, почти удвоила общий объем спама, рассылаемого за предыдущие 11 месяцев, — свидетельство того, что хакерская группа отражает «культуру стартапов в своей преданности доллару и рутинной работе».

TA444 пересекается с другими хакерскими группами Пхеньяна, известными как APT38, Bluenoroff, BlackAlicanto, Stardust Chollima и Copernicium group.

Северная Корея — это редкая страна, чьи спонсируемые государством хакеры совершают атаки ради финансовой выгоды своей страны. Не далее как во вторник ФБР США приписало кражу 100 миллионов долларов с криптовалютного моста Horizon северокорейским хакерам.

В 2019 году Организация Объединенных Наций подсчитала, что ограбления криптовалют и онлайн-банков позволили Пхеньяну также инвестировать 2 миллиарда долларов в разработку ядерного оружия и межконтинентальных баллистических ракет (см.: Северокорейские хакерские фонды Программы ОМУ, Отчет ООН предупреждает).

Proofpoint говорит, что не может исключить возможность того, что всплеск активности TA444 является свидетельством подработки. Если это так, то исследователи безопасности должны начать обнаруживать доказательства повторного использования инструментов и инфраструктуры, а также «продолжающееся отклонение от таргетинга в сторону от основных криптовалютных и финансовых учреждений».

Грег Лесневич, старший исследователь угроз в Proofpoint, говорит, что TA444 демонстрирует способность тестировать продукты на лету.

Злоумышленник использует фишинговые электронные письма для первоначального доступа. По его словам, он обычно содержит хорошо продуманный контент-приманку, который включает в себя анализ блокчейнов криптовалюты, возможности трудоустройства в престижных фирмах и даже корректировку заработной платы.

Фишинговые электронные письма доставляют полезную нагрузку, доступную в двух форматах файлов — запутанном LNK-файле и цепочке, начинающейся с документов, использующих удаленные шаблоны. TA444 продолжает использовать оба метода, но теперь также использует другие типы файлов, такие как файлы установщика MSI, виртуальный жесткий диск, ISO для обхода Windows Mark of the Web и скомпилированный HTML.

Злоумышленник также использует платформы социальных сетей, такие как LinkedIn, для взаимодействия с жертвами, прежде чем размещать вредоносные ссылки в попытке улучшить коэффициент попаданий. TA444 продемонстрировал понимание английского, испанского, польского и японского языков.

Кража криптовалюты является основным мотивом злоумышленника, но исследователи безопасности также обнаружили «впечатляющий набор» бэкдоров после эксплуатации.

Исследователи называют TA444 «способным противником», поскольку в 2021 году он украл криптовалюту и цифровые активы на сумму почти 400 миллионов долларов и легко превзошел эту стоимость за одно ограбление, завершив 2022 год с более чем 1 миллиардом долларов». ***(Mihir Bagwe. North Korean Crypto Hackers Keep Nose to the Grindstone // Information Security Media Group, Corp. (https://www.govinfosecurity.com/north-korean-crypto-hackers-keep-nose-to-grindstone-a-21013). 25.01.2023).***

***

«Игривый Taurus, также известный как Vixen Panda, использует новый вариант турианского бэкдора

Исследователи кибербезопасности говорят, что китайская группа продвинутых постоянных угроз несет ответственность за нападения на иранские правительственные организации в период с июля по декабрь 2022 года.

Подразделение 42 Palo Alto Networks сообщает, что Playful Taurus был активен как минимум с 2010 года. Playful Taurus — это прозвище, данное группе ATP в процессе присвоения имен созвездиям. Группа также носит названия BackdoorDiplomacy, Vixen Panda, APT15, KeChang и Nickel.

Playful Taurus известен тем, что использует фишинговые методы для нападения на правительственные и дипломатические учреждения в Северной и Южной Америке, Африке и на Ближнем Востоке для кибершпионажа.

Группа недавно обновила свой инструментарий, включив в него новый вариант бэкдора Turian и свою инфраструктуру управления и контроля.

Отслеживая подключения к вредоносной инфраструктуре, исследователи заметили, что четыре иранские организации пытались подключиться к IP-адресу,

контролируемому хакерами, в 152.32.181.16период с июля по конец декабря 2022 года. Организация.

«Постоянный ежедневный характер этих подключений к инфраструктуре, контролируемой Playful Taurus, предполагает вероятную компрометацию этих сетей. Более того, эти цели также соответствуют историческим шаблонам таргетинга группы», — говорят исследователи.

Последняя версия Turian оснащена дополнительной обфускацией и модифицированным сетевым протоколом.

Одним из основных наблюдаемых отличий является алгоритм дешифрования C2. В более старых образцах «C2 расшифровывались с помощью XOR против жестко запрограммированного байта, такого как 0xA9», — говорят исследователи. «Обновленный бэкдор предлагает довольно общие функции, от обновления C2 для связи до выполнения команд и создания обратных оболочек. Основным отличием этого от других вариантов Turian являются идентификаторы команд. Предыдущие идентификаторы начинались с 0x01 и следовали порядку., новые идентификаторы кажутся рандомизированными."

Деятельность китайской группы осуществляется на фоне подписанного в 2021 году между двумя странами соглашения о сотрудничестве сроком на 25 лет, в котором содержится обещание о сотрудничестве в экономической, военной сфере и в сфере безопасности, поскольку обе страны сталкиваются с различными уровнями санкций США.

Срыв суда

Федеральный суд США в Вирджинии в декабре 2021 года проложил путь технологическому гиганту Microsoft для пресечения деятельности китайской хакерской группы, известной тогда как Nickel.

Окружной суд США Восточного округа штата Вирджиния удовлетворил просьбу Microsoft об аресте веб-сайтов, используемых хакерской группой для сбора разведданных от государственных органов, аналитических центров и правозащитных организаций в США и 28 других странах.

Приказ позволил подразделению компании по цифровым преступлениям перекрыть доступ Nickel к его жертвам и предотвратить использование веб-сайтов для проведения атак...

Microsoft, которая отслеживает Nickel с 2016 года и анализирует его деятельность с 2019 года, заявила, что атаки используют различные методы для достижения одной цели: внедрить трудно обнаруживаемое вредоносное ПО, которое облегчает вторжение, слежку и кражу данных.

Никель ранее нацеливался на организации как в частном, так и в государственном секторах, включая дипломатические организации и министерства иностранных дел в Северной Америке, Центральной Америке, Южной Америке, Карибском бассейне, Европе и Африке». ***(Prajeet Nair. Chinese APT Targets Iranian Government Organizations // Information Security Media Group, Corp. (https://www.govinfosecurity.com/chinese-apt-targets-iranian-government-organizations-a-20977). 19.01.2023).***

***

«Исследователи обнаружили, что вредоносное ПО Kinsing получило доступ к серверам Kubernetes, используя неправильно настроенные и незащищенные серверы PostgreSQL. Злоумышленники получили доступ, используя слабо настроенные контейнеры PostgreSQL и уязвимые образы контейнеров.

Исследователи из Microsoft Defender for Cloud заметили растущее число контейнеров PostgreSQL, зараженных вредоносной программой Kinsing. Он использует уникальные методы, нацеленные на контейнерные среды, сказал Сандерс Брускин, исследователь безопасности для Microsoft Defender for Cloud, в отчете, опубликованном на прошлой неделе.

Было замечено, что вредоносное ПО на основе Golang, Kinsing, нацелено на среды Linux.

«Тот факт, что это новый образ, на который направлено вредоносное ПО, означает, что к нему были добавлены некоторые новые способы заражения. Основная цель криптомайнеров — использовать ресурсы клиента. чтобы нацелить их и запустить вредоносное ПО», — сказал Брускин в интервью Information Security Media Group.

Неправильно настроенный PostgreSQL

В неправильных конфигурациях используется параметр «доверительная аутентификация», который, если он указан, разрешает доступ ко всем серверам, предполагая, что они являются авторизованными соединениями.

Брускин говорит, что предоставление доступа к широкому диапазону IP-адресов подвергает контейнер PostgreSQL потенциальной угрозе.

«Даже если метод незащищенной доверительной аутентификации не используется, а вместо него используются другие методы, он может открыть злоумышленникам несколько вариантов, таких как перебор учетных записей PostgreSQL, атака на доступность контейнера с помощью DoS- и DDoS-атак и попытка использовать контейнер и сама БД», — добавляет Брускин.

Использование образов контейнеров

Также было обнаружено, что зараженные образы уязвимы для удаленного выполнения кода, что в конечном итоге позволяет злоумышленникам, имеющим доступ к сети, использовать контейнер и запускать свою вредоносную полезную нагрузку.

Злоумышленники использовали несколько уязвимых версий приложений, таких как PHPUnit, Liferay, WebLogic и WordPress.

Брускин говорит, что они сосредоточились на эксплуатации Oracle WebLogic, поскольку наблюдали за «широкомасштабной кампанией Kinsing, нацеленной на уязвимые версии серверов WebLogic».

В 2020 году Oracle раскрыла серию уязвимостей высокой степени серьезности, позволяющих удаленно выполнять код, отслеживаемых как CVE-2020-14882, CVE-2020-14750 и CVE-2020-14883.

Уязвимость WebLogic можно использовать по сети без необходимости вводить имя пользователя и пароль. Согласно предыдущему обновлению Oracle, субъекту угрозы достаточно отправить вредоносный HTTP-запрос на консоль управления WebLogic Server, чтобы инициировать атаку.

«Атаки начинаются со сканирования широкого диапазона IP-адресов в поисках открытого порта, соответствующего порту WebLogic по умолчанию (7001). Если злоумышленники уязвимы, они могут использовать один из эксплойтов для запуска своей вредоносной полезной нагрузки», — говорит Брускин.

Oracle и Агентство США по кибербезопасности и безопасности инфраструктуры выпустили предупреждения о важности применения исправления, доступного с октября 2020 года.

«Мы рекомендуем свести к минимуму доступ контейнеров к Интернету. Помните о конфигурации и используйте пропатченные образы и известные репозитории», — говорит Брускин». ***(Prajeet Nair. Misconfigured PostgreSQL Used to Target Kubernetes Clusters // Information Security Media Group, Corp. (https://www.govinfosecurity.com/misconfigured-postgresql-used-to-target-kubernetes-clusters-a-20899). 10.01.2023).***

***

«…В понедельник, 9 января, регулятор BaFin (Федеральное управление финансового надзора Германии) опубликовал публичное предупреждение о вирусе Godfather. Ведомство утверждает, что количество случаев атак и кражи данных посредством этого ПО в стране постоянно растет.

Мы подробно рассказывали как о самом вирусе, так и о масштабах его распространения в отдельном материале. Первыми на него обратили внимание аналитики Group-IB.

Вирус маскируется под официальный сервис Google (в отдельных случаях под стороннее приложение) и ворует данные пользователя. Это формы заполнения, пароли, номера счетов и прочее.

По данным BaFin, под удар Godfather попало более 400 банковских приложений, клиентов крипто-платформ и цифровых кошельков. Пострадавшие есть в США, Германии, странах Еврозоны и даже Азии.

Как ни странно, пользователи из РФ, Беларуси, Казахстана и стран ТС находятся вне опасности. Если на устройстве установлен один из этих языков, вирус просто отключается. Это наталкивает на мысль о его происхождении.

В своем обращении BaFin также опубликовал ролик от Федерального управления цифровой безопасности (BSI). В нем приведены рекомендации для пользователей, которые помогут уберечь себя от этой угрозы.

Их можно свести к таким тезисам:

не устанавливать мобильное ПО из подозрительных источников;

тщательно следить за публикуемой информацией и разрешениями приложений;

регулярно проверять устройство на наличие вирусов и фишингового ПО.

Отметим, тот факт, что BaFin официально высказался касательно Godfather, говорит о серьезности угрозы. Помните, вирус атакует не только банковские приложения, но и клиенты крипто-платформ. Тщательно следите за тем, что установлено на вашем смартфоне, и какие данные отправляют эти приложения». ***(Иван Павловский. Немецкий регулятор предупредил о частых атаках вируса***

Godfather // incrypted (https://incrypted.com/regulyator-predupredil-o-atakah-virusa-godfather/?utm_source=rss&utm_medium=rss&utm_campaign=regulyator-predupredil-o-atakah-virusa-godfather). 10.01.2023).

***

«Исследователи кибербезопасности обнаружили новый загрузчик вредоносных программ для Linux, который нацелен на плохо защищенные серверы Linux с помощью майнеров криптовалюты и IRC-ботов DDoS.

Исследователи из ASEC обнаружили атаку после того, как компилятор сценариев оболочки (SHC), использованный для создания загрузчика, был загружен на VirusTotal. Судя по всему, SHC загружали корейские пользователи, и корейские пользователи также являются мишенями.

Дальнейший анализ показал, что злоумышленники преследуют плохо защищенные серверы Linux, взламывая учетные записи администраторов через SSH.

Как только они войдут, они либо установят майнер криптовалюты, либо IRC-бот DDoS. Используемый майнер — XMRig, возможно, самый популярный майнер криптовалюты среди хакеров. Он использует вычислительную мощность конечных точек жертвы (открывается в новой вкладке) для генерации Monero, криптовалюты, ориентированной на конфиденциальность, чьи транзакции, по-видимому, невозможно отследить, а пользователей предположительно невозможно идентифицировать.

Что касается бота DDoS IRC, злоумышленники могут использовать его для запуска таких команд, как TCP Flood, UDP Flood или HTTP Flood. Они могут запускать сканирование портов, сканирование Nmap, убивать различные процессы, очищать журналы и многое другое.

«В связи с этим администраторы должны использовать для своих учетных записей пароли, которые трудно угадать, и периодически менять их, чтобы защитить сервер Linux от атак методом грубой силы и атак по словарю, а также обновлять до последнего исправления для предотвращения атак с использованием уязвимостей», — говорится в сообщении ASEC. отчет.

«Администраторы также должны использовать программы безопасности, такие как брандмауэры, для серверов, доступных извне, чтобы ограничить доступ злоумышленников».

Системы Linux постоянно подвергаются вредоносным развертываниям, чаще всего программам-вымогателям и криптоджекингу.

В отчете VMware за февраль 2022 года говорится, что продолжающийся успех сервисов Linux в цифровой инфраструктуре и облачной индустрии, а также тот факт, что большинство решений для защиты от вредоносных программ и кибербезопасности ориентированы на защиту устройств на базе Windows, ставят Linux на тонкий лед». ***(Sead Fadilpašić. This new Linux malware floods machines with cryptominers and DDoS bots // Future US, Inc. (https://www.techradar.com/news/this-new-linux-malware-floods-machines-with-cryptominers-and-ddos-bots). 06.01.2023).***

***

«Исследователи кибербезопасности из HP Wolf Security предупредили о нескольких активных кампаниях, направленных на доставку различных типов вредоносных программ (откроется в новой вкладке) ничего не подозревающим жертвам с помощью опечатанных доменов и вредоносной рекламы.

Команда объяснила в сообщении в блоге (открывается в новой вкладке), как они обнаружили злоумышленников, создающих несколько опечатанных веб-сайтов, выдающих себя за популярные программы, такие как Audacity, Blender или GIMP.

Мошенники также платили различным рекламным сетям за размещение рекламы, продвигающей эти поддельные веб-сайты. Таким образом, когда люди ищут эти программы, поисковые системы могут в конечном итоге показывать вредоносные версии веб-сайтов рядом с законными. Если пользователь не будет осторожен и дважды не проверит URL-адрес посещаемого веб-сайта, он может оказаться не в том месте.

Поддельные установщики

Если жертвы и окажутся не в том месте, они вряд ли заметят разницу. Веб-сайты спроектированы таким образом, чтобы они выглядели почти так же, как и настоящие, вплоть до мельчайших деталей. В примере Audacity на сайте размещен вредоносный файл.exe, маскирующийся под установщик программы. Он называется «audacity-win-x64.exe» и имеет размер более 300 МБ.

Благодаря такому большому размеру злоумышленники стараются не вызывать подозрений (вредоносное ПО обычно измеряется в КБ), а также стараются избегать антивирусных программ. По словам исследователей, функции автоматического сканирования некоторых антивирусных программ не сканируют очень большие файлы.

Исследователи заявили, что файлы размещены в облачном хранилище 4sync.com, добавив, что все поддельные установщики в этой кампании были размещены там, намекая на то, что хорошим защитным механизмом может быть полная блокировка доступа к этому сервису.

В кампании распространяются разные типы вредоносных программ. Крупнейшие кампании, которые наблюдали исследователи, использовали этот подход к доставке для развертывания трояна IcedID, но наблюдались и Infostealer Vidar, BatLoader и Rhadamanthys Stealer. По данным HP Wolf Security, с ноября прошлого года наблюдается всплеск этих кампаний. ***(Sead Fadilpašić. This dangerous malvertising campaign mimicks popular software to steal victim info // Future US, Inc. (https://www.techradar.com/news/this-dangerous-malvertising-campaign-mimicks-popular-software-to-steal-victim-info).*** **18.01.2023).**

***

«Хотя некоторые отрасли ценятся больше, чем другие, прибыль важнее всех соображений

По мере того, как программы-вымогатели продолжают атаковать множество секторов, как любая конкретная организация становится мишенью или жертвой?

Организации в некоторых географических регионах с большей вероятностью станут жертвами. Фирма по кибербезопасности Group-IB сообщает, что с июля 2021 года по июнь 2022 года 43% известных атак программ-вымогателей поразили американские организации. Следующими на очереди были Германия, Великобритания, Канада, Италия и Франция.

Некоторые сектора также становятся жертвами больше, чем другие. В прошлом квартале компания Coveware, занимающаяся реагированием на инциденты с программами-вымогателями, сообщила, что большинство жертв приходится на государственный сектор, за которым следуют службы программного обеспечения, здравоохранение, профессиональные услуги и сектор материалов.

Сравнивая последние три месяца 2022 года с третьим кварталом, Coveware заметила, что пострадало меньше фирм, предоставляющих профессиональные услуги, включая небольшие юридические фирмы и фирмы, предоставляющие финансовые услуги, что, по ее мнению, связано с тем, что группы вымогателей отдают предпочтение более крупным и прибыльным целям...

В некоторых отраслях зафиксирован рост атак. В частности, во второй половине прошлого года количество известных атак на производственный сектор увеличилось на 30%, сообщает фирма по кибербезопасности Dragos. Этот сектор включает все, от автомобильных фирм и поставщиков промышленного оборудования до электроники и аэрокосмической отрасли.

Ответьте на этот вопрос о курице и яйце: набирают ли группы вымогателей жертв, сосредотачиваясь на предпочтительных секторах, или определенные сектора просто с большей вероятностью в конечном итоге станут жертвами?

Прибыль Императив

Главной заботой групп вымогателей, по-видимому, остается простая: прибыль.

На своем сайте утечки данных группа LockBit сообщает аффилированным лицам, что ее «интересуют только деньги», что подкрепляется католическим вкусом группы к жертвам, который охватывает все отрасли, включая больницы и критически важную инфраструктуру.

Сообщение для партнеров, которые обычно получают 70% каждого выкупа, ясно: взламывайте кого хотите, пока это максимизирует доход…

Следовательно, жертвы, по-видимому, сначала накапливаются полуслучайным образом — на основе доступа, который группа покупает у брокера первоначального доступа, организаций, которые могли быть напрямую взломаны филиалом группы вымогателей, или систем, захваченных вредоносным ПО, используемым группой. В этот момент, возможно, группы решают, на ком сосредоточиться в первую очередь.

«Киберпреступники всегда анализируют доходы своих жертв — брокеры начального доступа в своих предложениях указывают финансовые показатели своих жертв», — говорит Владимир Тимофеев, руководитель подпольной исследовательской и мониторинговой группы Group-IB. «Логика этого проста: если у потенциальной жертвы мало денег, то вряд ли она заплатит выкуп. ОВД также начали включать краткое описание компании-жертвы с указанием ее местонахождения и отрасли».

Group-IB сообщает, что из 2348 первоначальных предложений доступа, которые она рекламировала на подпольных форумах с июля 2021 года по июнь 2022 года, наибольшая часть — что составляет 6% всех предложений IAB — касалась компаний производственного сектора.

