Науково-дослідний інститут інформатики і права
Національної академії правових наук України
Національна бібліотека України імені В. І. Вернадського

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 6 (червень)

Київ – 2020

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К., 2020– №6 (червень) . – 142 с.

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

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

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

ЗМІСТ

«Видавництво #книголав представить новинку для дітей про безпеку в мережі, яка матиме назву «Життя онлайн. Як уберегтися від кібербулінгу, вірусів та інших халеп в інтернеті»…

У виданні буде низка практичних порад зі створення сторінок у соціальних мережах, правила поведінки з інформацією, приватними даними, взаємодії з користувачами й дотримання авторського права. Крім того, у книжці читач знайде інформацію та корисні підказки щодо секстингу, кібербулінгу та інтернет-шахрайства.

В Україні популяризацією цифрової грамотності активно займається Міністерство цифрової трансформації. Крім того, питанням захисту дітей та підлітків від сексуального насильства в інтернеті з 2018 року займається проєкт #Stop_sextинг. Сьогодні вони у співпраці досліджують і проблему захисту дітей у мережі.

Саме тому першими читачами книжки «Життя онлайн…» стали заступниця Міністра цифрової трансформації з питань євроінтеграції Валерія Іонанта засновниця інформаційно-освітнього проєкту #Stop_sextинг Анастасія Дьякова…». ***(В Україні з'явиться книжка для дітей про безпечну поведінку в інтернеті // Новини Полтавщини (https://np.pl.ua/2020/06/v-ukraini-z-iavyt-sia-knyzhka-dlia-ditey-pro-bezpechnu-povedinku-v-interneti/) 10.06.2020).***

****

«Віце-прем'єр-міністр – міністр цифрової трансформації Михайло Федоров хотів би мати змогу захистити персональні дані громадян на конституційному рівні. Про це він заявив на презентації нового освітнього серіалу…

"Сьогодні ми займаємось повністю комплексним вирішенням питання захисту реєстру, ми працюємо над новим законом разом з нашою командою, комітетом, уповноваженим, і я сподіваюсь що десь через кілька місяців – рік кожен українець зможе конкретно відчути як змінилось ставлення держави, бізнесу до питання персональних даних… Сьогодні питання захисту персональних даних – це базове питання цифрової грамотності, і взагалі було б добре навіть, не знаю можливо це чи ні, в найближчий час, на конституційному рівні захистити права людей в цьому питанні", - сказав Федоров.

З його слів, його Міністерство все більше уваги буде приділяти захисту персональних даних і кібербезпеки.

"На сьогодні я почав координувати спеціалістів Кіберполіції і профільного управління СБУ на рахунок вирішення конкретних питань, коли злодії продають дані українців. Ми кожного тижня зустрічаємось, в нас вже є прогрес, скоро ви всі дізнаєтесь про конкретні справи, які були відкриті, зареєстровані на рахунок захисту даних", - зазначив міністр…». ***(Саша Картер. Федоров: було б добре захистити персональні дані громадян на конституційному рівні // Інформаційне агентство «Українські Національні Новини»***

(https://www.unn.com.ua/uk/news/1873173-fedorov-bulo-b-dobre-zakhistiti-personalni-dani-gromadyan-na-konstitutsiynomu-rivni). 04.06.2020).

****

«Міністерство цифрової трансформації України за підтримки Програми розвитку ООН в Україні, Уповноваженого Верховної Ради України з прав людини та ГО "PrivacyHub" презентувало освітній серіал «Персональні дані»…

"Персональні дані — це всі дані про вас, наприклад, прізвище, ім'я, по батькові, паспортні дані, електронна пошта, дата народження та інше. І навіть ваші лайки та коментарі у соцмережах є персональними даними. По-суті, будь-яка інформація, яка відноситься до вас, є персональними даними. Освітній серіал про персональні дані пояснює складну та серйозну тему в серйозній формі", — розповіла заступник міністра цифрової трансформації з питань євроінтеграції Валерія Іонан.

З її слів, участь у серіалі взяли "зірки" — актор театру та кіно, народний артист України Олексій Вертинський та блогер, акторка та співачка Марія Кондратенко.

Серіал складається з семи серій тривалістю до 8 хвилин і охоплює теми:

- Що таке персональні дані?
- Підстави для обробки персональних даних
- Ваші права у сфері персональних даних
- Як перевірити, чи безпечно оброблятиме сайт персональні дані?
- Персональні дані в соціальних мережах тощо…»

(Саша Картер. Мінцифри презентувало новий освітній серіал про персональні дані // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1873180-mintsifri-prezentuvalo-noviy-osvitniy-serial-pro-personalni-dani). 04.06.2020).

****

«Секретар РНБО України Олексій Данилов та Заступник Секретаря РНБО України Сергій Демедюк нагородили переможців першого в Україні онлайн-хакатону «Говерла» для суб'єктів Закону України «Про основні засади забезпечення кібербезпеки України» та працівників критичної інфраструктури, проведеного Національним координаційним центром кібербезпеки при РНБО України та фондом CRDF Global в Україні…

О. Данілов зазначив, що подібні заходи надзвичайно актуальні і відповідають вимогам часу. «Вкотре хочу наголосити, що традиційні війни відходять в минуле, сучасні загрози мають кібернетичний та біологічний характер, а також актуальним є питання протистояння у космосі. Події останнього часу навколо пандемії довели це», - сказав він, підкресливши важливість посилення співпраці між державним та приватним сектором у сфері протидії кіберзагрозам.

Заступник Секретаря РНБО України С. Демедюк зазначив, що онлайн-хакатон дав можливість фахівцям державних структур та приватних компаній

продемонструвати свої навички на практиці та виробити спільні підходи до реагування на кіберінциденти.

Переможці онлайн-хакатону поділилися позитивними враженнями, відзначивши елемент змагальності та цінність практичного досвіду.

За результатами штабних кібернавчань найвищих показників досягли представники червоної команди етичних хакерів: представники компаній Cyber Unit, ITLab, Berezha Security, 10Guards». ***(У РНБО нагородили переможців першого в Україні онлайн-хакатону з кібербезпеки // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/100620-u-rnbo-nagorodyly-peremozhciv-pershogo-v-ukrayini-onlayn-hakatonu-z-kiberbezpeky). 10.06.2020).***

***

«Міністерство цифрової трансформації запустило новий онлайн-курс "Кіберняні", який допоможе зменшити ризики втрати приватної інформації. Про це йдеться на сайті "Дія. Цифрова освіта".

Як зазначається, з часом українці частіше проводять час у мережі та надають своїм гаджетам все більше особистої інформації. Однак, не всі громадяни вміють протистояти загрозам з боку інтернет-злочинців та шахраїв.

"З цього курсу ви дізнаєтеся, як мінімізувати ризики втрати вашої приватної, чутливої інформації. Як попередити кібератаку або кібершахрайство та як швидко відновитися після них, у випадку якщо вони все ж таки сталися. Участь у серіалі взяли експерти, для яких кібербезпека - це не тільки робота, а спосіб життя", - пояснили розробники курсу.

До слова, проєкт "Кіберняні" виник у результаті співпраці Міністерства цифрової трансформації України, компанії з кібербезпеки 10Guards, компанії Cyberlab і компанії Moneyveo. Освітній серіал вже доступний на платформі з цифрової грамотності "Дія. Цифрова освіта".» ***(Мінцифри створило освітній серіал "Кіберняні" // Західна інформаційна корпорація (https://zik.ua/news/ludyna/mintsyfry_stvorylo_osvitnii_serial_kiberniani_970708). 04.06.2020).***

***

«Основной функцией любого государства (в том числе электронного) остается обеспечение безопасности его граждан. Это означает, что Украине нужно защищать данные ее жителей, реестры и ресурсы в киберпространстве точно так же, как если бы речь шла о физическом имуществе. Но с кибербезопасностью у нас сегодня проблема.

Чтобы прийти к такому выводу, достаточно просмотреть заголовки последних новостей, вроде "Базы данных украинской таможни продают в интернете за $100" или "Сбережения в Приват24 под угрозой. Деньги крадут даже у специалистов по кибербезопасности". Можно вспомнить и недавний скандал с анонимным Telegram-каналом, взлом сайта президента в 2014 году, пропавшие из фискальной службы терабайты информации в 2016-м, не говоря уже про вирусы WannaCry и PetyA, которые ударили по большинству государственных компаний.