«Сетевой доступ к компаниям производственного сектора — один из самых востребованных активов для групп вымогателей», — говорит Тимофеев. Учитывая этот спрос, IAB могут взимать более высокую плату за такой «доступ», а это означает, что более крупные группы могут быть теми, кто с большей вероятностью будет рисковать более высокими первоначальными затратами ради потенциальной большой отдачи от своих инвестиций.

«Промышленные и производственные компании всегда готовы платить больше, поскольку простои сильно влияют на производство и приводят к многомиллионным финансовым потерям», — говорит он. «В то время как другие компании могут опасаться публичного обнародования своих данных, компании-производители всегда будут страдать непосредственно от атак программ-вымогателей».

Согласно исследованиям Kela и Group-IB, за последние 18 месяцев, вероятно, неслучайно производство было отраслью, которая чаще всего подвергалась атакам операторов программ-вымогателей.

Таким образом, хотя точная механика того, как группа вымогателей в конечном итоге выбирает потенциальных жертв, кажется переменной, если группа считает, что из любой организации, к которой они получили удаленный доступ, можно выжать приличную прибыль, это, похоже, возможность, которую они могут использовать». ***(Mathew J. Schwartz. Targets of Opportunity: How Ransomware Groups Find Victims // Information Security Media Group, Corp. (https://www.govinfosecurity.com/blogs/targets-opportunity-how-ransomware-groups-find-victims-p-3365). 27.01.2023).***

***

«…Глобальная рабочая группа по борьбе с программами-вымогателями, возглавляемая Австралией и состоящая из 37 правительств-единомышленников, начала работу в понедельник с целью обмена разведывательными данными для предотвращения будущих атак цифрового вымогательства.

Целевая группа является продуктом Инициативы по борьбе с программами-вымогателями, возглавляемой США, которая в последний раз встречалась в ноябре в Белом доме (см. Конференция Белого дома по программам-вымогателям заканчивается обещанием об обмене данными).

Целевая группа нацелена на укрепление сотрудничества между глобальными правоохранительными органами и органами кибербезопасности. Помимо обмена разведывательными данными, он будет делиться передовой практикой, политикой и правовыми рамками.

Глобальная инициатива проводится Министерством внутренних дел Австралии и его недавно созданным Координационным центром кибербезопасности и критических технологий. Во второй половине 2022 года Австралия подверглась очевидной нарастающей волне кибератак, включая утечку данных с помощью программы-вымогателя у оператора связи Optus и у крупнейшей частной страховой компании страны...

«Недавние киберинциденты в Австралии и во всем мире являются ярким напоминанием о коварной природе программ-вымогателей и способности киберпреступников причинять массовые разрушения и вред широким слоям общества», — заявила министр внутренних дел Австралии Клэр О’Нил..

В результате серии атак О'Нил поклялась, что к 2030 году ее страна станет «самой кибербезопасной страной в мире». В недавнем интервью Bloomberg она сказала, что получила официальный обзор атак на Medibank и Optus и опубликует результаты «относительно скоро». ***(Mihir Bagwe. Australia Initiates Global Ransomware Task Force Operations // Information Security Media Group, Corp. (https://www.govinfosecurity.com/australia-initiates-global-ransomware-task-force-operations-a-20997). 23.01.2023).***

***

«…Общая сумма выкупа, отправляемого жертвами группам вымогателей, в прошлом году, похоже, сильно упала.

Аналитическая компания Chainalysis сообщает, что, основываясь на доступных в настоящее время данных, «общий доход от программ-вымогателей в 2022 году упал как минимум до 456,8 млн долларов в 2022 году с 765,6 млн долларов в 2021 году — огромное падение на 40,3%».

Он добавляет, что «данные свидетельствуют о том, что это связано с растущим нежеланием жертв платить злоумышленникам-вымогателям», а не с уменьшением числа атак программ-вымогателей.

Действительно, согласно многочисленным источникам, количество атак программ-вымогателей за последние годы не уменьшилось или, по крайней мере, ненамного.

Одно предостережение относительно выводов Chainalysis заключается в том, что они основаны на отслеживании потоков криптовалюты на кошельки, которые, как известно, управляются или принадлежат преступникам. Фирма регулярно обновляет свои прошлые оценки объемов потоков криптовалюты по мере появления новой информации, например, когда полиция арестовывает группу киберпреступников или рынок даркнета и делится адресами криптовалютных кошельков и другой информацией.

Например, в начале прошлого года фирма сообщила, что в 2021 году выплата программ-вымогателей составила 602 миллиона долларов, а на данный момент она пересмотрела ее до 766 миллионов долларов.

Но выводы Chainalysis совпадают с выводами охранной фирмы Coveware. В октябре компания по реагированию на инциденты с программами-вымогателями сообщила, что меньше жертв программ-вымогателей платили выкуп.

Как часто жертва программы-вымогателя платила?

	2109	2020	2021	2022
Оплаченный	76%	70%	50%	41%
не заплатил	24%	30%	50%	59%

Источник: Coveware, основано на тысячах случаев, когда это сработало.

Coveware заявила, что это отчасти связано с «снижением качества и надежности» инструментов дешифрования, предоставляемых злоумышленниками, что привело к тому, что больше жертв отказались платить.

Изменения программ-вымогателей

Анализируя ситуацию с программами-вымогателями в 2022 году, Chainalysis также обнаружила:

Больше штаммов: число активных штаммов программ-вымогателей, как сообщается, резко возросло в прошлом году. Только в первой половине прошлого года в Fortinet было обнаружено более 10 000 штаммов, но львиная доля доходов от выкупа по-прежнему достается относительно небольшому числу групп.

Более короткая продолжительность жизни: хотя в 2021 году средняя продолжительность жизни штамма программ-вымогателей составляла 153 дня, в прошлом году она сократилась до 70 дней, возможно, потому что злоумышленники пытались лучше «запутать свою деятельность», создавая новые типы вредоносных программ.

Изменения в отмывании денег: программы-вымогатели все чаще использовали «основные централизованные биржи» для отмывания денег вместо бирж с высоким уровнем риска или даркнетов для отмывания денег, хотя использование миксеров немного увеличилось.

Небольшой кадровый резерв: «Хотя многие штаммы активны в течение года, фактическое количество людей, составляющих экосистему программ-вымогателей, вероятно, довольно мало».

Преданность в сфере киберпреступности кажется дешевой, по крайней мере, для аффилированных лиц или деловых партнеров групп вымогателей, которые фактически арендуют код атаки у операторов. Специалисты по безопасности давно отследили, как аффилиаты работают с разными группами, иногда одновременно. Некоторые филиалы, по-видимому, используют разные штаммы в зависимости от выбора цели. Хотя аффилированные лица обычно получают до 70% от каждого выплаченного выкупа, некоторые из них могут договариваться с операторами о различных соглашениях о распределении прибыли.

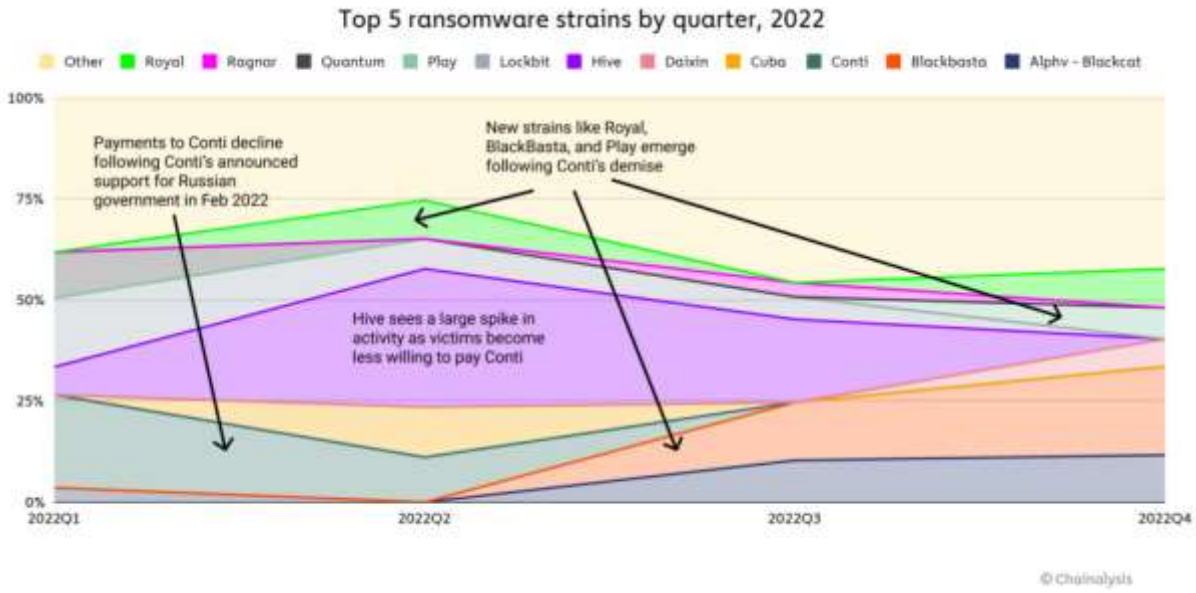
В прошлом году все больше аффилиатов отказались от работы с громкими именами, опасаясь, что они пририсовывают себе слишком много мишени. Кроме того, из Conti, Hello Kitty и LockBit просочился исходный код, а это означает, что у потенциальных злоумышленников есть несколько вариантов развертывания

собственных программ-вымогателей, и им не нужно делить доходы с помощью операции «программа-вымогатель как услуга», которая обычно сохраняет 30% от каждого выплаченного выкупа (см.: Экосистема программ-вымогателей: известные бренды становятся ответственностью).

В октябре прошлого года Microsoft сообщила, что группа Vice Society использовала два разных предложения программ-вымогателей как услуги — Quantum Locker и BlackCat, также известных как Alphv, — а также готовые программы-вымогатели Zeppelin и Hello Kitty, источник которых код общедоступен бесплатно.

Несмотря на такие сдвиги, Chainalysis сообщает, что большая часть доходов от программ-вымогателей по-прежнему направляется на операции «программы-вымогатели как услуга».

Конти «уходит в отставку», но игроки продолжают



Источник: Цепной анализ

Одним из важных изменений в прошлом году стал уход знаменитой компании Conti в мае из-за ее катастрофической публичной поддержки войны России на Украине, за которой последовало меньшее количество жертв, решивших заплатить.

Chainalysis говорит, что точным виновником, вероятно, была утечка сообщений Conti в феврале прошлого года, которая выявила очевидные связи между ее главой «Штерном» и Федеральной службой безопасности России, или ФСБ. В то время как Conti никогда не подвергалась санкциям Министерства финансов США, ФСБ подверглась санкциям, и ее очевидных связей с Conti могло быть достаточно, чтобы отпугнуть потенциальных плательщиков выкупа.

Chainalysis сообщает, что многие филиалы Conti начали работать с новыми группами после того, как жертвы перестали платить.

В июне прошлого года Microsoft подробно описала две разные партнерские группы, работающие с BlackCat, также известной как Alphv, — операцией по вымогательству: DEV-0237, которая ранее использовала Ryuk, Conti и Hive; и DEV-

0504, в котором использовались Ryuk, REvil — он же Sodinokibi — предшественник BlackCat BlackMatter, и Conti.

По словам Chainalysis, лидер Conti Стерн также оставался активным, проводя транзакции «с адресами, связанными с такими штаммами, как Quantum, Karakurt, Diavol и Royal в 2022 году после кончины Conti». По крайней мере, некоторые из них, похоже, являются брендами, выделенными Conti до выхода на пенсию.

Таким образом, в то время как группы вымогателей появились и исчезли в прошлом году, многие из вовлеченных лиц, похоже, держатся и наживаются». ***(Mathew J. Schwartz. Victims' Known Ransom Payments to Ransomware Groups Decline // Information Security Media Group, Corp. (https://www.govinfosecurity.com/blogs/victims-known-ransom-payments-to-ransomware-groups-decline-p-3357). 19.01.2023).***

***

«…Программа-вымогатель по-прежнему остается самой серьезной угрозой кибербезопасности в Соединенном Королевстве, и в 2023 году страну может ожидать всплеск разрушительных атак, предупреждает бывший глава национального агентства по кибербезопасности Великобритании.

Киаран Мартин, директор Sans Institute и профессор практики Оксфордского университета, говорит, что в 2022 году общая активность программ-вымогателей по всему миру резко упала, но в ближайшие месяцы атаки, вероятно, увеличатся. Он добавляет, что недавние взломы газеты The Guardian и британская Королевская почта являются примерами этих атак на ранней стадии.

Мартин, который до 2020 года был генеральным директором Национального центра кибербезопасности Великобритании, говорит, что одним из факторов, способствующих успеху программ-вымогателей, по-прежнему является то, что большинство преступных группировок действуют за пределами России, которая, по его словам, является «убежищем» для мошенников. «действовать безнаказанно».

«Киберпреступники процветают в более слабых государствах. Они не процветают во Франции, Соединенных Штатах или Канаде», — сказал Мартин в интервью Information Security Media Group во время конференции CyberThreat 2022 в Великобритании на этой неделе. «Итак, в обозримом будущем я думаю, что этот регион, вероятно, станет источником значительного киберпространства».

Снижение числа атак программ-вымогателей в 2022 году на 23%, основанное на отчете SonicWall, вероятно, связано с нарушениями, вызванными продолжающейся войной на Украине и в России, и большинство операторов программ-вымогателей в регионе вынуждены бежать или присоединяться в качестве призывников в Служба государственной безопасности, говорит он.

«В 2023 году первые признаки, к сожалению, заключаются в том, что его стало немного больше», — говорит он. «Поэтому, я думаю, мы можем ожидать еще несколько громких дел, особенно против организаций на Западе».

Этот анализ также поддерживает Агентство Европейского союза по кибербезопасности, которое в своем отчете об угрозах за ноябрь 2022 года предупредило об увеличении числа целевых атак на критически важную инфраструктуру в странах Запада и НАТО, особенно со стороны пророссийских и

поддерживаемых государством хакеров, использующих программы-вымогатели в ответ. за поддержку Украины.

В отчете за декабрь 2022 года охранная фирма Palo Alto Networks сообщила, что хакерская группа, предположительно связанная с Россией, нацелилась на крупную нефтеперерабатывающую компанию, базирующуюся в стране НАТО, на ранних этапах войны в Украине.

Мартин добавляет, что распространенность слабых корпоративных сетей в западных странах и успех нынешних моделей программ-вымогателей, поскольку большинство жертв предпочитают платить выкуп, являются двумя факторами, способствующими росту программ-вымогателей.

«Представление о том, что проще заплатить выкуп, — это прокриминальный нарратив», — говорит он. «Дело в том, что у жертв больше свободы воли, чем они думают, и чего они не осознают, так это того, что стоимость восстановления в большинстве случаев дешевле, чем выплата выкупа», — говорит Мартин. Он указывает на Школьную федерацию Харриса в Лондоне, которая восстановила свои файлы за 600 000 долларов, в отличие от первоначального требования хакеров-вымогателей в 4 миллиона долларов.

Мартин также говорит, что реализация политики на национальном уровне, направленная на то, чтобы отговорить потенциальных жертв программ-вымогателей от уплаты выкупа, остается проблемой, которая по-прежнему ускользает от политиков.

«Двадцать лет назад британское правительство приняло очень трудное решение запретить выплату выкупа террористам, которые похищают людей. Это привело к некоторым действительно трудным решениям, но в конечном итоге это сработало, поскольку было похищено меньше британских граждан», — говорит Мартин. «Что меня поражает, так это то, что, несмотря на серьезные проблемы с введением запрета на выкуп, мы на самом деле не проделали работу, чтобы увидеть, сможем ли мы преодолеть этот запрет»…» ***(Akshaya Asokan. Ransomware Remains Top Cyberthreat, Former NCSC Chief Says // Information Security Media Group, Corp. (https://www.govinfosecurity.com/ransomware-remains-top-cyberthreat-former-ncsc-chief-says-a-20966). 18.01.2023).***

***

«…Как сообщает британская газета The Telegraph, группа LockBit, занимающаяся программами-вымогателями, несет ответственность за кибер-инцидент, который продолжает препятствовать доставке международной почты из Соединенного Королевства.

Британская национальная почтовая служба Royal Mail впервые сообщила клиентам в среду о цифровом инциденте, нарушившем международные экспортные услуги, и этот сбой продолжался до четверга. «Пожалуйста, не отправляйте экспортные товары, пока мы работаем над решением проблемы», — написал почтовый перевозчик в Твиттере.

Источники, идентифицированные как «знакомые с ходом расследования», сообщили The Telegraph, что причиной инцидента является программа-вымогатель

LockBit. Газета сообщила, что он заразил машины, используемые для печати таможенных этикеток для посылок, отправляемых за границу.

The Belfast Telegraph сообщила, что во вторник на объекте Королевской почты в Северной Ирландии печатные машины печатали записки с требованием выкупа.

Королевская почта не сразу ответила на запрос о комментарии. Почтовый перевозчик предупредил Национальный центр кибербезопасности Великобритании и Национальное агентство по борьбе с преступностью. Ни одно из агентств не предоставило дополнительных подробностей о взломе.

LockBit — это активная группа по вымогательству, действующая с конца 2019 года. Группа до сих пор не публиковала данные Королевской почты на своем официальном сайте утечки. Группу часто считают победителем конкурса на смену Conti как самой известной в мире банды цифрового вымогательства (см. Ключи к успеху LockBit: самореклама, техническая сообразительность).

Его недавние жертвы включают порт Лиссабона, французскую оборонную транснациональную компанию Thales и немецкого производителя автозапчастей Continental.

Программа-вымогатель, вероятно, останется главной угрозой кибербезопасности в 2023 году, спустя годы после того, как в 2019 году высокопоставленные чиновники по кибербезопасности Соединенного Королевства назвали ее «ключевой угрозой». За последние несколько лет значительно возросли не только частота, но и требования о вымогательстве, и одна фирма, занимающаяся кибербезопасностью, в 2022 году оценила средний спрос на выкуп почти в 1 миллион долларов.

Большинство группировок, предлагающих программы-вымогатели как услугу, действуют внутри России, но большинство из них открыто аполитичны, чтобы не усложнять выплаты по вымогательству, заставляя фирмы беспокоиться о том, что они нарушают финансовые санкции США.

Официальный представитель США сообщил журналистам в прошлом году во время встречи возглавляемой США международной организации по борьбе с программами-вымогателями, что в борьбе с бандами программ-вымогателей были достигнуты успехи. Тем не менее, «мы видим, что темпы и изощренность атак программ-вымогателей растут быстрее, чем наши усилия по обеспечению устойчивости и разрушению», — признал чиновник (см. Конференция по программам-вымогателям в Белом доме завершается обещанием об обмене данными)». ***(Akshaya Asokan. LockBit Ransomware Group Reportedly Behind Royal Mail Attack // Information Security Media Group, Corp. (https://www.govinfosecurity.com/lockbit-ransomware-group-reportedly-behind-royal-mail-attack-a-20919). 12.01.2023).***

***

«Британская газета The Guardian попросила большую часть своих сотрудников продолжать работать из дома до 23 января, поскольку организация продолжает восстанавливаться после декабрьской атаки программ-вымогателей на ее сети.

В электронном письме, отправленном в понедельник, почти через две недели после атаки, генеральный директор Guardian Media Group Анна Бейтсон попросила сотрудников продолжать работать из дома, чтобы снизить нагрузку на сети организации, поскольку она продолжает восстанавливать пострадавшие системы.

Указ распространяется на сотрудников лондонской штаб-квартиры The Guardian, а также сотрудников в Австралии и Нью-Йорке. По оценкам, тираж Guardian Media Group составляет 105 000 экземпляров, и это седьмой по популярности новостной сайт в мире.

21 декабря организация подверглась атаке программ-вымогателей, в ходе которой хакеры взломали ИТ-инфраструктуру газеты. Хотя инцидент не повлиял на производство газет или другие операции, организация попросила сотрудников работать из дома в качестве меры предосторожности.

«Мы попросили большинство сотрудников работать из дома в течение следующих трех недель, чтобы позволить нашим техническим командам сосредоточиться на важной технической работе», — заявил представитель The Guardian Media Group в среду. «Работа по полному восстановлению наших систем продолжается и займет несколько недель».

Хотя подробности об участниках угрозы и причастных к выкупу остаются неясными, британский эксперт по кибербезопасности Кевин Бомонт сообщил в сообщении Mastodon, что атака The Guardian, по-видимому, затронула локальную инфраструктуру публикации.

«Хотя облачная инфраструктура The Guardian остается в сети, — сказал он, — похоже, что локальная инфраструктура Windows устарела. Внешние сетевые каналы работают, BGP работает нормально, но внутреннюю сеть полностью отключили». ***(Akshaya Asokan. Guardian Newspaper Offices Still Empty After December Attack // Information Security Media Group, Corp. (https://www.govinfosecurity.com/guardian-newspaper-offices-still-empty-after-december-attack-a-20851). 04.01.2023).***

***

«Rackspace сообщает, что злоумышленники, вооруженные программами-вымогателями, которые в прошлом месяце нарушили работу его размещенной среды Microsoft Exchange Server, использовали эксплойт нулевого дня для получения удаленного доступа к серверам, сообщают несколько новостных агентств.

Фирма CrowdStrike, занимающаяся кибербезопасностью, описала основную уязвимость как «ранее нераскрытый метод эксплойта для Exchange». В сообщении в блоге от 20 декабря 2022 г. говорится, что, хотя Microsoft выпустила исправление для Exchange в ноябре прошлого года для решения проблемы ProxyNotShell, она не уточняла или не знала, что, если организации не установят исправление, а не будут использовать рекомендуемые меры по смягчению последствий, это новое Метод эксплойта можно использовать для получения прямого удаленного доступа к серверам Exchange через веб-клиент Outlook.

Microsoft не сразу ответила на запрос о комментариях.

Rackspace, базирующаяся в Сан-Антонио, штат Техас, сообщает, что ФБР и CrowdStrike приписали атаку, о которой оно впервые сообщило 6 декабря 2022 года, группе вымогателей Play, сообщили San Antonio Express-News и другие СМИ.

Атака затронула тысячи клиентов Rackspace по всему миру. Начиная с 1 декабря 2022 года они не могли получить доступ к электронной почте, размещенной на Microsoft Exchange.

В рамках своего ответа Rackspace прекратила предлагать размещенные службы Exchange и помогает клиентам перейти на Microsoft 365, хотя предлагала и другие подходы. Эти усилия по миграции, а также получение до декабря. 2 электронная почта восстановлена для некоторых клиентов, остается в силе.

Rackspace — крупнейший в мире поставщик управляемых облачных услуг, насчитывающий более 300 000 клиентов по всему миру, в том числе две трети из 100 крупнейших публичных компаний мира. Фирма заявляет, что ее хостинговый бизнес Exchange составляет около 1% ее общего годового дохода и в основном скомпрометирован малыми и средними организациями.

Атака Play, по-видимому, оставила серверы Exchange, размещенные Rackspace, либо зашифрованными, либо иным образом нарушенными из-за реакции компании на атаку. Компания не сразу ответила на запрос о дополнительной информации.

Rackspace не сразу применила исправление Exchange, выпущенное Microsoft в ноябре прошлого года, из-за многочисленных сообщений пользователей о том, что исправление вызывало ошибки, в том числе оставляя Microsoft Outlook Web Access — OWA — недоступным, сообщает San Antonio Express-News со ссылкой на неназванного внешнего консультанта. в компанию. Сообщается, что в ожидании полностью рабочего патча Rackspace использовала меры, рекомендованные Microsoft.

«Упреждающее отключение»

Rackspace ранее сообщала, что 1 декабря 2022 г. она «произвела серьезный сбой в нашей среде Hosted Exchange» и в ответ «заблаговременно закрыла среду, чтобы избежать дальнейших проблем, пока мы продолжаем работу по восстановлению службы» и определила «первопричина проблемы». Компания также привлекла компанию CrowdStrike, занимающуюся реагированием на инциденты кибербезопасности в Остине, штат Техас, для оказания помощи и расследования.

«Благодаря быстрым действиям со стороны компании по отключению своей сети и выполнению планов реагирования на инциденты CrowdStrike подтвердила, что инцидент был быстро локализован и ограничен исключительно бизнесом электронной почты Hosted Exchange», — сообщил Rackspace в форме от 9 декабря 2022 г. 8-K подачи в Комиссию по ценным бумагам и биржам США.

Rackspace принесла извинения клиентам за сбои. Он также предупредил инвесторов, что атака может повлиять на доходы его размещенной биржи, которая составляет около 30 миллионов долларов в год, а также привести к непредвиденным расходам. Но фирма говорит в своем заявлении: «Rackspace поддерживает страхование кибербезопасности, соизмеримое с размером ее бизнеса, и уверена в своей способности покрыть потенциальные финансовые затраты,

связанные с инцидентом, и выполнить свои обязательства перед другими клиентами».

Акции Rackspace закрылись на уровне 2,91 доллара за акцию во вторник, что на 41% ниже по сравнению с 4,94 доллара на 1 декабря 2022 года, за день до того, как начали проявляться перебои в обслуживании, связанные с атакой.

Всего через несколько дней после того, как Rackspace сообщила, что стала жертвой предполагаемой атаки программы-вымогателя, на нее был подан коллективный иск, в котором ее обвинили в халатности.

Рекомендуется: миграция Microsoft 365…

Rackspace заявляет, что продолжает восстанавливать электронные письма клиентов, но этот процесс еще не завершен. Компания подробно описала пятиэтапный процесс: восстановление старых систем в изолированной среде, восстановление данных с поврежденных серверов, подготовка новой среды для обработки извлечения данных, извлечение данных и, наконец, восстановление данных электронной почты.

Rackspace по-прежнему рекомендует всем затронутым клиентам перейти на Microsoft 365 и заявляет, что предоставляет им «лицензии Microsoft Exchange Plan 1 на Microsoft 365» без дополнительной платы, по крайней мере, на данный момент.

Rackspace предлагает две альтернативы: перенести почтовые ящики клиентов Hosted Exchange в Rackspace Email или «использовать внутреннюю ретрансляцию для поддержания маршрутизации почты для вашей гибридной установки».

«Крайне важно, что страница состояния показывает, что они действительно полностью откажутся от службы Hosted Exchange — клиентам будет предоставлен экспорт почтовых ящиков в PST в какой-то момент в будущем, и это завершение продукта», — говорит британский эксперт по кибербезопасности Кевин Бомонт в своем посте. к мастодонту. Файл.pst— это экспорт файла данных Outlook.

CrowdStrike подробно описывает эксплойт нулевого дня

Патчи Exchange, выпущенные Microsoft в ноябре прошлого года, включали исправления для пары уязвимостей нулевого дня, которые использовались для атак в дикой природе, впервые обнаруженных в сентябре 2022 года.

Пара недостатков вместе известна как ProxyNotShell из-за их сходства с тремя недостатками Exchange, обнаруженными в 2021 году, известными как ProxyShell.

Первая уязвимость ProxyNotShell — CVE-2022-41040 — представляет собой уязвимость подделки запросов на стороне сервера, которую злоумышленники могут использовать для доступа к внутренним серверам. Вторая уязвимость — CVE-2022-41082 — допускает удаленное выполнение кода при активации Remote PowerShell. Используя первую уязвимость, злоумышленники могут активировать вторую.

CrowdStrike сообщила в своем блоге 20 декабря, что после расследования «нескольких вторжений программ-вымогателей Play, где было подтверждено, что общим вектором проникновения является Microsoft Exchange», подозрение заключалось в том, что злоумышленники использовали две уязвимости ProxyNotShell вместе. Но там написано, что это не так.

Вместо этого с помощью метода эксплойта, который он назвал OWASSRF, злоумышленники смогли соединить уязвимость повышения привилегий Microsoft Exchange Server — CVE-2022-41080 — со второй частью цепочки атак ProxyNotShell, CVE-2022-41082, «для достижения удаленное выполнение кода (RCE) через Outlook Web Access (OWA)».

CrowdStrike добавляет: «После первоначального доступа с помощью этого нового метода эксплойта субъект угрозы использовал легитимные исполняемые файлы Plink и AnyDesk для поддержания доступа и применил методы защиты от криминалистики на сервере Microsoft Exchange, пытаясь скрыть свою активность».

Хотя в сообщении в блоге CrowdStrike Rackspace не упоминается как одна из организаций, атакованных таким образом, директор по безопасности хостингового гиганта Карен О'Рейли-Смит подтвердила, что была использована уязвимость CVE-2022-41080.

«Microsoft раскрыла CVE-2022-41080 как уязвимость повышения привилегий и не включила примечания о том, что она является частью цепочки удаленного выполнения кода, которую можно было использовать», — сказал О'Рейли-Смит Cybersecurity Dive.

Совет по смягчению последствий

CrowdStrike рекомендует всем организациям, использующим Microsoft Exchange, применить исправление Exchange от ноября 2022 г., обозначенное Microsoft как KB5019758, «для предотвращения эксплуатации, поскольку средства защиты от перезаписи URL-адресов для ProxyNotShell неэффективны против этого метода эксплуатации».

«Если вы не можете немедленно применить исправление KB5019758, вам следует отключить OWA до тех пор, пока не будет применено исправление», — говорится в нем. Любой, кто использует серверы Exchange, также должен «следовать рекомендациям Microsoft по отключению удаленного PowerShell для пользователей без прав администратора, где это возможно», — добавляет он.

CrowdStrike выпустил через GitHub сценарий для журналов сервера Microsoft Exchange, который организации могут использовать для отслеживания признаков использования метода эксплойта OWASSRF». ***(Mathew J. Schwartz. Rackspace Blames Zero-Day Exploit for Ransomware Hit Success // Information Security Media Group, Corp. (https://www.govinfosecurity.com/rackspace-blames-zero-day-exploit-for-ransomware-hit-success-a-20849). 04.01.2023).***

***

«Группа BlackCat, занимающаяся программами-вымогателями как услугой, пробует новую тактику давления на жертв, чтобы они платили за вымогательство: создание поддельного веб-сайта в общедоступном Интернете, раскрывающего личные данные, украденные у жертвы.

Группа, также известная как Alphv, якобы украла 3,5 ГБ данных у небольшой бухгалтерской фирмы в США. Все эти данные, по-видимому, доступны на поддельном веб-сайте, который разрешается в доменное имя с одной крошечной орфографической ошибкой, отличающейся от законного имени бухгалтерской фирмы.

«Мы создали клиринговый сайт с украденными данными, надеемся, вам понравится!» BlackCat написал на своем сайте утечки. Украденные данные также находятся на файлообменнике, ссылка на который есть на сайте утечки.

Данные, просмотренные Information Security Media Group, по-видимому, принадлежат сотрудникам и клиентам бухгалтерской фирмы и содержат пароли в открытом виде, сведения о сотрудниках, аудиторские отчеты, сведения о налоговых декларациях ее клиентов, водительские права и неотредактированные сканы паспортов.

По состоянию на ранний вечер вторника поддельный веб-сайт все еще находится в сети. Данные WHOIS показывают, что неназванная сторона — регистрация является частной — зарегистрировала домен с опечаткой 22 декабря.

Развивающийся тренд

BlackCat использовал аналогичный метод против роскошного спа-курорта в Орегоне во время июньской атаки. Группа создала опечатанный веб-сайт c.xyz доменом в открытом Интернете для отображения сведений о сотрудниках и гостях спа-салона и курорта. В то время веб-сайт, подвергшийся опечатке, содержал личные данные 1534 сотрудников и в общей сложности расходы 2789 названных гостей (см. Техника вымогательства BlackCat: публичный доступ к взломанным данным).

По словам Бретта Кэллоу, аналитика угроз в компании Emsisoft, злоумышленники постоянно изобретают новые стратегии.

«Мы видели, как они перешли от атак только с шифрованием к шифрованию и эксфильтрации, и теперь мы видим, как они ищут новые способы использования эксфильтрованных данных», — сказал Кэллоу ISMG». ***(Mihir Bagwe. BlackCat Spoofs Victim Website to Leak Stolen Data // Information Security Media Group, Corp. (https://www.govinfosecurity.com/blackcat-spoofs-victim-website-to-leak-stolen-data-a-20847). 03.01.2023).***

***

«Многие злоумышленники, владеющие программами-вымогателями, умеют наживаться на принуждении своих жертв наводить порядок.

Поэтому жертвы часто сталкиваются с множеством вариантов: заплатите выкуп за дешифратор, и вы сможете разблокировать принудительно зашифрованные данные. Заплатите больше, и ваше имя будет удалено из списка жертв на сайте утечки данных группы вымогателей. Заплатите еще больше, и вы получите обещание, что любые данные, которые они украли или уже просочились, будут немедленно удалены.

Конечно, многие жертвы почувствуют импульс сделать что-нибудь, что угодно, из-за иллюзии, что они могут запоздало защитить украденные данные и спасти свою репутацию. Этот порыв понятен. Но это не только слишком поздно, но и используется против них вымогателями. Говоря психологическим языком, преступники без колебаний находят рычаги, которые заставят жертву действовать — например, дать ей деньги.

Обещания большинства групп вымогателей — чепуха, и больше всего они гарантируют то, что жертва не может проверить.

К сожалению, видеть, как жертвы платят за обещания удалить данные, не новость. Возьмите BlackBaud, публичную фирму из Южной Каролины, которая предоставляет облачное программное обеспечение для маркетинга, сбора средств и управления взаимоотношениями с клиентами, используемое тысячами благотворительных организаций, университетов, организаций здравоохранения и других организаций. После атаки программы-вымогателя в мае 2020 года, которая включала кражу данных, три месяца спустя бизнес сообщил: «Поскольку защита данных наших клиентов является нашим главным приоритетом, мы заплатили киберпреступнику, подтвердив, что копия, которую они удалили, была уничтожена».

Преступники жертвам: «доверьтесь нам»

Такие подтверждения не стоят бумаги, на которой они могут быть напечатаны.

«Они не собираются удалять ваши данные. Я имею в виду, что они просто сделают вид, что удаляют ваши данные», — говорит Аллан Лиска, главный аналитик разведки в Recorded Future. «Мы видели это снова и снова, и я думаю, что организации полностью осознают это. Тогда возникает вопрос: «Заплатят ли они за иллюзию того, что данные были удалены?»

К сожалению, ответ слишком часто кажется «да». В июле британские власти призвали адвокатов посоветовать своим клиентам не платить за гарантии удаления данных от преступников. Управление Комиссара по информации, которое обеспечивает соблюдение законов Великобритании о конфиденциальности, в том числе Общего регламента по защите данных, подчеркнуло этот момент, заявив, что, если оно расследует организацию после взлома и обнаружит недостатки в кибербезопасности, тот факт, что она заплатила за обещание удаления данных, не будет иметь значения. каким-либо образом уменьшить размер штрафа, который может грозить компании.

Билл Сигел, соучредитель и генеральный директор компании Coveware, которая помогает организациям реагировать на атаки программ-вымогателей, включая иногда согласование требований о выкупе, продолжает призывать жертв перестать платить за обещания об удалении данных, не в последнюю очередь потому, что это плохо для них.

«Откровенно говоря, это может усугубить проблему», — говорит он. Получается, что жертва, которая платит за абстрактные заверения, похоже, соблазняет злоумышленников вернуться и попытаться вымогать у них еще больше.

С точки зрения бизнеса есть нюансы в том, чего компании могут добиться с помощью выкупа.

«Шифрование сопряжено с реальными затратами на восстановление, и если ваши резервные копии были повреждены и так далее, у вас может не быть другого выбора, кроме как заплатить», — говорит Лиска.

Но платить за инструмент — это не то же самое, что платить за обещание. «Если вы платите выкуп за инструмент или ключ дешифрования и получаете инструмент или ключ дешифрования, он не деградирует и не исчезает, верно?» — говорит Сигел из Coveware. «Надеюсь, вы сможете восстановить свои данные, если заранее проявите должную осмотрительность и протестируете их».

Несколько групп реагирования на инциденты и юридические фирмы, в том числе те, которые работают со страховщиками, отслеживают группы вымогателей, изучая их подход к переговорам и готовность предоставлять работающие дешифраторы. Все это может лучше повлиять на решение жертвы о том, платить выкуп или нет, и что они получат взамен.

С группами вымогателей полезно быть информированным — и на благо всех, чтобы не увековечивать экосистему вымогателей, расплачиваясь за изначально пустые обещания». ***(Mathew J. Schwartz. Why Do Ransomware Victims Pay for Data Deletion Guarantees? // Information Security Media Group, Corp. (https://www.govinfosecurity.com/blogs/do-ransomware-victims-pay-for-data-deletion-guarantees-p-3342). 02.01.2023).***

***

«Атаки программ-вымогателей стали одним из самых распространенных киберпреступлений, совершаемых против американских компаний. Злоумышленник, часто из-за рубежа, получит доступ для загрузки вредоносного ПО в сетевое хранилище компании или платформы приложений, которые шифруют все файлы, к которым он может получить доступ. Сообщение или текстовый файл обычно оставляют с инструкциями о том, как связаться с злоумышленником, чтобы заплатить выкуп за ключ дешифрования. В худшем случае атака программы-вымогателя может заморозить бизнес-операции, эффективно лишив доступа к критически важным системам компании и сделав их бесполезными. Помимо воздействия на бизнес, какие юридические последствия создает атака программ-вымогателей?

Конфиденциальность

Наибольшую юридическую озабоченность вызывает конфиденциальность. По определению, атаки программ-вымогателей получают доступ к внутренним системам, которые обслуживаются или принадлежат бизнесу. Однако не все атаки программ-вымогателей одинаковы, и обязательства в отношении конфиденциальности различаются от одной атаки к другой.

Самая безобидная атака программы-вымогателя — это та, которая шифрует данные в идентифицируемом месте, которое, как подтверждено, не содержит никакой личной информации для сотрудников или клиентов и которое можно легко восстановить из чистых резервных копий. Предполагая, что информация, которая соответствует определению персональных данных (включая PII или PHI), затронута, требуется дальнейший юридический анализ, чтобы определить, несет ли компания дополнительные юридические обязанности. При такой оценке доступность надежных системных журналов, сетевого трафика и другой информации становится критически важной. Например, законы некоторых штатов об уведомлении об утечке данных не требуют уведомления потенциально затронутых лиц, если только информация не была получена неавторизованным злоумышленником. Другими словами, если данные не были скопированы или удалены злоумышленником, нарушения нет. Однако другие государства определяют утечку данных как несанкционированное получение или доступ к определенным категориям защищенной информации. В штатах, которые включают

«доступ» в свое определение нарушения, злоумышленник-вымогатель, который может удаленно просматривать сетевое окружение и выбирать целевые системы файлов для атаки, получил доступ. Если вредоносное ПО работает самостоятельно и к нему не было доступа извне, помимо выполнения компьютерного кода, можно утверждать, что не было несанкционированного доступа человека. Получить конкретную информацию о том, привела ли атака к потере данных, может быть сложно, но простое шифрование без дополнительных действий, возможно, является «лучшим сценарием» по сравнению со сценарием, связанным с потерей или удалением информации.

Хакеры это заметили. В некоторых случаях атакующая программа-вымогатель предоставит доказательства того, что они получили доступ к личной информации и могут опубликовать ее в даркнете. Эти атаки «доказательство жизни» предоставляют фрагмент личной информации — например, один из многих номеров социального страхования, хранящихся в теперь зашифрованной базе данных, — и хакеры будут угрожать опубликовать всю личную информацию, если их требования не будут выполнены. К сожалению, несмотря на то, что злоумышленники-вымогатели, когда им платят, почти всегда выполняют свою часть сделки, предоставляя ключи дешифрования и удаляя похищенные данные, тот факт, что информация была получена неуполномоченными лицами, несомненно, является нарушением, даже если злоумышленники соглашаются удалить ее. Это означает, что если речь идет о личной информации, атака, включающая эксфильтрацию, скорее всего, вызовет обязательство сообщать об этом.

Конгресс внес несколько законопроектов, которые требуют сообщать об атаках программ-вымогателей в Министерство внутренней безопасности в течение определенного периода времени, обычно от 24 до 72 часов, с уже действующими определенными обязательными обязательствами по отчетности для определенных отраслей. Однако неясно, какие обязательства возьмет на себя атакованная сторона и изменит ли эти обязательства эксфильтрация личной информации.