Что мы можем противопоставить угрозе повторения подобных атак и сливов?

В мировом рейтинге компетенции кибербезопасности ITU Украина сегодня находится на 54 месте, в рейтинге National Cyber Security Index – на 29 месте. Если в 2016 году украинские команды были на первых местах в международном Capture The Flag, то сегодня их там уже нет. Конечно, есть крутые специалисты, и много, но наличие крутых специалистов в частных компаниях, с которыми государство не сотрудничает, к сожалению, не влияет на уровень киберзащиты страны. И в результате мы имеет то, что имеем.

Какие же у нас фундаментальные проблемы и какие могли бы быть решения?

Основные проблемы следующие:

- нет государственной программы кибербезопасности, начиная от современного законодательства до плана его реализации;
- нет современных требований по защите баз данных, отслеживания их выполнения и наказания за нарушения;
- в Украине официально существует около 350 основных баз данных, но можно предположить, что еще больше баз данных находится "в тени";
- нет понятной государственной политики по интеграции реестров и прозрачной технической архитектуры государственных решений;
- нехватка профессиональных кадров, отсутствие отраслевых и региональных CERT (computer emergency response team – компьютерная группа реагирования на чрезвычайные ситуации), нежелание системно привлекать частный сектор.

Перечень можно продолжить, но для нас важен вывод, что мы не можем быть до конца уверены, что все системы и реестры будут защищены, а масштабные кибератаки – отражены. Не зря в некоторых странах Украину называют киберполигоном и оттачивают здесь свои хакерские навыки.

Как в такой ситуации можно было бы усилить защищенность украинского киберпространства?

Принять закон про кибербезопасность и разработать план его внедрения;

- выделить достаточные ресурсы для выполнения плана, так как кибербезопасность – это тоже часть национальной безопасности;
- сделать требования КСЗИ (комлексной системе защиты информации) более современными, но при этом бескомпромиссно требовать выполнения правил и соответствия всех реестров новым требованиям;
- принять законопроект про облака, так как сертифицированные облака более безопасные, чем "сервера под столом", и создать стратегию перехода в облака Cloud First;

Начинать систематически привлекать частный сектор к защите систем и реестров. Для этого нужно сотрудничество с "белыми хакерами" (white hat hackers), "подконтрольные" попытки взлома (bounty hunt), постоянная работа с центрами реагирования на кибератаки (SOC – операционный центр безопасности, и CERT) обучение сотрудников силовых органов для повышения компетенций в кибербезопасности и обучение граждан кибергигиене;

- поддерживать создание отраслевых и региональных центров кибербезопасности (SOC, Cert) также в сотрудничестве с частным рынком.

Конечно, на этом список возможных мероприятий не заканчивается, однако даже этого могло бы хватить, чтобы существенно улучшить готовность государства защитить персональные данные физических и юридических лиц, реестры и системы, без чего масштабная диджитализация несет реальный риск». ***(Полигон для хакеров. Как Украине защитить свое киберпространство и данные граждан // ФОКУС (https://focus.ua/opinion/technologies/456599-poligon_dlia_khakerov_kak_ukraine_zashchitit_svoe_kiberprostranstvo_i_dannye_grazhdan). 03.06.2020).***

***

«…Студентів Академії патрульної поліції навчать основ кібербезпеки. Викладачами стануть фахівці Департаменту кіберполіції Національної поліції України, повідомляють у відомстві.

Сторони уклали між собою меморандум і домовились разом протидіяти кіберзлочинності через покращення в освітньому процесі. Після курсу студенти зможуть також пройти практику на базі Департаменту.