Интеллектуальная собственность

Многие компании хранят свой «секретный соус» как коммерческую тайну. Независимо от того, разрабатывает ли компания программное обеспечение, производит клей или торгует на Уолл-стрит, защита коммерческой тайны имеет первостепенное значение для нематериальных активов компании, которые не запатентованы. Атака программы-вымогателя может привести к эксфильтрации коммерческой тайны и возможной публикации коммерческой тайны — действие, которое устранит любую защиту имеющейся коммерческой тайны. И жертвы таких атак с удивлением узнают, что их киберстраховка часто не покрывает такие убытки. Действительно, важные коммерческие тайны должны храниться под замком, чтобы защитить их от использования или публикации злоумышленниками с программами-вымогателями.

Атаки программ-вымогателей принимают разные формы. Многие из них связаны с эксфильтрацией или несанкционированным доступом к личной информации или коммерческой тайне сотрудников или клиентов, что может привести к катастрофическим потерям для компании с большим объемом

конфиденциальной или коммерческой тайны. В дополнение к обеспечению надежной защиты сети и данных, обучению сотрудников и хранению записей для сведения к минимуму воздействия атак, крайне важно (а в некоторых штатах требуется), чтобы предприятия имели письменную программу реагирования на информационную безопасность для управления и устранения кибератак. При расследовании инцидента и реагировании на него важно определить тип атаки программы-вымогателя, чтобы компания могла определить полученное в результате уведомление о конфиденциальности и потерю интеллектуальной собственности, связанную с атакой…» ***(Jason Priebe, Patrick Muffo. Ransomware Attacks: Harmless Annoyances or Catastrophic Events? // Seyfarth Shaw LLP. (https://www.tradesecretslaw.com/2023/01/articles/privacy-2/ransomware-attacks-harmless-annoyances-or-catastrophic-events/#page=1). 19.01.2023).***

***

Програми-трояни

«Банковский троянец Hook может имитировать клики и отправлять сообщения в WhatsApp

Усовершенствованный банковский троянец Android, получивший от исследователей безопасности название Hook, способен удаленно управлять мобильными устройствами, способствуя растущему пересечению вредоносного ПО для наблюдения и финансового мошенничества.

Троянец, который анализ датской фирмы по кибербезопасности ThreatFabric характеризует как улучшенную версию существующего трояна Ermac, способен выполнять «полную цепочку атак от заражения до мошеннической транзакции».

Hook использует реализацию совместного использования экрана, известную как виртуальные сетевые вычисления, для достижения функциональности инструмента удаленного доступа, способного выполнять такие функции, как создание снимка экрана, имитация щелчков и ввод команд жестами смахивания. Он может передавать данные геолокации и контролировать файлы.

Крюк также может открывать приложение чата WhatsApp для извлечения сообщений, а также отправлять новостное сообщение, которое может быть использовано операторами троянца для распространения вредоносного ПО.

ThreatFabric сообщает, что злоумышленник, известный как DukeEugene, который арендует Ermac уже около 18 месяцев, начал предлагать Hook в середине января. Фирма сообщила The Hacker News, что доступ к Hook стоит 7000 долларов в месяц.

Появление Hook происходит в момент растущей глобальной тревоги по поводу превращения передового шпионского ПО в товар и беспокойства по поводу легкости, с которой злоумышленники и правительства могут собирать личные данные с личных устройств.

ThreatFabric утверждает, что Hook — это вариант Ermac, а не совершенно новый троянец, основанный на сходстве кода с Ermac, включая некоторые команды на русском языке, которые не добавляют функциональности.

Сам Ermac является потомком мобильного банковского трояна Cerberus, исходный код которого попал в сеть в 2020 году на российский даркнет-форум (см. Атаки с использованием Cerberus Banking Trojan Surge)». ***(Mihir Bagwe. Malware Blurs Line Between Banking Trojan and Surveillance // Information Security Media Group, Corp. (https://www.govinfosecurity.com/malware-blurs-line-between-banking-trojan-surveillance-a-21002). 23.01.2023).***

***

Фішингові атаки

«Південнокорейська компанія з кібербезпеки AhnLab попереджає користувачів про фішинговий сайт, який пропонує завантажити карткову гру з NFT-токенами під брендом Pokémon. Насправді ж ресурс поширює зловмисне програмне забезпечення. Шкідливий сайт пропонує власний NFT-маркетплейс, а також спонукає робити ставки за допомогою цифрових токенів — і все це базується на популярній японській медіафраншизі.

Геймери, які користувалися фішинговим сайтом, замість гри завантажували інструмент віддаленого доступу до ПК. Це дозволило хакерам отримати віддалений контроль над ґаджетами жертв.

В AhnLab підкреслили, що утиліта NetSupport Manager дозволяє зловмисникам дистанційно керувати мишею та клавіатурою комп'ютера, перевіряти системне керування файлами, історію браузера та навіть інсталювати ще більше шкідливих програм. Геймерів та прихильників франшизи Pokémon попросили користуватися лише офіційними ресурсами та повідомляти про підозріле ПЗ зі сторонніх сайтів.

З моменту створення бренду «Pokémon» вигаданий персонаж не перестає бути популярним — багато користувачів і досі бажають отримати власну казкову істоту, а чимало підприємців спекулюють на імені бренду. Так наприкінці грудня стало відомо, що на розробників NFT-гри про покемонів PokeWorld подали до суду за незаконне використання покемонів у проекті. Керівництво The Pokemon Company (TPC) могло б і не дізнатися про піратство, якби зловмисники самі себе не видали через пресреліз.

Розробник Джастін Пінкні пішов ще далі й створив модель штучного інтелекту, що створює покемонів, схожих на людей — користувачу достатньо детально описати бажаного персонажа й алгоритм створить його покемон-копію». ***(Гра з цифровими токенами Pokemon поширює віруси // No worries! (https://noworries.news/gra-z-czyfrovymy-tokenamy-pokemon-poshyryuye-virusy/). 09.01.2023).***

***

«Служба інформаційних технологій та кібербезпеки Молдови (STISC) повідомила про хвилю фішингових атак на сайти держустанов. На електронні адреси надійшло понад 1330 шкідливих повідомлень.

Про це йдеться у заяві на сайті STISC. Згідно з повідомленням, користувачам домену.md повідомляють про закінчення терміну дії імені домену і просять продовжити його, перейшовши за посиланням для оплати.

«STISC рекомендує не переходити за такими посиланнями та блокувати їх. Також закликає завжди перевіряти справжнє джерело повідомлення та дотримуватись правил кібергігієни», – повідомило відомства.

Раніше SPEKA повідомляла, що у Польщі знайшли хакерську групу, яка восени провела кібератаки на уряд країни». ***(Руслан Сорока. У Молдові зафіксували хвилю фішингових атак на сайти держустанов // Speka.Media (https://speka.media/xakeri-atakuyut-derzustanovi-moldovi-shho-vidomo-98xowv). 05.01.2023).***

***

«Фишинг набирает обороты, и любой, кто использует электронную почту, текстовые сообщения и другие формы связи, является потенциальной жертвой.

Эти атаки, при которых киберпреступник отправляет вводящее в заблуждение сообщение, предназначенное для того, чтобы обмануть пользователя и заставить его предоставить конфиденциальную информацию, такую как номера кредитных карт, или запустить вредоносное ПО в системе пользователя, могут быть чрезвычайно эффективными, если все сделано правильно.

Эти типы атак становятся все более изощренными, что делает их более опасными и более распространенными. Исследование, проведенное в октябре 2022 года поставщиком средств безопасности обмена сообщениями SlashNext, проанализировало миллиарды URL-адресов на основе ссылок, вложений и сообщений на естественном языке в электронной почте, мобильных устройствах и каналах браузера за шестимесячный период и обнаружило более 255 миллионов атак. Это на 61% больше числа фишинговых атак по сравнению с 2021 годом.

Исследование показало, что киберпреступники переносят свои атаки на мобильные и личные каналы связи, чтобы добраться до пользователей. Он показал 50-процентное увеличение атак на мобильные устройства, при этом мошенничество и кража учетных данных находятся в верхней части списка полезной нагрузки.

«То, что мы наблюдаем, — это увеличение использования голосовой почты и текстовых сообщений в рамках двусторонних кампаний фишинга и BEC [компрометация деловой электронной почты]», — сказала Джесс Берн, старший аналитик Forrester Research. «Злоумышленники оставляют голосовое сообщение или отправляют текст об отправленном им электронном письме, либо повышая доверие к отправителю, либо повышая срочность запроса».

По словам Берна, фирма получает много запросов от клиентов об атаках BEC в целом. «Поскольку геополитические разногласия подрывают деятельность групп вымогателей, а криптовалюта — предпочтительный метод выплаты выкупа — в последнее время рушится, злоумышленники возвращаются к старомодному мошенничеству, чтобы заработать деньги», — сказал он. «Таким образом, BEC находится на подъеме».

Преступники, использующие фишинговые атаки, основанные на налоговом сезоне, торговых сделках

Одна из итераций фишинга, о которой люди должны знать, — это целевой фишинг, более целенаправленная форма фишинга, в которой часто используются актуальные приманки.

«Хотя это не новая тактика, темы и темы могут меняться в зависимости от мировых или даже сезонных событий», — сказал Люк Макнамара, главный аналитик консалтинговой компании по кибербезопасности Mandiant Consulting. «Например, поскольку мы находимся в праздничный сезон, мы можем ожидать увидеть больше фишинговых приманок, связанных с покупками. Во время региональных налоговых сезонов злоумышленники могут аналогичным образом пытаться использовать пользователей в процессе подачи налоговых деклараций с помощью фишинговых электронных писем, содержащих налоговые темы в строке темы».

По словам Макнамара, фишинговые темы также могут быть общими, например, электронное письмо от поставщика технологий о сбросе учетной записи. «Более продуктивные преступные кампании могут использовать менее конкретные темы, и, наоборот, более целенаправленные кампании злоумышленников, вовлеченных в такую деятельность, как кибершпионаж, могут использовать более конкретные фишинговые приманки», — сказал он.

Что люди должны делать, чтобы предотвратить попытки фишинга

Отдельные лица могут предпринять шаги, чтобы лучше защитить себя от фишинговых атак.

Один из них заключается в том, чтобы проявлять бдительность при предоставлении личной информации, будь то человеку или на веб-сайте.

«Фишинг — это форма социальной инженерии, — сказал Берн. «Это означает, что фишеры используют психологию, чтобы убедить своих жертв совершить действие, которое они обычно не предпринимают. Большинство людей хотят быть полезными и делать то, что говорит им власть. Фишеры знают об этом, поэтому они охотятся на эти инстинкты и просят жертву помочь с проблемой или сделать что-то немедленно».

Если электронное письмо от определенного отправителя неожиданное, если оно просит кого-то сделать что-то срочно или если оно запрашивает информацию или финансовые данные, которые обычно не предоставляются, сделайте шаг назад и внимательно посмотрите на отправителя, сказал Бёрн.

«Если отправитель выглядит законным, но что-то по-прежнему кажется неправильным, не открывайте никаких вложений и не наводите курсор мыши на какие-либо гиперссылки в теле письма и смотрите на URL-адрес, на который указывает ссылка», — сказал Берн. «Если это не похоже на законное место назначения, не нажимайте на него».

По словам Бёрна, если подозрительное сообщение поступает из известного источника, свяжитесь с этим человеком или компанией по отдельному каналу и узнайте, отправили ли они сообщение. «Вы избавите себя от многих проблем и предупредите человека или компанию о фишинговой афере, если электронное письмо исходит не от них», — сказал он.

Рекомендуется быть в курсе новейших методов фишинга. «Киберпреступники постоянно совершенствуют свои методы, поэтому люди должны быть начеку», — сказала Эмили Моссберг, глобальный кибер-лидер Deloitte. «Фишеры наживаются на человеческих ошибках».

Другой хорошей практикой является использование антифишингового программного обеспечения и других инструментов кибербезопасности для защиты от потенциальных атак и обеспечения безопасности личных и рабочих данных. Это включает в себя инструменты автоматизированной поведенческой аналитики для обнаружения и снижения индикаторов потенциального риска. «Использование этих инструментов среди сотрудников значительно возросло», — сказал Мосбург.

Другая технология, многофакторная аутентификация, «может обеспечить один из лучших уровней безопасности для защиты вашей электронной почты», — сказал Макнамара. «Это обеспечивает еще один уровень защиты, если злоумышленник успешно скомпрометирует ваши учетные данные». ***(Bob Violino. Phishing attacks are increasing and getting more sophisticated. Here's how to avoid them // CNBC LLC (https://www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html?__source=iosappshare%7Ccom.flipboard.flipboard-ipad.ShareExtension). 07.01.2023).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Правоохоронці США спільно з Німеччиною та Нідерландами ліквідували одну з найбільших мереж хакерів-вимагачів Hive, повернувши вкрадені цифрові активи більшості жертв.

Як повідомили представники Міністерства юстиції США, спільна з Федеральним бюро розслідувань операція зі знищення міжнародної групи криптозлочинців завершилась успішно. Хакери атакували школи, банки та лікарні у понад 80 країнах. З червня 2021 року їх жертвами стали приблизно 1 500 установ по всьому світу, а самі зловмисники заробили понад $ 100 мільйонів у криптовалютах.

У чому полягала схема роботи хакерів? Спершу вони викрадали конфіденційні дані з електронних листів, документів та файлів та шифрували їх. Після чого вимагали у власників цієї інформації викуп у біткоїнах — це мало гарантувати видалення даних в архівах хакерів та збереження конфіденційності. Якщо жертви відмовлялася платити, всі викрадені дані вимагачі Hive публікували у даркнеті.

ФБР вдалося проникнути в мережу Hive ще в липні 2022 року, відтоді правоохоронці знайшли та вилучили понад 1 300 ключів дешифрування, щоб допомогти жертвам повернути свої кошти. Правоохоронці Німеччини та

Нідерландів координували операцію — вони взяли під контроль сервіси та сайти шахраїв, що і допомогло знищити Hive.

Ліквідація мережі Hive — не єдина успішна операція ФБР з боротьби з криптозлочинцями. У липні 2022 року поліція Естонії разом зі спеціалістами ФБР затримала двох засновників хмарного майнера біткоїнів HashFlare. Сергія Потапенка та Івана Туригіна підозрюють у шахрайстві з криптовалютою на $ 575 мільйонів. Згідно з інформацією, зібраною в ході розслідування, громадяни Естонії працювали за схемою Понці, використовуючи гроші нових інвесторів для виплат тим, хто вклав свої кошти у HashFlare раніше». ***(Хакерів, які зламали 1500 державних установ у 80 країнах, затримало ФБР // No worries! (https://noworries.news/hakeriv-yaki-zlamaly-1500-derzhavnyh-ustanov-u-80-krayinah-zatrymalo-fbr/). 27.01.2023).***

***

«Євроюст і Європол, правоохоронні органи країн-членів ЄС, ліквідували масштабну мережу кіберзлочинців — ними виявилися резиденти з Німеччини, Кіпру, Болгарії та Сербії (де сьогодні ховається До Квон). За інформацією обох відомств, злочинці пропонували довірливим вкладникам «виняткові можливості для інвестицій у криптовалюти». Інвесторів заманювали за допомогою таргетованої реклами у соцмережах, фейкових сайтів та спеціалізованих кол-центрів.

За попередніми даними, найбільших втрат зазнали інвестори з Німеччини. Загальні фінансові збитки, завдані жертвам, перевищили € 2 млн. Європол зазначив, що тільки на території східної Європи діяло мінімум чотири підконтрольні злочинцям кол-центри. Слідчі припускають, що в ході розслідування можуть бути виявлені нові злочинні факти, а кількість постраждалих, як і незаконний прибуток кібершахраїв, кратно зросте.

Загалом правоохоронцями було затримано 261 особу: 42 у Болгарії, 2 на Кіпрі, 3 у Німеччині та 214 у Сербії. Декілька членів злочинної мережі вже опинилися за ґратами. На цей час поліція конфіскувала 3 апаратні гаманці з приблизно $ 1 млн у криптовалютах, близько € 50 000 євро готівкою, 3 транспортні засоби, електронне обладнання, документи та резервні копії даних…». ***(У ЄС затримали угруповування міжнародних кібер злочинців, що крали криптовалюту // No worries! (https://noworries.news/u-yes-zatrymaly-ugrupovuvannya-mizhnarodnyh-kiber-zlochyncziv-shho-kraly-kryptovalyutu/). 17.01.2023).***

***

«Человек, предположительно стоящий за схемой на 114 миллионов долларов по обману децентрализованной криптовалютной платформы Mango Markets, теперь сталкивается с гражданским иском от федеральных регулирующих органов США, а также с уголовным преследованием.

Комиссия по торговле товарными фьючерсами подала иск в федеральный суд Манхэттена с требованием вернуть Аврааму Айзенбергу деньги, которые он якобы украл, выплатить штраф в размере не менее 1 миллиона долларов и запретить торговать цифровыми активами в будущем.

Гражданский иск, вероятно, беспокоит Айзенберга меньше всего. Он находится в тюремной камере Пуэрто-Рико с момента его ареста в конце декабря ФБР.

В уголовных и гражданских делах против Айзенберга утверждается, что он раздул стоимость криптовалюты Mango Markets посредством серии крупных покупок валюты, которая обычно мало торгуется. CFTC и прокуратура говорят, что он отозвал завышенную стоимость длинной позиции по криптовалюте Mango, используя токены в качестве залога, и в процессе истощил децентрализованную платформу почти всех ее доступных средств, включая депозиты клиентов.

«Mango Markets осталась с почти пустой сумкой», — написали адвокаты CFTC в своей жалобе. Уголовное дело Айзенберга включает обвинения, наказуемые десятилетиями тюремного заключения.

Иск CFTC представляет собой первое правоприменительное действие агентства, касающееся децентрализованной финансовой платформы, и его первое действие против конкретного метода, который Айзенберг якобы использовал для завышения стоимости криптовалюты Mango — так называемой «стратегии манипулирования ценами оракула».

Mango Markets рассчитала стоимость своего токена, взяв среднее значение рыночных цен на трех независимых криптовалютных биржах. Приложения, которые принимают эти потоки данных и получают среднее значение торговых цен, являются оракулами. Федеральное правительство заявляет, что Айзенберг знал, какие три торговые платформы функционируют как потоки данных оракула, и нацелил их на быстрые покупки токена Mango, чтобы поднять цену. По данным CFTC, он увеличил токен в 13 раз за счет торгов, которые проводились в течение 30 минут.

Компания CertiK, занимающаяся безопасностью блокчейна, ранее сообщила Information Security Media Group, что злоумышленник использовал два кошелька, чтобы манипулировать ценой токена Mango до пиковой отметки в 0,91 доллара. Mango Markets объяснила технические детали атаки в серии твитов.

Прокуратура утверждает, что Айзенберг, вероятно, знал о последствиях своих действий. Он сел на рейс в Израиль, и время полета подразумевает, что поездка могла быть «попыткой избежать задержания правоохранительными органами сразу после схемы манипулирования рынком», — заявил специальный агент ФБР Брэндон Рач в интервью 19 декабря. 23 федерального уголовного дела. Айзенберг совершил предполагаемое мошенничество, находясь в Пуэрто-Рико.

4 января суд Пуэрто-Рико постановил, что Айзенберг должен оставаться в тюрьме до суда». ***(Rashmi Ramesh. Mango Markets Hacker in US Regulator's Crosshairs // Information Security Media Group, Corp. (https://www.govinfosecurity.com/mango-markets-hacker-in-us-regulators-crosshairs-a-20901). 10.01.2023).***

***

«Сэм Бэнкман-Фрид не признал себя виновным в мошенничестве и других уголовных обвинениях в федеральном суде Манхэттена, через

несколько недель после того, как Министерство юстиции обвинило 30-летнего парня в многолетней афере на FTX на несколько миллиардов долларов.

Сообщается, что окружной судья Южного округа Нью-Йорка Льюис А. Каплан назначил предварительную дату судебного разбирательства на 2 октября в отношении обанкротившегося основателя торговой платформы криптовалюты. Если вина бывшего миллиардера и крипто-вундеркинда будет доказана, ему грозит до 115 лет лишения свободы.

У Каплана есть опыт работы с мошенничеством с криптовалютами. В 2016 году он вынес приговор по первому делу о мошенничестве с ценными бумагами, связанному с биткойнами.

В декабре правоохранительные органы арестовали Бэнкмана-Фрида на Багамах после того, как федеральное большое жюри США вынесло ему обвинительный акт по восьми пунктам, обвиняя его в мошенничестве с использованием электронных средств, мошенничестве с товарами, мошенничестве с ценными бумагами, отмывании денег и нарушении законов о финансировании избирательных кампаний.

Он впервые предстал перед федеральным судом Нью-Йорка 22 декабря после своего решения не оспаривать экстрадицию из островной тюрьмы. С тех пор он вышел под залог в 250 миллионов долларов и находится под домашним арестом в Пало-Альто, штат Калифорния, где живут его родители, оба профессора права Стэнфордского университета.

Прокуратура получила соглашения о признании вины от двух сотрудников Bankman-Fried, бывшего технического директора FTX и соучредителя Гэри Ванга и Кэролайн Эллисон, генерального директора Alameda Research, дочерней компании FTX. Эллисон грозит до 110 лет лишения свободы после того, как она признала себя виновной по семи пунктам обвинения, включая два пункта обвинения в мошенничестве с использованием электронных средств, два пункта обвинения в сговоре с целью совершения мошенничества с использованием электронных средств, сговоре с целью совершения мошенничества с товарами, мошенничестве с ценными бумагами и отмывании денег. Вану грозит до 50 лет тюремного заключения после того, как он признал себя виновным по обвинению в сговоре с целью совершения мошенничества с ценными бумагами, мошенничества с товарами и мошенничества с использованием электронных средств. Освобожденные под залог в размере 250 000 долларов, Эллисон и Ван в настоящее время помогают прокурорам в их деле против Бэнкман-Фрид». ***(Rashmi Ramesh. Sam Bankman-Fried Pleads 'Not Guilty' in Criminal Case // Information Security Media Group, Corp. (https://www.govinfosecurity.com/sam-bankman-fried-pleads-not-guilty-in-criminal-case-a-20843). 03.01.2023).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Версії Windows 7 Professional і Enterprise більше не отримуватимуть розширені оновлення безпеки для критичних і важливих уразливостей, починаючи з вівторка, 10 січня 2023 року. Корпорація Майкрософт випустила застарілу операційну систему в жовтні 2009 року. Потім у січні 2015 року завершилася її підтримка, а в січні 2020 року – розширена підтримка.

Програма Extended Security Update (ESU) була останньою можливістю для клієнтів, яким все ще потрібно було запускати застарілі продукти Microsoft після завершення підтримки в системах Windows 7. Усі випуски Windows 8.1, випущені дев'ять років тому в листопаді 2013 року, також досягнуть EOS того самого дня.

«Більшість пристроїв з Windows 7 не відповідатимуть апаратним вимогам для оновлення до Windows 11, як альтернативу, сумісні комп'ютери з Windows 7 можна оновити до Windows 10, придбавши та встановивши повну версію програмного забезпечення», — пояснює Microsoft.

«Перш ніж інвестувати в оновлення Windows 10, врахуйте, що термін підтримки Windows 10 закінчиться 14 жовтня 2025 року».

Корпорація Майкрософт рекомендує клієнтам із пристроями, які не відповідають технічним вимогам для останньої версії Windows, замінити їх на пристрої, які підтримують Windows 11, щоб скористатися перевагами найновіших апаратних можливостей. Наразі Windows 7 працює на понад 11% усіх систем Windows у всьому світі, а Windows 8.1 використовують 2,59% клієнтів Microsoft, за даними Statcounter GlobalStats.

Веб-браузери також припиняють підтримку Windows 7

Наступного тижня Redmond також випустить Microsoft Edge 109, останню версію веб-браузера з підтримкою Windows 7 і Windows 8/8.1. Ця версія Microsoft Edge також буде останньою, яка підтримуватиме Windows Server 2008 R2, Windows Server 2012 і Windows Server 2012 R2. Подібне оголошення було зроблено Google у жовтні, коли компанія заявила, що версія 110 веб-браузера Google Chrome також, ймовірно, припинить підтримку Windows 7 і 8.1, починаючи з лютого 2023 року.

Microsoft Edge 109 і Google Chrome 110 продовжуватимуть працювати на застарілих операційних системах, але вони більше не отримуватимуть оновлення системи безпеки та виправлення помилок, наражаючи своїх користувачів на ризики безпеки. Google Chrome зараз має частку ринку понад 64%, за ним йдуть Safari з приблизно 18% і Microsoft Edge (який використовує механізм рендерингу Chrome Blink з удосконаленнями від Microsoft) з трохи більше ніж 4%. Інші постачальники вже відмовилися від підтримки Windows 7 до дати, коли ОС перестане отримувати оновлення безпеки. Наприклад, NVIDIA більше не надає драйвери для Windows 7 і Windows 8.1 з минулого року, починаючи з жовтня 2021 року». ***(Володимир Неволін. Windows 7 припинить отримувати розширені оновлення безпеки // Т4***

(https://t4.com.ua/soft/windows-7-prypynyt-otrymuvaty-rozshyreni-onovlennya-bezpeky/). 08.01.2023).

***

«…Американська компанія Microsoft повідомила, що 10 січня 2022 року відключить Windows 7 та Windows 8.1 від оновлень безпеки та припинить технічну підтримку.

Тижнем раніше підтримку цих популярних версій систем припинив браузер Microsoft Edge, а версія Microsoft Edge 109 стане останньою, яку підтримують застарілі операційні системи. Також з 7 лютого їх підтримку припить популярний браузер Google Chrome.

Попри це обидва браузери продовжать працювати на цих операційних системах, вони більше не отримають жодних критично важливих оновлень або нових функцій.

Також буде припинено підтримку WebView2 – інструмента, який дозволяє розробникам вбудовувати веб-контент в свої додатки, буде припинено 10 січня, тобто сьогодні.

За оцінками експертів станом на 2021 рік Windows 7 все ще користувалося понадю 100 мільйонів осіб. Опитування Lansweeper, проведене, в жовтні минулого року показало, що кількість комп'ютерів з XP, 7 та 8 все ще перевищує кількість комп'ютерів з Windows 11.

Microsoft вперше повідомила про плани припинити підтримку цих популярних систем ще в 2020 році. Єдине виключення це ті, хто оплатив за додаткові три роки оновлень.

Якщо комп'ютери чи ноутбуки користувачів не підтримують операційні системи вище Windows 7 та 8,1, то рекомендовано придбати більш потужні гаджети, що уникнути ймовірних проблем з безпекою. Проте навряд чи ці системи стануть менш популярними, і справа навіть не в слабких комп'ютерах, а в зручності використання.

Раніше Microsoft припинили підтримку вже легендарної Windows XP, але чимало користувачів продовжують користуватися системою ризикуючи своїми даними. Зважаючи на регулярні кібератаки російських спецслужб, краще перестрахуватися та подбати про свою безпеку вже зараз, адже невідомо чим легковажність може обернутися в майбутньому». ***(Дані мільйонів користувачів будуть під загрозою: припиняється підтримка популярних версій Windows // GSMinfo (https://gsminfo.com.ua/136522-dani-miljoniv-korystuvachiv-budut-pid-zagrozoyu-prypynyayetsya-pidtrymka-populyarnyh-versij-windows.html). 10.01.2023).***

****

«Хакери навчились використовувати вразливості Galaxy App Store і таємно встановлювати шкідливі додатки на гаджети Samsung. Про дефект у магазині додатків Samsung стало відомо ще наприкінці грудня минулого року — тоді ж експерти з кібербезпеки NCC Group виявили вразливості та попередили про це виробника. Втім, розв'язати всі проблеми Galaxy App Store вдалось лише зараз, після запуску оновлення.

Перша вразливість магазину додатків Samsung стосувалась неналежного контролю доступу. Без відома власників, хакери могли встановлювати на пристрої жертв довільні програми. Другий дефект стосувався неправильної перевірки коду — він дозволяв хакерам запускати на пристроях користувачів шкідливий JavaScript-код.

Для експлуатації першої вразливості зазвичай необхідний локальний доступ до гаджета жертви, але, як пояснили фахівці, досвідчені зловмисники роблять це дистанційно. Захищеними від атак були лише пристрої на ОС Android 13 (навіть з неоновленою версією Galaxy App Store). Втім, основна проблема полягала в тому, що лише 7% всіх Android-пристроїв завантажили оновлення ОС.

Щодо другої вразливості, вона стосувалась роботи WebView-компонента (вбудованого браузера) Galaxy App Store — він підтримує обмежену кількість доменних імен. До виправлення проблеми фільтр доменів був налаштований некоректно, що дозволяло обходити обмеження та відкривати сторінки за підконтрольними хакерам адресами, в які зловмисники вбудовували шкідливий код…». ***(Хакери навчились таємно встановлювати шкідливі додатки на гаджети Samsung // No worries! (https://noworries.news/hakery-navchylys-tayemno-vstanovlyuvaty-shkidlyvi-dodatky-na-gadzhety-samsung/). 25.01.2023).***

***

«Представники Apple підтвердили, що хакери тривалий час використовували вразливість нульового дня на пристроях iPhone та iPad. За словами спеціалістів з безпеки компанії, проблема давно усунута — це відбулось завдяки запуску чергового оновлення.

Вразливістю нульового дня (або 0-day) є дефект безпеки ПЗ, який невідомий тому, хто зацікавлений у його усуненні, наприклад, розробнику. Хакерські атаки не можливо передбачити чи вберегти від них пристрої - зловмисники використовують вразливість на свою користь до того, як постачальник дізнається про її існування

У ситуації з Apple кіберзлочинці будь-якими доступними їм методами змушували своїх жертв відвідати шкідливий сайт. Після зараження пристрою у них з’являлася можливість виконувати команди в базовій операційній системі, розгортати додаткові шкідливі/шпигунські програми та запускати інші шкідливі дії. Вразливість торкнулась старих iPhone та iPad: iPhone 5s, iPhone 6, iPhone 6 Plus, iPad Air, iPad mini 2, iPad mini 3 та iPod touch (6-го покоління).

Більш конкретної інформації про хакерські атаки спеціалісти Apple поки не опублікували. Очевидно, компанія очікує, коли оновлення безпеки розгорнеться на більшості пристроїв, щоб у зловмисників було менше даних для написання експлойтів.

Нагадаємо, що вчора ми розповідали про масштабну хакерську схему Vastflux. Кіберзлочинці підробили понад 1700 відомих додатків для iOS — все для отримання прибутків з реклами. Хакери впроваджували шкідливий JavaScript-код у рекламні оголошення, а потім «нашаровували» відеоплеєри з рекламою один на одний. Так, що жодного з них не було видно користувачеві — всі вони відображалися за активним вікном. Однак із кожного запущеного відео шахраї отримували прибуток від монетизації». ***(Apple визнала, що хакери можуть***

контролювати старі версії iPhone // No worries! (https://noworries.news/apple-vyznala-shho-hakery-mozhut-kontrolyuvaty-stari-versiyi-iphone/). 25.01.2023).

***

«Згідно з інформацією видання New Scientist, хакери знайшли ще одну вразливість техніки та вже використовують її для атак. Цього разу зловмисники звернули увагу на можливість пристроїв з підтримкою бездротового протоколу Wi-Fi обмінюватися даними між собою, навіть якщо вони не підключені до однієї мережі. Хакери дистанційно розряджають акумулятори гаджетів, наприклад камер спостереження.

Експерти зі Стенфордського університету назвали виявлену вразливість «ввічливим Wi-Fi». За словами Алі Абеді, щоб розряджати пристрої хакерам не потрібні доступи, паролі чи спеціальні дозволи. Достатньо лише знайти безпровідні пристрої з Wi-Fi.

Як з'ясували дослідники, постійний пінг пристроїв з Wi-Fi, що працюють від акумуляторів, не дозволяє гаджетам йти в режим сну, через що заряд акумуляторів падає швидше. Команда спеціалістів з безпеки протестувала 5000 різних пристроїв від 186 виробників і з'ясувала, що всі вони є вразливими до атак такого типу.

Пристрої автоматично підтверджують запити на відправку пакетів фейкових даних, користувач навіть не отримує сповіщення про це. Схема працює на відстані до 200 метрів. Дослідники переконані, що з часом такі атаки стануть набагато поширенішими, адже їх неможливо передбачити чи уникнути наразі.

Ще на початку серпня ми розповідали як хакери майнять криптовалюти на відстані, заражаючи чужі пристрої. У деяких VPN-сервісах можуть бути віруси, які використовуються зловмисниками для видобутку цифрової валюти. Існує декілька ознак, які вказують на те, що зловмисники отримали доступ до пристрою та майнять криптовалюту: сильне нагрівання девайсу, занадто швидка розрядка та витрата великого обсягу трафіку». ***(Хакери навчились розряджати гаджети на відстані // No worries! (https://noworries.news/hakery-navchylys-rozryadzhaty-gadzhety-na-vidstani/). 11.01.2023).***

***

«Устройства с выходом в Интернет — цель для поддерживаемых государством хакеров

По словам Mandiant, злоумышленник, возможно, связанный с правительством Китая, воспользовался уже исправленной уязвимостью нулевого дня в виртуальной частной сети Fortinet.

Эксплойт, вероятно, является частью китайской модели использования устройств безопасности, подключенных к Интернету, говорится в сообщении в блоге фирмы по кибербезопасности, добавляя, что устройства безопасности обычно обеспечивают пользователям ограниченную прозрачность своей внутренней работы.

Такие устройства, как брандмауэры или FortiOS SSL-VPN от Fortinet, «часто сами по себе не защищены по своей сути», особенно потому, что они могут не позволять устанавливать на них другие продукты безопасности, такие как

обнаружение конечных точек и ответ. Основные функции могут быть закрыты производителями устройств, а интерфейсы администратора могут иметь ограниченные функции настройки и ведения журнала.

Сложность обнаружения вредоносной активности на устройстве безопасности делает эти устройства привлекательными для хакеров, спонсируемых государством. Поддерживаемые государством группы угроз также с большей вероятностью, чем рядовые киберпреступники, будут вкладывать ресурсы в разработку эксплойтов для устройств безопасности, учитывая высокий уровень ресурсов, необходимых для этого, говорит Мандиант. Это делает правительство и оборонный сектор вероятными целями.

Неизвестный злоумышленник, использующий уязвимость Fortinet VPN, официально обозначенную как CVE-2022-42475, возможно, начал делать это за несколько недель до того, как компания выпустила патч в декабре.

Он использовал эту уязвимость для создания бэкдора, который Mandiant дублирует Boldmove, включая вариант Linux, «специально разработанный для работы на брандмауэрах FortiGate».

Версия Boldmove для Windows, похоже, была скомпилирована в 2021 году, и Mandiant не обнаружил никаких эксплойтов, связанных с этим вариантом.

Расширенная версия бэкдора для Linux содержала команду, активирующую блокировку индикаторов путем отключения служб ведения журналов. Расширенная версия также содержала команду, которая позволяет хакерам отправлять запросы во внутреннюю службу Fortinet, «возможно, для изменения настроек устройства или предоставления доступа к Интернету внутренних частей связанной сети».

Собственный анализ Fortinet исправленной уязвимости пришел к выводу, что эксплойт потребовал бы от злоумышленника «глубокого понимания» FortiOS и связанного с ним оборудования. Знания Fortinet о злоумышленнике, который воспользовался им, свидетельствовали о группе с расширенными возможностями и предпочтениями правительственных или связанных с правительством целей». ***(Mihir Bagwe. Fortinet VPN Flaw Shows Pitfalls of Security Appliances // Information Security Media Group, Corp. (https://www.govinfosecurity.com/fortinet-vpn-flaw-shows-pitfalls-security-appliances-a-20990). 20.01.2023).***

***

«…Следующая итерация программы вознаграждения за обнаружение ошибок «Взломать Пентагон» становится буквальной: новый список целей для белых хакеров привязан к сети, контролирующей здание штаб-квартиры Министерства обороны США.

Военные периодически проводят программы вознаграждения за обнаружение ошибок с момента запуска «Взломать Пентагон» в 2016 году. Участники выявили уязвимости в тактическом воздушном истребителе F-15 и усовершенствованной защищенной аппаратной архитектуре. В нем приняли участие более 3000 хакеров, которые в совокупности заработали более 650 000 долларов в виде вознаграждений.

В запросе контракта на следующую сессию этического взлома сеть Пентагона, связанная с объектами, указана как цель. Сеть подключена к командно-

коммуникационному центру, используемому президентом и министром обороны, к близлежащему офисному зданию, в котором размещается ряд агентств Пентагона, и к коммунальному предприятию на территории кампуса. Исследователи также должны будут исследовать слабые места в отдельных коридорах Пентагона, подвале и мезонине.

Как следует из списка, к сети FCRS подключены как операционные технологии, так и операционные технологии.

Баунти-программа продлится не более 72 часов, физически хакеры будут находиться в кампусе Пентагона.

За последнее десятилетие вознаграждение за обнаружение ошибок стало мейнстримом, особенно после того, как крупные технологические компании, включая Google, Facebook и Microsoft, создали программы для приема незапрошенных отчетов от сторонних исследователей.

В сентябре 2020 года Агентство по кибербезопасности и безопасности инфраструктуры приказало большинству агентств и департаментов исполнительной власти создать свои собственные программы раскрытия информации об уязвимостях.

В апреле 2020 года Центр киберпреступности Министерства обороны США и Агентство оборонной контрразведки и безопасности запустили 12-месячную программу раскрытия информации об уязвимостях оборонной промышленной базы для сторонних фирм и компаний, входящих в сектор оборонной промышленной базы и работающих с Пентагоном. технологии и исследования.

Подразделения вооруженных сил США также запустили свои собственные программы раскрытия уязвимостей. Программа 2018 года, запущенная BBC, выявила 120 уязвимостей и выплатила 130 000 долларов хакерам, которые их выявили.

Ранее, в 2021 году, армия запустила свою третью программу «Взломай армию» совместно с Defense Digital Service и HackerOne». ***(Prajeet Nair. 'Hack the Pentagon' Hackers Will Literally Hack the Pentagon // Information Security Media Group, Corp. (https://www.govinfosecurity.com/hack-pentagon-hackers-will-literally-hack-pentagon-a-20956). 17.01.2023).***

***

«…Уязвимость высокой степени серьезности, исправленная Google Chrome несколько месяцев назад, позволила хакерам украсть конфиденциальные файлы, такие как криптокошельки.

Уязвимости в проекте веб-браузера Chromium затрагивают миллиарды людей по всему миру, поскольку Chromium является основой доминирующего веб-браузера Google Chrome и лежит в основе браузеров Microsoft Edge и Opera. В совокупности на технологию Chromium приходится более 70% глобальной доли веб-браузеров, говорится в сообщении фирмы по кибербезопасности Imperva в блоге с подробным описанием ошибки, которая отслеживается как CVE-2022-3656.

Исследователь Imperva Рон Масас говорит, что обнаружил уязвимость, изучая, как браузеры Chromium обрабатывают файловые системы. Компания сообщила об ошибке Google и отложила публичное раскрытие до тех пор, пока

Google не исправит ее. Масас говорит, что Google потребовалось две попытки, чтобы исправить ошибку, и Chrome 108, наконец, исправил ошибку в конце ноября.

Недостаток связан с тем, как Chromium анализирует символические ссылки. Также известные как символические ссылки, это файлы, которые указывают путь к указанному файлу или каталогу. «Браузер не проверил должным образом, указывает ли символическая ссылка на место, которое не должно было быть доступным, что позволило украсть конфиденциальные файлы», — написал Масас.

Браузеры Chromium обычно имеют функции безопасности, гарантирующие, что пользователи действительно намерены загружать файлы, когда другие приложения обращаются к API для загрузки файлов, но это не относится к обработке символических ссылок.

Злоумышленники могут воспользоваться этим, заставив пользователей загрузить файл, содержащий символическую ссылку, которая представляет собой путь к файлу с конфиденциальными данными.

В случае использования, описанном Масасом, служба криптокошелька контролируется злоумышленниками, которые заставляют пользователей загружать свои ключи восстановления. Этот сценарий не является надуманным: многие криптокошельки требуют, чтобы пользователи загружали ключи восстановления. Результатом будут украденные файлы из систем пользователей.