«Ми вважаємо, що майбутнє – за кібернетикою, і багато професій, які є на сьогодні, вже через 20 років будуть не потрібні. Але завжди потрібен буде патрульний поліцейський, який вміє користуватися різними інформаційними технологіями. Саме тому меморандум – це перший крок до нашої спільної взаємодії та підготовки кваліфікованих поліцейських», – переконаний Вадим Лісничук, керівник Академії…» ***(Патрульним викладатимуть основи кібербезпеки // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/24920/2020-06-22-patrulnim-vikladatimut-osnovi-kiberbezpeki/). 22.06.2020).***

***

«З 17 по 23 червня Система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала 44 399 підозрілих подій, що на 3% менше, ніж минулого тижня…

Переважна більшість зафіксованих підозрілих подій стосується спроб мережевого сканування (48%), виявлення нестандартних протоколів або подій (30%), виявлення мережевого трояна (9%), веб-атак (7%) та спроб отримання прав адміністратора (5%)…

Зазначається, що система захищеного доступу державних органів до мережі Інтернет заблокувала 8 892 різних видів атак, що на 14% більше, ніж попереднього тижня. Переважна більшість (99%) — це мережеві атаки прикладного рівня. Також заблоковано 7 DDoS-атак, переважна більшість — на сайти Офісу Президента України.

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 5637 кіберінцидентів.

"Переважна більшість опрацьованих інцидентів належить доменній зоні UACOM (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (98% від загальної кількості) та фішингу (1%)",- додається у повідомленні…». ***(Валерія Гуржий. У Держспецзв'язку заявили про зменшення кібератак на***

сайти органів влади // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1876902-u-derzhspetszvyazku-zayavili-pro-zmenshennya-kiberatak-na-sayti-organiv-vladi). 24.06.2020).

***

Національна система кібербезпеки

«Кабінет міністрів України на засіданні у середу призначив заступника міністра з питань цифрового розвитку, цифрових трансформацій і цифровізації (CDTO) у Міністерстві охорони здоров'я. Про це повідомляє пресслужба Міністерства цифрової трансформації України…

Зі слів міністра цифрової трансформації Михайло Федорова, CDTO допоможе розробити та реалізувати стратегію цифрової трансформації системи охорони здоров'я.

"Змінити підхід до послуг, які вже існують, та впровадити нові," – додав він.

Зазначається, що CDTO займатиметься е-послугами та електронними реєстрами. Визначатиме, які процеси потребують оптимізації та першочергової цифровізації. Працюватиме над реалізацією цифрової трансформації на всіх рівнях. А також буде працювати над посиленням кібербезпеки та захисту інформації.

"Невдовзі CDTO будуть призначені в кожному міністерстві та усіх центральних органах виконавчої влади", - додали в Мінцифри…». ***(Саша Картер. Уряд призначив Степанову CDTO // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1872949-uryad-priznachiv-stepanovu-cdto). 03.05.2020).***

***

«Кабінет Міністрів України призначив Валерія Бушкова CDTO у Міністерстві соціальної політики.

CDTO – Chief Digital Transformation Officer, профільний заступник Міністра з питань цифрового розвитку, цифрових трансформацій і цифровізації.

“Державна система потребує рішучих трансформацій за допомогою IT-технологій. CDTO допоможуть нам розробити єдину стратегію ефективної цифровізації нашої держави. Тому профільні заступники скоро з`являться в усіх центральних органах виконавчої влади”, – прокоментував Віце-прем’єр-міністр – Міністр цифрової трансформації Михайло Федоров.

Основне завдання CDTO – цифровізація надання послуг громадянам та оптимізація процесів у Міністерстві за допомогою використання сучасних IT-технологій.

Профільний заступник з питань цифровізації працюватиме за підтримки Мінцифри. До його основних функціональних обов’язків також входить визначення та аналіз процесів, які потрібно цифровізувати, формування пріоритетів. Спрощення адміністративних процедур. CDTO впроваджуватиме е-послуги, оптимізуватиме інформаційні системи та державні реєстри та

визначатиме, які процеси потребують цифровізації у першу чергу. Також він працюватиме над посиленням кібербезпеки та захисту інформації.

CDTO – це не просто IT-фахівець, а в першу чергу цифровий реформатор. Він допоможе не лише створити, але й втілити стратегію цифрової трансформації галузі». ***(У Мінсоцполітики з'явиться заступник Міністра з цифрової трансформації // Офіційно (https://oficiyno.com.ua/2020/06/17/u-minsotspolitiki-zjavitsja-zastupnik-ministra-z-tsifrovoji-transformatsiji-36165/). 17.06.2020).***

***

Правове забезпечення кібербезпеки в Україні

«Верховна Рада ухвалила Закон щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації. Зміни до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» стосуються підтвердження відповідності інформаційної системи вимогам про захист інформації ЄС. Їх подали народні депутати Комітету цифрової трансформації.