Масас пишет о возможности использования уязвимости для кражи криптовалюты, поскольку «хакеры все чаще нацеливаются на отдельных лиц и организации, владеющие криптовалютами, поскольку эти цифровые активы могут быть очень ценными». Мораль этой истории, добавил он, такова: всегда обновляйте программное обеспечение». ***(Mihir Bagwe. Patched Chromium Vulnerability Allowed File Theft // Information Security Media Group, Corp. (https://www.govinfosecurity.com/patched-chromium-vulnerability-allowed-file-theft-a-20931). 13.01.2023).***

***

«Первый ежемесячный дамп патчей Microsoft в этом году включает в себя исправление активно используемой уязвимости нулевого дня, которая позволяет локальному злоумышленнику получить полные системные привилегии.

Уязвимость, отслеживаемая как CVE-2023-21674, представляет собой уязвимость повышения привилегий, затрагивающую широкий спектр версий Windows. Он использует механизм межпроцессного взаимодействия, используемый компонентами операционной системы, называемый расширенными локальными вызовами процедур, и может привести к выходу из песочницы браузера.

«Ошибки этого типа часто сочетаются с какой-либо формой сбора кода для доставки вредоносного ПО или программ-вымогателей. Учитывая, что об этом сообщили Microsoft исследователи из Avast, такой сценарий кажется здесь вероятным», — сказал Дастин Чайлдс, аналитик по безопасности в Zero Day Initiative, инициатива по уязвимости программного обеспечения, проводимая фирмой по кибербезопасности Trend Micro. Исследователи безопасности Ян

Войтешек, Миланек и Пшемек Гмерек из антивирусного поставщика Avast обнаружили уязвимость.

Исправление поставляется вместе с исправлениями для 98 других уязвимостей, в том числе 11, классифицированных как критические, и 87 как важные.

Адам Барнетт, ведущий инженер-программист Rapid7, сказал, что уязвимость требует мониторинга, учитывая ее низкую сложность атаки, наличие функционального кода для проверки концепции и возможность выхода из песочницы.

«Нулевой день ALPC в 2018 году быстро нашел свое применение в кампании вредоносных программ», — сказал Барнетт.

Другие уязвимости

Microsoft также устранила уязвимость обхода функции безопасности сервера SharePoint, отслеживаемую как CVE-2023-21743.

Процесс исправления требует дополнительных действий администратора после установки обновления для системы безопасности SharePoint Server. Чайлдс предупреждает, что администраторы также должны инициировать действие обновления SharePoint, включенное в обновление.

Еще одной ключевой уязвимостью, которая была устранена, является повышение прав блока сообщений Windows Server, отслеживаемое как CVE-2023-21549.

«Чтобы воспользоваться этой уязвимостью, злоумышленник может запустить специально созданный вредоносный сценарий, который выполняет вызов RPC к хосту RPC. Это может привести к повышению привилегий на сервере», — говорится в сообщении Microsoft. «Злоумышленник, успешно воспользовавшийся этой уязвимостью, может выполнять функции RPC, доступные только для привилегированных учетных записей».

Microsoft исправила две уязвимости Microsoft Exchange, отслеживаемые как CVE-2023-21763 и CVE-2023-21764. Уязвимость Microsoft Exchange Server, связанная с повышением привилегий, была обнаружена исследователем ZDI Петром Базыдло в результате неудачного исправления CVE-2022-41123.

Две другие исправленные уязвимости, связанные с удаленным выполнением кода Office, отслеживаются как CVE-2023-21734 и CVE-2023-21735. Пользователь должен быть обманут, чтобы запустить вредоносные файлы.

«К сожалению, обновление безопасности для Microsoft Office 2019 для Mac и Microsoft Office LTSC для Mac 2021 недоступно сразу, поэтому администраторам с затронутыми активами необходимо будет проверить позже, а пока полагаться на другие средства защиты», — говорит Барнетт». ***(Prajeet Nair. Microsoft's First 2023 Patch Tuesday Fixes 0-Day, 98 Vulns // Information Security Media Group, Corp. (https://www.govinfosecurity.com/microsofts-first-2023-patch-tuesday-fixes-0-day-98-vulns-a-20906). 11.01.2023).***

***

«Исследователи обнаружили тысячи серверов Citrix, уязвимых для двух критических недостатков, один из которых активно используется хакерами из

национальных государств. Netgear также предупредила своих клиентов об уязвимости отказа в обслуживании, затрагивающей некоторые из ее устройств.

Обе компании призвали своих клиентов как можно скорее обновить свои устройства до последней версии прошивки.

Две уязвимости в серверах Citrix, отслеживаемые как CVE-2022-27510 и CVE-2022-27518, затрагивают Citrix ADC и Citrix Gateway, облачные решения компании для сетевого трафика и контроля доступа.

Хотя компания выпустила исправления для обеих уязвимостей и попросила своих пользователей установить последние обновления, недавний анализ, проведенный исследователями Fox-IT, показал, что тысячи серверов по-прежнему уязвимы для этих уязвимостей.

К ним относятся около 500 устройств, уязвимых как для недостатков безопасности, так и около 4000 встроенных устройств версий 12.1-65.21, уязвимых для CVE-2022-27518, в Германии, Великобритании и Нидерландах. На США приходится наибольшее количество непропатченных устройств.

Недостатки серверов Citrix

В то время как первая уязвимость допускает несанкционированный доступ при эксплуатации, вторая позволяет удаленно выполнять произвольный код для получения несанкционированного доступа к системе. Китайские хакеры уже используют его для получения несанкционированного доступа к уязвимым устройствам, как предупредило Агентство национальной безопасности США в декабрьском предупреждении (см.: Китайские хакеры используют уязвимости Citrix).

По данным АНБ, китайские хакеры изменяют законные двоичные файлы в Citrix ADC, которые необходимы для запуска приложения. Поэтому агентство рекомендовало пользователям Citrix проверять наличие злонамеренных действий с ключевыми двоичными файлами, такими как nsppe, nsaaad, и nsconf, добавив, что любое изменение этих кодов должно быть немедленно расследовано .nsreadfilensconmsg

Агентство также рекомендовало Citrix ADC проводить поведенческие проверки для выявления необычной активности учетной записи пользователя или несанкционированного изменения разрешений пользователя. Если кто-либо из пользователей Citrix ADC обнаружил такую активность, АНБ рекомендовало пользователям переместить устройство за VPN или аналогичные приложения, требующие многофакторной аутентификации перед предоставлением доступа, или изолировать уязвимую систему, чтобы сдержать распространение вредоносного ПО.

Недостатки устройств Netgear

Компания по производству сетевого оборудования Netgear еще не раскрыла информацию о том, какой компонент затронут, но компания заявила, что уязвимость позволяет злоумышленнику создать переполнение буфера на устройстве, вызывая отказ в обслуживании.

Затронутые устройства включают модели Wireless AX Router Nighthawk RAX75 и RAX80; Беспроводные маршрутизаторы переменного тока Nighthawk

R7000, R7000P, R7960P и R8000P; и другие беспроводные маршрутизаторы переменного тока.

Уязвимость отслеживается как PSV-2019-0104 и имеет оценку CVSS 7,5.

«Уязвимость переполнения буфера перед аутентификацией остается, если вы не выполните все рекомендуемые шаги, и NETGEAR не несет ответственности за какие-либо последствия, которых можно было бы избежать», — заявили в компании.

Предыдущие недостатки Netgear

В прошлом году Netgear исправила три критические уязвимости, затрагивающие несколько интеллектуальных коммутаторов, которые в случае использования дают злоумышленнику полный контроль над скомпрометированным устройством. Netgear выпустила бюллетень по безопасности, подтверждающий выпуск исправлений для 20 продуктов Netgear, затронутых этими уязвимостями.

Джинвал Колдвинд, исследователь безопасности из группы безопасности Google, определил критические уязвимости и сообщил о них в Netgear.

CVE для этих уязвимостей еще не назначены, но Coldwind называет три уязвимости Demon's Cries — оценка CVSS: 9,8, Draconian Fear — оценка CVSS: 7,8 и еще не опубликованное Seventh Inferno…» ***(Prajeet Nair. Flaws in Citrix Servers; Netgear Issues Critical Advisory // Information Security Media Group, Corp. (https://www.govinfosecurity.com/flaws-in-citrix-servers-netgear-issues-critical-advisory-a-20838). 02.01.2023).***

***

«Ваш будинок або офіс можуть залишитися без охорони та відеоспостереження, якщо пристрої працюють через Wi-Fi.

Кіберзлочинці можуть надсилати спеціальний запит на будь-який видимий в «ефірі» Wi-Fi-пристрій і так знеструмити його, пише видання NewScientist. До того ж для цього не потрібно якихось хакерських навичок — пристрої прямо із заводу мають вразливість.

Справа в тому, що всі бездротові гаджети з увімкненим Wi-Fi можуть розпізнавати один одного навіть якщо вони не пов'язані між собою в одній мережі. За допомогою нехитрого пристрою вартістю всього $10 зловмисник може постійно посилати фейкові запити на підключення, а пристрій-жертва йому відповідатиме. Навіть якщо це буде повідомлення на відмову підключення (адже пароль зашифрований і невідомий хакеру), велика кількість фейкових запитів витрачає ресурси батареї гаджета, адже він не може піти в режим сну.

Експерти з безпеки кажуть, що, хоча на перший погляд ця здатність здається невинною, її можна використовувати для відключення камер відеоспостереження або в межах скоординованої атаки з іншими вразливостями. Адже злочинці можуть розрядити автономні камери, оснащені Wi-Fi, і об'єкт, що охороняється, залишиться без захисту.

Фейкові запити можна використовувати для відстеження потрібного пристрою в радіусі до двохсот метрів. Наприклад, постійні запити отримують

постійну відповідь, і зловмиснику стає відоме місце розташування гаджета в просторі та куди його власник рухається.

Дивно, але експерти протестували більше п'яти тисяч різноманітних гаджетів із Wi-Fi, і всі вони схильні до подібної вразливості. Джейк Мур із компанії з кібербезпеки ESET каже, що сьогодні неможливо передбачити, як можуть діяти хакери, використовуючи подібну вразливість, адже їхній творчий потенціал просто нескінченний.

Раніше Фокус писав, що ШІ навчився писати віруси, і хакери отримали у свої руки новий інструмент для атак». ***(Хакери навчилися розряджати батареї гаджетів через Wi-Fi: як це можливо // ФОКУС (https://focus.ua/uk/digital/544689-hakery-nauchilis-razryazhat-batarei-gadzhetov-cherez-wi-fi). 10.01.2023).***

***

«Министерство обороны планирует третью итерацию своей программы «Взломать Пентагон» с упором на выявление уязвимостей в операционных технологиях, обеспечивающих работу культового здания и территории.

Министерство обороны запустило программу Hack the Pentagon в 2016 году, а поставщик HackerOne координировал программу вознаграждения за обнаружение ошибок на общедоступных веб-сайтах министерства. Более 1400 хакеров присоединились к первому раунду, обнаружив 138 уникальных уязвимостей и получив вознаграждение в размере 75 000 долларов.

В 2018 году программа была расширена за счет включения еще двух поставщиков: Synack и Bugcrowd.

В проекте запроса, опубликованном в пятницу, Министерство обороны США объявило о планах третьего запуска и изложило ожидания поставщиков, которые будут управлять программой.

В рамках Hack the Pentagon 3.0 Служба штаб-квартиры в Вашингтоне, которая управляет ресурсами бэк-офиса для Пентагона и частей Министерства обороны, хочет высвободить белых хакеров в сети Facility Related Controls System, или FRCS. Сеть используется для управления механическими операциями в резервации Пентагона, такими как отопление и кондиционирование воздуха в главном здании, отопительно-холодильной установке Пентагона, модульном офисном комплексе и парковке, среди прочего.

«Общая цель состоит в том, чтобы получить поддержку от пула инновационных исследователей в области информационной безопасности посредством краудсорсинга для обнаружения уязвимостей, координации и раскрытия информации, а также для оценки текущего состояния кибербезопасности сети FRCS, выявления слабых мест и уязвимостей и предоставления рекомендаций по улучшению и усилению. общее состояние безопасности», — говорится в черновом рабочем заявлении о производительности.

В проекте документа отмечается, что хакерам будет предоставлен доступ только к незасекреченным ИТ- и ОТ-системам.

Поскольку третья фаза программы будет сосредоточена на операционных технологиях, фактический взлом будет происходить лично во время «этапа испытания», который продлится не более 72 часов.

В то время как программа «Взломать Пентагон» технически предназначена для подключения к большим сообществам с открытым исходным кодом, деликатный характер операций Министерства обороны означает, что когорта должна быть ограничена «частным сообществом квалифицированных и надежных исследователей, которое может быть ограничено гражданами США. только с критериями приемлемости, установленными Министерством обороны США», — говорится в PWS.

Поставщики-победители смогут собрать и организовать такое сообщество, а также предоставить хакерам платформу для безопасного исследования и документирования любых найденных уязвимостей…» ***(Aaron Boyd. Hackers to Get a Crack at Systems Running the Pentagon in New Bug Bounty // Nextgov (https://www.nextgov.com/cybersecurity/2023/01/hackers-get-crack-systems-running-pentagon-new-bug-bounty/381806/). 13.01.2023).***

***

«Исследователи кибербезопасности из команды Horizon3 Attack Team объявили о планах выпустить экспериментальный эксплойт (PoC) для критической уязвимости, обнаруженной в ряде продуктов VMware.

Выпуск PoC означает, что киберпреступники получат простое объяснение того, как использовать уязвимость, что может привести к значительному увеличению числа успешных взломов.

Рассматриваемая уязвимость отслеживается как CVE-2022-47966, уязвимость, которая позволяет злоумышленникам удаленно выполнять код на серверах ManageEngine, на которых в какой-то момент в прошлом была включена система единого входа (SSO) на основе SAML (т. отключение функции ничего не решит). По словам исследователей, уязвимые конечные точки используют устаревшую стороннюю зависимость под названием Apache Santuario, добавив, что злоумышленникам не нужно проходить аутентификацию для удаленного запуска кода.

Распылите и помолитесь

«Эту уязвимость легко использовать, и она является хорошим кандидатом для того, чтобы злоумышленники «распыляли и молились» через Интернет. Эта уязвимость позволяет удаленно выполнять код как NT AUTHORITY\SYSTEM, по сути, предоставляя злоумышленнику полный контроль над системой», — предупредили исследователи.

«Если пользователь определяет, что он был скомпрометирован, требуется дополнительное расследование для определения любого ущерба, нанесенного злоумышленником. Как только злоумышленник получит доступ на уровне SYSTEM к конечной точке, злоумышленники, вероятно, начнут сбрасывать учетные данные через LSASS или использовать существующие общедоступные инструменты для доступа. сохраненные учетные данные приложения для выполнения бокового перемещения».

Хотя почти все продукты ManageEngine уязвимы для этой уязвимости, материнская компания Zoho, как сообщается, уже выпустила исправление.

Используя Shodan для поиска неисправленных конечных точек, исследователи обнаружили «тысячи» уязвимых продуктов ManageEngine, экземпляры ServiceDesk Plus и Endpoint Central.

На данный момент нет никаких сообщений о том, что CVE-2022-47966 эксплуатируется в дикой природе, но если ИТ-администраторы вовремя не исправят уязвимость, мы можем ожидать, что такие сообщения начнут поступать раньше, чем позже». ***(Sead Fadilpašić. These VMware products can remotely execute code, so update now // Future US, Inc. (https://www.techradar.com/news/these-vmware-products-can-remotely-execute-code-so-update-now). 17.01.2023).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Растущая империя: выручка Microsoft от систем безопасности выросла на 33% с 2021 года и на 100% с 2020 года

Хотя чистая прибыль в прошлом квартале снизилась, рост бизнеса Microsoft в области кибербезопасности не разочаровал. Microsoft, крупнейший в мире поставщик средств кибербезопасности, продолжает отставать от конкурентов. В 2022 году его продажи систем безопасности превысили 20 миллиардов долларов после годового роста на 33%.

Гигант облачных вычислений и программного обеспечения из Сиэтла достиг рубежа в 20 миллиардов долларов всего через 12 месяцев после достижения 15 миллиардов долларов дохода от безопасности и через два года после раскрытия 10 миллиардов долларов годовых продаж систем безопасности, согласно отчету о прибылях и убытках во вторник. Увеличение бизнеса Microsoft в области безопасности на 5 миллиардов долларов в 2022 году больше, чем доход, полученный любым поставщиком кибербезопасности, за исключением Palo Alto Networks, который, как ожидается, достигнет 6,85 миллиарда долларов.

«Мы получаем долю во всех основных категориях, которые мы обслуживаем», — сообщил инвесторам во вторник председатель и главный исполнительный директор Сатья Наделла. «Клиенты объединяются в нашем стеке безопасности, чтобы снизить риск, сложность и стоимость».

«Это место, где клиенты могут сэкономить деньги»

Наделла рекламировал широту портфеля средств безопасности, заявив, что Microsoft — единственный поставщик, который имеет интегрированные инструменты, охватывающие идентификацию, безопасность, соответствие требованиям, управление устройствами и конфиденциальность. По словам Наделлы, количество клиентов с четырьмя и более рабочими нагрузками в Microsoft увеличилось более чем на 40% за последний год.

Генеральный директор призвал британского спортивного ритейлера Frasers Group стоимостью 4,46 миллиарда долларов за его решение объединить инструменты и услуги от 10 отдельных поставщиков кибербезопасности только в Microsoft.

По словам Наделла, американский производитель цифровых медиаплееров стоимостью 2,76 миллиарда долларов Roku перенес свой бизнес по управлению идентификацией и доступом в облако с помощью Azure Active Directory. По данным IDC, Microsoft контролирует 23,8% рынка управления идентификацией и доступом стоимостью 13,6 млрд долларов, а Okta занимает второе место с долей рынка всего 9,2%.

По словам Наделла, интегрированные возможности XDR и SIEM в Microsoft Sentinel убедили японского фармацевтического гиганта Astellas Pharma стоимостью 11,61 млрд долларов, испанской транспортной компании Ferrovial стоимостью 8,5 млрд долларов и Университета Торонто зарегистрироваться в качестве клиентов. В октябре Microsoft перепрыгнула на вершину магического квадранта SIEM Gartner, опередив IBM, Splunk, Securonix и Exabeam (см.: Microsoft, IBM, Splunk Dominate SIEM Gartner Magic Quadrant).

IDC обнаружила, что в области безопасности корпоративных конечных точек Microsoft захватила 11,2% рынка в 2021 году после роста выручки на 81,7% с 635,8 млн долларов в 2020 году до 1,16 млрд долларов в 2021 году. Только у CrowdStrike была большая доля рынка безопасности конечных точек — 12,6%, но темпы роста были немного меньше — 67,9%. CrowdStrike, Microsoft и Trend Micro возглавили апрельский Forrester Wave для поставщиков EDR.

Большая часть ценности, которую Microsoft может предоставить клиентам, заключается в таких пакетах, как Microsoft 365 E5, которые сочетают в себе расширенную безопасность и соответствие требованиям с голосовой связью и аналитикой. Среди недавних клиентов, готовых вложиться в лицензии E5, — шведский ритейлер Ikea стоимостью 45,6 млрд долларов, японская телекоммуникационная компания NTT Communications, англо-австралийская горнодобывающая компания Rio Tinto стоимостью 63,5 млрд долларов и правительство штата Вирджиния.

«Мы видели четыре или пять действительно успешных кварталов внедрения E5. Ценность для клиентов в этой среде просто очень высока», — заявила инвесторам во вторник исполнительный вице-президент и финансовый директор Microsoft Эми Худ. «Это место, где клиенты могут сэкономить деньги, переехав в этот люкс».

По словам Худа, количество корпоративных мобильных и безопасных установок Microsoft увеличилось на 16% до более чем 241 миллиарда рабочих мест в расчете на пользователя, но экономический спад повлиял на рост нового бизнеса.

Общий доход на несколько дюймов выше, прибыль падает

Категория	Квартал закончился 31 декабря 2022 г.	Квартал закончился 31 декабря 2021 г.	% Изменение
Общий доход	52,7 млрд долларов	51,7 млрд долларов	2%
Интеллектуальный облачный доход	21,5 млрд долларов	18,3 млрд долларов	17,8%
Производительность и доход от бизнес-процессов	17 млрд долларов	15,9 млрд долларов	6,7%
Больше доходов от персональных компьютеров	14,2 млрд долларов	17,5 млрд долларов	-18,8%
Чистая прибыль	16,4 млрд долларов	18,8 млрд долларов	-12,5%
Прибыль на разводненную акцию	2,20 доллара США	2,48 доллара США	-11,3%
Чистая прибыль не по GAAP	17,4 млрд долларов	Не разглашается	-7%
Прибыль на акцию без учета GAAP	2,32 доллара США	Не разглашается	-6%

Источник: Майкрософт

Выручка Microsoft в размере 52,7 млрд долларов за квартал, закончившийся 31 декабря, ниже оценки продаж Seeking Alpha в 53,15 млрд долларов. Между тем, прибыль компании не по GAAP в размере 2,32 доллара на акцию превзошла оценку Seeking Alpha без GAAP в 2,31 доллара на акцию.

Акции компании упали на 2,44 доллара, или 1,01%, до 239,60 доллара за акцию в нерабочее время во вторник. Это самая низкая цена акций Microsoft с пятницы.

Неделю назад Наделла поделился планами уволить 10 000 сотрудников до конца третьего квартала 23 финансового года в сообщении для сотрудников Microsoft. Сокращения представляют чуть менее 5% рабочей силы компании. Он сказал сотрудникам, что клиенты хотят «делать больше с меньшими затратами» в эти кризисные времена, а увольнения помогут Microsoft «привести нашу структуру затрат в соответствие с нашими доходами и тем, где мы видим потребительский спрос». ***(Michael Novinson. Microsoft Security Sales Hit $20B as Consolidation***

Increases // Information Security Media Group, Corp. (https://www.govinfosecurity.com/microsoft-security-sales-hit-20b-as-consolidation-increases-a-21015). 24.01.2023).

***

«Первое в истории слияние и поглощение Forter не позволит вредоносным ботам покупать товары ограниченного выпуска

Forter купил стартап по обнаружению ботов, основанный давним лидером Check Point Software, чтобы помешать злоумышленникам покупать предметы и предметы коллекционирования, выпущенные ограниченным тиражом.

По словам соучредителя и генерального директора Forter Майкла Райтблата, поставщик средств защиты от мошенничества из Нью-Йорка заявляет, что его приобретение израильской компании Immue в Тель-Авиве предотвратит наводнение сайтов электронной коммерции вредоносными ботами с тысячами попыток транзакций в секунду. Объем запросов от вредоносных ботов часто не позволяет законным людям делать ставки или покупать редкие предметы до того, как они будут распроданы.

«Мы хотели, чтобы Immue разработала вещи, характерные для работы нашей платформы», — говорит Рейтблат в интервью Information Security Media Group. «Мы действительно считаем, что их технология уникальна, и мы хотели владеть ею, чтобы продолжать расширять наше конкурентное преимущество на рынке и убедиться, что мы можем подключить ее так, как это лучше всего подходит для нашего решения».

Условия сделки, закрытой в начале января, не разглашаются, и все шесть членов технической команды Immue присоединились к Forter. Шира Ицхаки основала Immue в 2021 году, проработав 13 лет в Check Point, и в будущем сосредоточится на руководстве портфелем продуктов для обнаружения ботов в Immue и разработке технических аспектов продукта для ботов. Это первое приобретение за 11-летнюю историю Forter.

«Другой тип мышления и опыта»

Опыт Forter связан с определением того, являются ли люди, пытающиеся осуществить транзакции электронной коммерции, законными или мошенническими, и технология, разработанная Forter, имеет тенденцию думать о ботах как о людях. Но боты ведут себя совершенно иначе, чем люди, пытаясь совершать тысячи транзакций в секунду, а не от 10 до 50 транзакций, которые может предпринять человек-мошенник.

По словам Рейтблата, Immue отлично справляется с обнаружением нюансов того, как сложные боты создают виртуальные машины для манипулирования сеансами, манипулирования устройствами, местоположения и регулирования. Многие формулировки предотвращения мошенничества могут показаться похожими на формулировки, которые используют компании по обнаружению ботов, но Рейтблат говорит, что нюансы работы ботов сильно отличаются.

«Боты обычно встречаются в киберорганизациях, тогда как в сфере мошенничества это другой тип мышления и опыта», — говорит Рейтблат. «Мы

искали кого-то, кто знает и обладает этим опытом, и это одна из причин, по которой мы очень рады, что вся команда Immue присоединится к нам».

Reitblat ожидает, что к концу февраля возможности Immue будут полностью встроены в продукт Forter, а впоследствии он начнет развертывание расширенного продукта для клиентов Forter. Технология Immue позволит клиентам Forter быстрее и точнее обнаруживать как вредоносных, так и доброжелательных ботов и использовать их непроходимую и не поддающуюся взлому CAPTCHA, когда требуется пошаговая проверка.

Как отличить хороших ботов от плохих

Рейтблат говорит, что за последние 18 месяцев боты все чаще использовались в законных целях для оказания помощи в поездках и покупках, например, когда Alexa совершала покупку на Amazon от имени пользователя. Рейтблат говорит, что по мере того, как активность ботов становится законной, злоумышленникам стало легче маскировать свою деятельность и совершать покупки с помощью украденных кредитных карт, поддельных учетных записей или блокировки инвентаря.

Рейтблат говорит, что Immue усложняет продвинутым ботам процесс прохождения и совершения покупок, добавляя трения во время процесса CAPTCHA и удаляя как можно больше трафика ботов, прежде чем они смогут зарегистрировать учетную запись или инициировать транзакцию. По словам Рейтблата, клиентами Forter являются крупные платформы электронной коммерции и розничные продавцы, включая Nordstrom, Priceline, Sephora, Adobe, Instacart, Asics и ASOS.

Рейтблат говорит, что с точки зрения показателей он планирует внимательно следить за качеством, эффективностью и потреблением продукта Immue. По словам Рейтблата, Forter будет следить за точностью Immue в блокировании атак ботов, не блокируя при этом людей, заинтересованных в совершении законных покупок, а также за тем, в какой степени клиенты Forter, заявившие, что им нужна технология Immue, действительно покупают продукт.

«Если вы такой же хороший потребитель, я хочу вас немедленно пропустить», — говорит Рейтблат. «Но если вы мошенник, у которого есть имя, адрес электронной почты, адрес и местоположение IP законного пользователя, но я знаю, что это не вы, я вообще не хочу вас пропускать. И это здесь, я думаю, помогут некоторые новые возможности Immue». ***(Michael Novinson. Forter Acquires Startup Immue to Spot Malicious Bots Earlier // Information Security Media Group, Corp. (https://www.govinfosecurity.com/forter-acquires-startup-immue-to-spot-malicious-bots-earlier-a-20962). 18.01.2023).***

***

«После двух сенсационных лет на публичных рынках в разгар пандемии COVID-19 2022 год стал грубым пробуждением для индустрии кибербезопасности.

Четырехголовый монстр растущей инфляции, повышения процентных ставок, перебоев в цепочках поставок и продолжающейся российско-украинской войны сказался на продавцах ценных бумаг, и среди 32 публичных компаний, получающих большие доходы, средний курс акций упал на 40%. своих доходов от

кибербезопасности. Это намного круче, чем падение на 20%, 13% и 9%, зафиксированное S&P, Nasdaq и Dow Jones соответственно.

Устоявшиеся компании с большим опытом работы на публичных рынках, широким портфелем технологий и четким путем к прибыльности добились наилучших результатов, поскольку в 2022 году инвесторы приняли более консервативные ставки на акции. И наоборот, любимцы IPO последних лет с лучшими в своем классе возможностями в конкретной технологической области и высокие темпы роста, выражающиеся двузначными или трехзначными числами, привели к тому, что их состояния изменились, поскольку прибыльность заняла центральное место.

Ниже мы рассмотрим, как каждый из публично торгуемых поставщиков средств кибербезопасности справился с ситуацией в 2022 году, а также подробно рассмотрим некоторые из наиболее интересных тематических исследований.

Компания	Оценка	30 декабря 2022 г., Закрытие	3 января 2022 г., открытие	Изменение
Программное обеспечение Check Point	15,82 млрд долларов	$126,16	115,95 долларов США	8,8%
KnowBe4	5,53 млрд долларов	24,78 доллара США	23,21 доллара США	6,8%

Источник: Yahoo Финансы

Самая прибыльная компания в области кибербезопасности была наиболее щедро вознаграждена Уолл-стрит в 2022 году. Check Point была единственным поставщиком средств безопасности, который повысил цену своих акций, не продав их частной инвестиционной компании, благодаря колоссальной чистой прибыли в размере 527 миллионов долларов за сентябрь. Check Point ожидает самого высокого роста продаж за многие годы благодаря двузначному увеличению количества продуктов и подписок на безопасность.

Инвесторы вздохнули с облегчением, когда Vista Equity Partners согласилась купить KnowBe4 за 4,6 миллиарда долларов в октябре, всего через 18 месяцев после того, как компания, занимающаяся обучением по вопросам безопасности, стала публичной. Несмотря на то, что KnowBe4 зафиксировала прибыль в размере 11,2 млн долларов за сентябрь и рассчитывает увеличить продажи на 35% в 2022 году, цена акций фирмы упала более чем на 25% в прошлом году, прежде чем Vista заявила о своей заинтересованности в покупке KnowBe4.

Как избежать тяжелого удара

Компания	Оценка	30 декабря 2022 г., Закрытие	3 января 2022 г., открытие	Изменение
F-Secure	517 млн долларов США	$3,02	$3,18	-5%
ForgeRock	1,94 млрд долларов США	$22,77	$26,50	-14%
Trend Micro	6,57 млрд долларов США	$46,25	$55,70	-17%
Gen Digital	13,96 млрд долларов США	$21,43	$25,92	-17,3%
Qualys	4,26 млрд долларов США	$112,23	$137,55	-18,4%
Blancco	161 млн долларов США	$212,93	$280,48	-24,1%
Palo Alto Networks	42,19 млрд долларов США	$139,54	$186,15	-25%
CyberArk	5,28 млрд долларов США	$129,65	$173,74 $	-25,4%
Splunk	14,09 млрд долларов США	$86,49	$116,09	-25,5%
Akamai	13,26 млрд долларов США	$84,30	$117,17	-28,1%
Tenable	4,29 млрд долларов США	$38,15	$55,12	-30,8%
Fortinet	38,2 млрд долларов США	$48,89	$72,42	-32,5%
OneSpan	444 млн долларов США	$11,19	$16,99	-34,1%

Источник: Yahoo Финансы

У ForgeRock дела обстоят лучше, чем у большинства конкурентов, благодаря тому, что в октябре Thoma Bravo согласилась купить плеер для идентификации за 2,3 миллиарда долларов. Акции ForgeRock упали почти на 43% в 2022 году до предложения Thoma Bravo из-за более длительных циклов продаж, вынудивших компанию снизить прогнозы доходов. Министерство юстиции расследует сделку

Thoma Bravo-ForgeRock в связи с более ранними покупками Thoma SailPoint и Ping Identity.

Широта и масштаб Trend Micro позволили фирме обеспечить прибыльный рост, несмотря на экономические препятствия. Продажи выросли на 16,5%, а чистая прибыль за сентябрь подскочила до 217,6 млн долларов. Trend Micro — одна из двух компаний, признанных Gartner лидером как в EDR, так и в XDR, и фирма планирует использовать больше возможностей на рынках правительства США и критической инфраструктуры.

Gen Digital была образована в результате слияния гигантов потребительской кибербезопасности NortonLifeLock и Avast стоимостью 8,6 млрд долларов и предлагает экспертные знания в области безопасности, конфиденциальности и идентификации. Фирма стоимостью 3,5 миллиарда долларов имеет 500 миллионов пользователей и планирует добиться синергии затрат в размере 280 миллионов долларов, половина из которых будет получена за счет внедрения общих передовых методов, сокращения дублирующих ролей и сокращения числа сотрудников до менее чем 4000 человек.

Palo Alto Networks не смогла плыть против экономического течения, несмотря на то, что является крупнейшим и наиболее ценным поставщиком услуг кибербезопасности в мире. Компания произвела фурор в мае, обещая достичь прибыльности по GAAP в ближайшем будущем, и в ноябре, купив стартап по безопасности приложений Cider Security за 250 миллионов долларов, но инвесторы по-прежнему опасаются проверки со стороны финансового директора и продления циклов продаж.

Бизнес Akamai в области безопасности вырос на 18% в сентябре благодаря агрессивному подходу к слияниям и поглощениям, который включал покупку фирмы Guardicore, занимающейся микросегментацией, за 600 миллионов долларов и фирмы Inverse, занимающейся безопасностью IoT, за 17,1 миллиона долларов. Поставщик интеллектуальной пограничной платформы стал предметом ряда слухов о сделках. В октябре StreetInsider сообщила, что провела переговоры с частной инвестиционной компанией о поглощении.

Последовательное обеспечение прибыльного роста Fortinet было щедро вознаграждено Уолл-стрит в 2020 и 2021 годах, и за это время инвесторы подняли акции компании на 28% и 119% соответственно. Но когда в ноябре 2022 года Fortinet представила прогноз выручки и счетов, который не оправдал ожиданий инвесторов, Уолл-стрит отреагировала быстро, в результате чего на следующий день акции поставщика безопасности упали на 14%.

Середина пакета

Компания	Оценка	30 декабря 2022 г., Закрытие	3 января 2022 г., открытие	Изменение
Darktrace	2,28 млрд долларов США	$312,09	$515,36	-39,4%
Sumo Logic	972 млн долларов США	$8,10	$13,76	-41,1%

CrowdStrike	24,68 млрд долларов США	$105,29	$205	-48,6%
Appgate	857 млн долларов США	$6,50	$13	-50%
Varonis	2,64 млрд долларов США	$23,94	$49,32	-51,5%
Radware	886 млн долларов США	$19,75	$41,50	-52,4%
ZeroFox	589 млн долларов США	$4,79	$10,17	-54,9%
Secureworks	541 млн долларов США	$6,39	$16	-60,1%

Источник: Yahoo Финансы

Инвесторы были раздавлены решением Darktrace прекратить переговоры о приобретении с Thoma Bravo после того, как обе стороны не смогли договориться об условиях, в результате чего акции фирмы упали на 36%. Darktrace стала публичной в апреле 2021 года с оценкой в 2,05 миллиарда долларов, но не смогла завоевать большого внимания инвесторов, несмотря на то, что впервые в истории получила прибыль и увеличила продажи почти на 46% в финансовом году, закончившемся 30 июня.

CrowdStrike сократила свой прогноз продаж в конце ноября из-за более длительного цикла покупки для малого бизнеса и задержки начала подписки для крупных предприятий, что привело к падению акций компании. Компания обнаружила, что для закрытия сделок с клиентами малого и среднего бизнеса в квартале, закончившемся 31 октября, потребовалось на 11% больше времени, и ожидает, что чистая новая ARR снизится на 10% в первой половине 2023 года из-за более пристального внимания к бюджетам.

Единственная компания в области кибербезопасности, которая станет публичной в 2022 году, столкнется с трудной борьбой, поскольку инвесторы переводят свои деньги в более безопасные убежища в более авторитетных компаниях. Внешний поставщик информации об угрозах ZeroFox вышел на фондовую биржу Nasdaq в августе, объединившись с публично торгуемой SPAC с оценкой в 1,4 миллиарда долларов. Но последние месяцы не были благоприятны для компании, и прибыльность ZeroFox упала намного ниже ожиданий.

Падение дальше всех

Компания	Оценка	30 декабря 2022 г., Закрытие	3 января 2022 г., открытие	Изменение
BlackBerry	1,89 млрд долларов США	$3,24	$9,32	-65,2%
Cloudflare	14,86 млрд долларов США	$45,65	$131,07	-65,2%
Zscaler	16,14 млрд долларов США	$111,90	$322,60	-65,3%
Okta	10,95 млрд долларов США	$68,33	$223,05	-69,4%
Rapid7	2,01 млрд долларов США	$33,98	$117,86	-71,2%
SentinelOne	4,12 миллиарда долларов США	$14,59	$52	-71,9%
WithSecure	258 миллионов долларов США	$1,46	$5,40	-72,9%
Cyren	5 миллионов долларов США	$0,62	$6	-89,7%
IronNet	24 миллиона долларов США	$0,25	$4,21	-94,1%

Источник: Yahoo Финансы

Zscaler был одним из самых популярных акций в области кибербезопасности в 2020 и 2021 годах. За этот период инвесторы подняли акции компании на 264% и 42% соответственно. Но летом аналитики снизили свои рейтинги Zscaler из-за опасений относительно более длительного цикла продаж и замедления роста. Задержки были вызваны тем, что клиенты покупали SWG, частный доступ и цифровые продукты компании в комплекте.

Акции Okta резко упали в конце лета после того, как компания признала, что изо всех сил пыталась интегрировать свой отдел продаж с отделом продаж гиганта идентификации клиентов Auth0, что привело к усилению увольнения сотрудников и путанице в отношении совместного портфеля продуктов. Акции поставщика немного восстановились после того, как усилия по репозиционированию его предложения по идентификации клиентов принесли свои плоды, а торговые представители увеличили количество сделок, заключенных с помощью инструмента Auth0.

SentinelOne был зеницей ока Уолл-стрит в 2021 году, когда инвесторы стремились к росту любой ценой. Компания провела крупнейшее IPO в области

кибербезопасности за все время благодаря росту продаж более чем на 100%, несмотря на то, что чистый убыток SentinelOne превысил ее годовой доход. Но поскольку в 2022 году инвесторы отдавали приоритет прибыльности, фирма обратилась к управлению затратами и добилась повышения операционной эффективности и эффективности исполнения.

IronNet пережила резкое падение в 2022 году, через несколько месяцев после того, как компания, возглавляемая генералом Китом Александром, стала публичной с оценкой в 1,2 миллиарда долларов. IronNet уволила половину своих сотрудников в июне и сентябре, уволила со-генерального директора Уильяма Уэлча и расследует обвинения в том, что руководители компании вводили инвесторов в заблуждение относительно прогнозов роста. IronNet 16 декабря заявила, что у нее не хватает средств для оплаты счетов в течение месяца». ***(Michael Novinson. A Few Cybersecurity Stocks Soared in 2022, But Most Stumbled // Information Security Media Group, Corp. (https://www.govinfosecurity.com/blogs/few-cybersecurity-stocks-soared-in-2022-but-most-stumbled-p-3344). 03.01.2023).***

***

«Сквозное шифрование для электронной почты и других облачных сервисов становится все более популярным. Учитывая, что электронная почта является одним из двух основных векторов кибератак, это неудивительно.

Согласно ежегодному отчету Verizon о расследовании нарушений данных за 2022 год, на почтовые серверы приходится 28% всего уязвимого оборудования, а 35% действий программ-вымогателей связаны с электронной почтой. В отчете Агентства ЕС по кибербезопасности за 2022 год отмечается, что на программы-вымогатели приходится 10 терабайт украденных данных в месяц, при этом 60% компаний, вероятно, заплатили выкуп. Исследование Gartner 2021 года, обновленное на 2022 год, показало, что около 40% атак программ-вымогателей начинаются с электронной почты.

Чтобы решить эти проблемы, Google, Microsoft и Proton, чей сервис Proton Mail был первопроходцем в области безопасной электронной почты, перешли к расширению предложений сквозного шифрования.

Новое шифрование электронной почты Google и Microsoft

В сообщении блога в прошлом месяце Google объявил о бета-версии сервисов шифрования на стороне клиента для Gmail в Интернете. Клиенты Google Workspace Enterprise Plus, Education Plus и Education Standard могут подать заявку на участие в бета-тестировании до 20 января 2023 г.

Отметив, что он шифрует все данные в состоянии покоя и при передаче в Google Workspace между своими объектами, Google заявил, что шифрование на стороне клиента «помогает повысить конфиденциальность ваших данных, помогая удовлетворить широкий спектр требований к суверенитету данных и соответствию требованиям».

Согласно Google, шифрование на стороне клиента уже доступно для Google Диска, Google Документов, Таблиц, Google Slides, Google Meet и Google Calendar.

Google объяснил, что для добавления шифрования на стороне клиента к любому сообщению пользователям нужно всего лишь щелкнуть значок замка и выбрать опцию дополнительного шифрования. Составление и добавление вложений происходит в обычном режиме.

Microsoft, которая в последний раз обновляла шифрование сообщений в 2019 году, объявила в апреле прошлого года, что Windows 11 будет получать обновления безопасности в новых выпусках, как сообщается, для устранения как фишинговых, так и вредоносных угроз.

Если это так, Microsoft, скорее всего, также включит сквозное шифрование, поскольку в настоящее время она использует шифрование Transport Layer Security для шифрования сообщений Office 365. Хотя компания объясняет, что эта служба позволяет пользователям шифровать и защищать права сообщений, предназначенных для внутренних и внешних получателей с помощью Office 365, почтовых приложений, отличных от Office 365, и почтовых веб-служб, таких как Gmail.com и Outlook.com, это действительно так. не предотвращать фишинговые или вредоносные атаки так же эффективно, как E2EE.

Новые приложения Proton

Объявление Google последовало за объявлением о Proton, платформе зашифрованного облачного хранилища, запущенной в 2013 году в Женеве, Швейцария, генеральным директором Энди Йеном. Прошлой осенью компания расширила свои предложения по шифрованию, сосредоточив внимание на мобильных устройствах, включая безопасное облачное хранилище и функцию безопасного календаря, с приложениями для устройств iOS и Android.

Протон Драйв

Proton Drive, который стал доступен в конце сентября в виде бесплатного зашифрованного облачного сервиса и был выпущен для iOS и Android в декабре, позволяет пользователям безопасно загружать, сохранять и обмениваться файлами со своего телефона и с него.

По данным компании Proton Drive:

Шифрует любой загружаемый файл на устройстве пользователя перед его сохранением на серверах Proton.

Шифрует метаданные, такие как имена файлов и папок, расширения файлов, размеры файлов и эскизы.

Включает срок действия файла и пароли для просмотра, что позволяет безопасно обмениваться файлами с пользователями, не являющимися пользователями Proton.

Proton заявил, что с момента запуска Proton Drive в сентябре прошлого года, когда в бета-тестировании участвовало более полумиллиона пользователей, ежедневно загружалось в среднем один миллион файлов, примерно половина из которых — фотографии.

Для индивидуальных пользователей Proton предлагает бесплатный уровень своего зашифрованного диска с 1 ГБ облачного хранилища, а также два дополнительных уровня обслуживания по цене: Drive Plus с хранилищем 200 ГБ стоит 4,99 долл. США в месяц или 47,88 долл. США в год, а Proton Unlimited с 500 ГБ — 11,99 долл. США. в месяц или 119,88 долларов в год…

Протонный календарь

Proton запустила приложение «Календарь» для iPhone в декабре после того, как в апреле 2022 года выпустила его для Android и Интернета. По словам Proton, новое приложение:

Интегрируется с Proton Mail, позволяя пользователям управлять приглашениями или добавлять события в календарь, не выходя из папки «Входящие».

Помимо сквозного шифрования, для защиты данных и расписаний используется криптография на основе эллиптических кривых (ECC Curve25519).

Приглашения зашифрованы вслепую, поэтому Proton не знает их личности. Это значительно повышает анонимность участников.

Является открытым исходным кодом, как и веб-приложение, и подвергается независимому аудиту с доступным для проверки кодом…

Представитель сказал, что календарь представляет собой более широкую стратегию создания полноценной экосистемы конфиденциальности.

«Мы наблюдаем огромный спрос на зашифрованные услуги — вот почему более 70 миллионов человек подписались на частные услуги, такие как Proton, и это доказывает, что капитал наблюдения — не единственная бизнес-модель, которая работает в сфере технологий», — сказал представитель.

По словам представителя, компания, которая также предлагает Proton VPN, конкурирующую с AtlasVPN, Nord, Express и HIDEme, имеет двоякое обоснование для создания Proton Calendar: во-первых, поскольку календарь является хранилищем чувствительного времени. и местоположение пользовательских данных, это представляет собой цель угрозы; во-вторых, это часть более крупной стратегии безопасности облачных сервисов Proton.

«Что касается конфиденциальности, Proton на сегодняшний день является наиболее полной экосистемой», — сказал Йен. «Ни у Google, ни у Apple нет ничего столь всеобъемлющего, поскольку их предложения по шифрованию ограничены (например, шифрование электронной почты Google доступно только для бизнес-пользователей)».

Он утверждал, что ключевое отличие от конкурентов заключается в бизнес-модели и деловой практике.

«Proton, как швейцарская компания, не подпадает под действие законов и практики наблюдения США, и, в отличие от Google и Apple, у которых есть надежный рекламный бизнес, единственным бизнесом Proton является конфиденциальность», — сказал он…» ***(Karl Greenberg. Cloud email services bolster encryption against hackers // TechnologyAdvice (https://www.techrepublic.com/article/cloud-email-services-bolster-encryption-against-hackers/amp/). 05.01.2023).***

***

«Розробка китайських вчених, щодо можливості сучасних квантових комп'ютерів зламувати RSA-ключі, поставила під загрозу не лише безпеку криптовалют, але й конфіденційність урядових даних усього світу. Як з'ясувалось, за допомогою квантового комп'ютера та квантового алгоритму Шора можна легко розкласти великі числа на прості множники та розшифрувати ключ або повідомлення. Якщо хакери отримають доступ до технології зламу ключів RSA, сотні тисяч конфіденційних даних опиняться під загрозою.

Алгоритм RSA використовується у криптографії. Він застосовується для шифрування даних на мобільних пристроях, комп'ютерах, у банківській справі. «Це величезна претензія. Це виходить за межі лише однієї сфери. Насправді розвиток такого механізму дешифрування означає, що уряди зможуть красти секрети один у одного. Це може стати проривом у комп'ютерній науці», — поділився своєю точкою зору експерт з безпеки у сфері IT Роджер Граймс.

Про те, що квантові комп'ютери можуть негативно вплинути на безпеку біткоїна, ще у жовтні 2022 року почали говорити експерти біржі LocalBitcoins та Сассекського університету. Тоді японська технологічна компанія Fujitsu анонсувала запуск квантових комп'ютерів, які матимуть набагато більшу потужність, ніж Frontier — найшвидший у світі комп'ютер. Як з'ясували дослідники, майбутні квантові комп'ютери від Fujitsu здатні зламати алгоритм SHA256, з яким працює мережа біткоїна.

«Це просто знищить ринок. За одну секунду. Біткоїн більше не буде безпечним засобом обміну або накопичення. Але, повторюся, це стосується не тільки криптографії. Це буквально все, кожна система, будь-яке сховище — все це під загрозою», — сказав головний операційний директор Halborn Девід Швед.

Достеменно невідомо чи розробки китайських та японських вчених реальні, втім у будь-якому випадку спеціалісти з безпеки мають «в запасі» 10−20 років, поки квантові комп'ютери стануть поширеними, а хакери навчаться зламувати алгоритм SHA256. Наразі IT-спеціалісти працюють над рішеннями, що допоможуть усунути загрозу квантових обчислень. Так, фонд Ethereum розробив схему «квантової стійкості», яка підходить тільки для блокчейну Ethereum». ***(Китайські вчені поставили під загрозу конфіденційність усього світу через квантові комп'ютери // No worries! (https://noworries.news/kytajski-vcheni-postavyly-pid-zagrozu-konfidenczijnist-usogo-svitu-cherez-kvantovi-kompyutery/). 06.01.2023).***

***

«Група китайських вчених навчила сучасні квантові комп'ютери зламувати довгі RSA-ключі. Як повідомили науковці у своїй роботі, за допомогою квантового комп'ютера з 10 надпровідними кубітами їм вдалось здійснити перший в історії злам 48-бітного криптографічного алгоритму з відкритим ключем (RSA). Відповідно, для зламу ключа RSA-2048 потрібно не більше 400 кубітів, що знаходиться в діапазоні можливостей квантового комп'ютера.

Як відомо, за допомогою квантового комп'ютера та квантового алгоритму Шора можна легко розкласти великі числа на прості множники та розшифрувати ключ або повідомлення. Це відбувається набагато швидше, ніж на класичному комп'ютері. Єдина проблема із запуском алгоритму Шора в тому, що для факторизації криптографічно значущих довгих ключів потрібні квантові системи із сотень тисяч, якщо не мільйонів кубітів.

Китайські дослідники заявили, що знайшли можливість зламувати RSA-ключі, використовуючи значно менше надпровідних кубіт. Згідно з розрахунками вчених, для зламу ключа RSA-2048 потрібно всього 372 кубіти. Наразі система RSA використовується для захисту програмного забезпечення й у схемах цифрового підпису. Також вона є у відкритій системі шифрування PGP. Якщо хакери отримають доступ до технології зламу ключів RSA, сотні тисяч конфіденційних даних опиняться під загрозою…». ***(Науковці навчили квантові комп'ютери зламувати криптографічне шифрування // No worries! (https://noworries.news/naukovczi-navchyly-kvantovi-kompyutery-zlamuvaty-kryptografichne-shyfruvannya/). 05.01.2023).***

***

«В конце прошлого месяца группа китайских ученых без лишнего шума опубликовала статью, в которой пыталась показать, как сочетание методов классических и квантовых вычислений, а также достаточно мощный квантовый компьютер могут разрушить современное шифрование. Прорыв — если он реален — поставит под угрозу не только большую часть коммуникаций между военными и разведывательным сообществом США, но и финансовые транзакции и даже ваши текстовые сообщения.

Один эксперт по квантовым технологиям сказал просто: «Если это правда, это довольно катастрофично».

Но прорыв может быть не всем, чем он должен быть.

Статья «Факторизация целых чисел с сублинейными ресурсами на сверхпроводящем квантовом процессоре» в настоящее время находится на рецензировании. Компания утверждает, что нашла способ использовать 372-кубитный квантовый компьютер для факторизации 2048-битных чисел в системе шифрования RSA, используемой учреждениями, от вооруженных сил до банков и разработчиков коммуникационных приложений.

Это очень важно, потому что специалисты по квантовым вычислениям полагали, что для взлома шифрования RSA потребуется квантовый компьютер гораздо большего размера. А у IBM уже есть квантовый процессор на 433 кубита.

Китайские исследователи утверждают, что достигли этого успеха, используя квантовый компьютер для масштабирования классического алгоритма факторизации, разработанного немецким математиком Клаусом Петером Шноором.

«По нашим оценкам, квантовая схема с 372 физическими кубитами и глубиной в тысячи необходима, чтобы бросить вызов RSA-2048 с использованием нашего алгоритма. Наше исследование показывает большие перспективы в ускорении применения современных шумных квантовых компьютеров и

прокладывает путь к факторизации больших целых чисел реалистичной криптографической значимости», — написали они.

Лоуренс Гасман, основатель и президент Inside Quantum Technology, говорит, что он немного скептичен, но «чрезвычайно важно, чтобы некоторые люди на Западе пришли к некоторым реальным выводам по этому поводу, потому что, если это правда, это довольно катастрофично».

Гасман сказал, что наиболее тревожным аспектом статьи является идея о том, что можно взломать протоколы шифрования ключей не с помощью гипотетического будущего квантового компьютера, а относительно простого, который уже может существовать или появится в ближайшее время…

Defense One связалась с несколькими экспертами правительства США, которые отказались комментировать статью. Но профессор компьютерных наук Техасского университета в Остине Скотт Ааронсон был немного резче в своем блоге в начале этого месяца. А именно: «Нет. Просто нет."

Ааронсон писал: «Мне кажется, что потребуется чудо, чтобы этот подход принес хоть какую-то пользу по сравнению с простым запуском классического алгоритма Шнорра на вашем ноутбуке. И если бы последний смог взломать RSA, он бы уже это сделал. В общем, это одна из самых активно вводящих в заблуждение работ по квантовым вычислениям, которые я видел за 25 лет, а я видел… много».

Так является ли газета мошенничеством, «катастрофой» или чем-то средним? Гасман говорит, что, хотя политическая гонка за квантовое превосходство ужесточается, для китайского исследовательского сообщества было бы нехарактерно делать смелые, легко опровергаемые ложные заявления. Он охарактеризовал большинство опубликованных квантовых исследований в Китае как довольно «обычные» и сказал, что маловероятно, что Китай будет рисковать своим статусом лидера в области квантовой науки, продвигая чушь.

«Никто не скажет: «О, это китайцы, и они, знаете ли, лукавят, и все дело в соперничестве с Западом или соперничестве с [Соединенными Штатами]», — сказал он.

Гасман добавил, что в то время как Китай лидирует в некоторых аспектах квантовой науки (таких как потрясающие сети) и квантовой информатики, создав «самый быстрый» квантовый компьютер в мире, Соединенные Штаты лидируют во многих других аспектах.

Даже если эта статья окажется ошибочной, это предупреждение о том, что грядет. Правительство США все больше беспокоит то, как быстро стандарты ключевого шифрования могут устареть перед лицом настоящего квантового прорыва. В мае прошлого года Белый дом поручил федеральным агентствам быстро перейти к квантово-безопасному шифрованию в своей деятельности.

Но даже этого может быть слишком мало, слишком поздно…» ***(Patrick Tucker. Is China About To Destroy Encryption As We Know It? Maybe // Nextov (https://www.nextgov.com/emerging-tech/2023/01/china-about-destroy-encryption-we-know-it-maybe/382070/). 23.01.2023).***

***

«Швейцарские исследователи, частично финансируемые США, разрабатывают более сильные меры противодействия сетевой безопасности для борьбы с потенциалом жизнеспособной системы квантовых вычислений.

Будущее безопасности данных может зависеть от передачи информации в виде зашифрованных частиц света, а новое совместное американо-швейцарское исследование проложит путь квантовым криптографическим устройствам для создания новой схемы кибербезопасности.

Возможная разработка полнофункционального квантового компьютера может сделать текущие методы защиты данных совершенно неэффективными. Финансируемая США исследовательская инициатива в области квантовых технологий направлена на решение этой проблемы путем объединения как классической, так и квантовой технологий для дополнительной защиты цифровых сетей в преддверии появления квантовых вычислений.

Благодаря недавнему двустороннему сотрудничеству США и Швейцарии в области квантовых технологий группа исследователей в Швейцарии работает конкретно над аппаратно-независимой квантовой криптографией — процессом, который позволит стандартным компьютерам сегодня передавать безопасное шифрование с квантово-способным дополнением. на.

Ренато Реннер, профессор теоретической физики и глава исследовательской группы квантовой теории информации в ETH Zürich, является одним из ведущих теоретиков в рамках американо-швейцарского партнерства. Он объяснил Nextgov, что эти устройства призваны вооружить нынешние знакомые вычислительные системы квантовой защитой.

«Мы можем надеяться на лучшие классические схемы, которые настолько хороши, что даже квантовый компьютер не может их взломать. Это постквантовая криптография», — сказал он в недавнем интервью. «Но то, что мы делаем, [является] также использованием квантовой технологии — то есть независимой от устройства квантовой криптографии — [для] защиты от атак квантовых компьютеров [с использованием] самой квантовой технологии».

Поскольку гонка за созданием систем квантовых вычислений, а вместе с ними и способности взломать современное шифрование, представляет угрозу для классических вычислительных систем, обеспечивающих безопасность подавляющего большинства современных цифровых сетей, основная защитная тактика опирается на квантово-устойчивые алгоритмы.

Реннер отмечает, что эти алгоритмы, хотя зачастую и эффективны, никогда не дают гарантии безопасности, поскольку они по-прежнему используют классические вычислительные схемы. Один такой предложенный алгоритм уже был взломан классическим компьютером. Партнерство между США и Швейцарией направлено на устранение этих серьезных угроз безопасности за счет использования квантовых технологий в качестве части своей защиты и устранения возможности будущих атак.

«Для аппаратно-независимой квантовой криптографии вы все еще можете использовать в основном классические устройства, но вам нужно иметь возможность кодировать информацию в легкие частицы», — сказал он. «Итак, вам

нужно некоторое квантовое оборудование, но оно не доходит до создания квантового компьютера».

Шифрование передаваемых данных с помощью световых частиц или фотонов вместо классических алгоритмов, содержащих численные решения, призвано помешать потенциальным хакерам и киберугрозам получить доступ к конфиденциальной информации, даже если в их распоряжении есть работающий квантовый компьютер.

Критически важным для безопасности является то, что закодированные фотоны располагаются в суперпозиции, в которой их истинное состояние не определено, когда они передаются из одного места в другое. В качестве основы основных принципов квантовой механики, запрещающих клонирование, наблюдение за закодированным фотоном в суперпозиции изменит значение хранимых данных этой частицы. Изменение, отмеченное в суперпозиции фотона, в идеале предупредит получателя, если имело место нарушение безопасности.

«Никто не может смотреть на фотон, не изменив его, если он находится в суперпозиции», — сказал Реннер. «И это то, что мы используем».

Схема дополнительно предназначена для отправки пустого тестового фотона перед зашифрованной частицей для проверки соединения и предотвращения захвата фактического сообщения. Любые признаки кибератак на эти зашифрованные фотоны сигнализируют сетевым операторам о необходимости приостановить дальнейшую передачу, прежде чем злоумышленник получит возможность перехватить ценные данные.

«Следовательно, как только у нас появится аппаратно-независимая квантовая криптография, доступная для связи, не останется места для атаки на схему», — сказал Реннер. «Конечно, остается «человеческий» аспект: злоумышленник может принудить например, пользователи схемы раскрывают свои секреты. Но это не проблема, которую может решить криптография».

Реннер отметил иронию роли квантовых технологий как в нападении, так и в защите.

«Квантовые вычисления действительно представляют угрозу для криптографии», — сказал он. «Но квантовая технология также помогает нам лучше защищать данные, и это то, что делает квантовая криптография».

Реннер сказал, что хотя использование квантовых технологий в этих криптографических усилиях призвано повысить безопасность от потенциально враждебных систем квантовых вычислений, все еще существуют нерешенные проблемы, препятствующие полномасштабному внедрению. Одной из таких проблем является потребность в оптоволоконных кабелях специального назначения или дорогих спутниках для передачи фотонов, несущих данные.

Потребность в большом наборе специальных оптических волокон для обеспечения безопасности, которую разрабатывают Реннер и его команда, приводит к тому, что непосредственные варианты использования ограничиваются в первую очередь приложениями с высоким уровнем безопасности между несколькими отдельными местоположениями. Реннер сказал, что широкая доступность зависит от более глубоких инвестиций, а также роста конкурирующих продуктов.

Кроме того, система, предложенная командой Реннера, требует высокой точности шифрования данных в виде фотонов.

«Вам нужно кодировать информацию в фотоны, в частицы света, и эти кодирующие устройства должны работать точно в соответствии со спецификацией», — сказал он. Реннер описал сценарий, в котором некоторые из работающих в настоящее время квантовых криптографических устройств неправильно шифруют частицы, что приводит к неверным показаниям.

«Как правило, проблема в том, что с технологиями, которые у нас есть сегодня, мы просто не можем гарантировать, что устройство в конечном итоге будет делать именно то, что мы от него хотим… слишком много вещей, которые могут пойти не так», — сказал он. «Если устройство не делает то, что должно, то оно больше не является безопасным».

Однако он добавил, что преимущества прикладной квантовой механики в современных усилиях по кибербезопасности, а именно постоянная и нерушимая безопасность, также могут помочь сохранить нынешний ажиотаж вокруг исследований в области квантовых вычислений.

«В традиционной классической криптографии безопасность на самом деле основана на том, что люди называют сложными задачами, например, на факторинге чисел. И как только кто-то изобретает алгоритм для решения этих сложных проблем, криптографическая схема становится небезопасной», — сказал он. «В квантовой криптографии мы вообще не полагаемся на сложные проблемы, мы полагаемся только на законы физики».

«И законы физики, конечно же, никто не может изменить». ***(Alexandra Kelley. The Future of Quantum Security Will Be Encoded in Light, Researchers Hope // Nextgov (https://www.nextgov.com/cybersecurity/2023/01/future-quantum-security-will-be-encoded-light-researchers-hope/382037/). 20.01.2023).***

***