«Ми впроваджуємо вимоги стандартів сімейства системи управління інформаційною безпекою (СУІБ) для окремих категорій інформації. Важливо, що ці вимоги діють для забезпечення інформаційної та кібербезпеки в ЄС і наближують Україну до європейських норм».

За Законом, підтвердження відповідності комплексної системи захисту інформації (КСЗІ) відбуватиметься за результатами держекспертизи.

Важливо! Тепер державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, може оброблятися в системі без застосування КСЗІ, у разі виконання умов:

підтвердження відповідності системи управління інформаційною безпекою національним стандартам України щодо систем управління інформаційною безпекою;

використання для захисту інформації в системі засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи;

жоден з елементів системи не може бути розташований на території України, де органи державної влади тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких застосовані санкції відповідно до Закону України «Про санкції», та на територіях держав, які належать до митних союзів з такими державами;

виконання особливих вимог, встановлених Урядом до забезпечення захисту інформації в системах залежно від категорії державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Схвалений закон запроваджує альтернативний спосіб підтвердження відповідності інформаційної системи вимогам із захисту інформації. Цікаво,що схожа практика законодавства вже застосовується в Україні у сфері публічних

закупівель». ***(В Україні ухвалили Закон про захист інформації в телекомунікаційних системах // Pingvin Pro (https://pingvin.pro/gadgets/news-gadgets/v-ukrayini-uhvalyly-zakon-pro-zahyst-informacziyi-v-telekomunikaczijnyh-systemah.html). 05.06.2020).***

***

«В Раде зарегистрировали проект закона о переводе трудовых книжек в цифровой формат — он призван облегчить бюрократическую составляющую как работодателям, так и сотрудникам…

В то же время бизнес обратил внимание, что у реформы есть и другая сторона, которая может перекрыть весь позитив, и из-за которой компании неизбежно столкнутся с большими трудностями при переходе в цифру.

Так, глава HR-департамента компании Nota Group Яна Декусар в своей колонке на Лига.net отмечает, что проект предлагает установить пятилетний переходный период для внесения в Госреестр сведений из бумажных трудовых книжек о трудовой деятельности работника. То есть в этот период будут использовать как бумажную трудовую, так и электронную.

"Это значит, что кадровиков в ближайшие 5 лет ожидает двойной учет. Пока трудовые книги будут существовать в привычном нам книжном формате, нам придется вести их по старой схеме — заполнять, делать копии по просьбе сотрудника и так далее. К этой работе добавится еще одна — перенесение всех сведений в онлайн формат", — говорит эксперт.

Она напоминает, что согласно проекту, после внесения сведений о трудовой деятельности работника в Госреестр, работодатель обязан выдать оригинал бумажной трудовой книжки ему на руки под роспись, при этом также работодатель должен вносить по требованию работника в бумажную трудовую записи о приеме на работу, переводе и увольнении.

"С большой уверенностью скажу, что первое время сотрудники будут просить на всякий случай продублировать записи в бумажную трудовую книжку. Поэтому обещанный покой "нам будет только сниться", — уверена Декусар.

По ее словам, могут возникнуть проблемы и из-за не совершенной системы электронного документооборота.

"Если в электронной версии была допущена ошибка (неправильное написание фамилии, компании) человека можно надолго "потерять" в цифровом поле вместе с его трудовой историей. Восстанавливать данные придется долго и мучительно, бюрократическим способом — очно, лично и с документами", — подчеркивает глава HR-департамента.

Она добавляет, что также возможны утечки информации или кибератаки. При этом Декусар, в принципе, одобряет реформу, однако считает, что инициативу нужно проработать с помощью эйчаров-практиков прежде, чем ее внедрять по всей стране». ***(Ольга Калинина. Бизнес обеспокоился переводом трудовых книжек в цифру: "Кадровиков ожидает двойной учет" // Зоряный (https://zoryanyy.tv/articles/economics/biznes_obespokoilsya_perevodom_trudovykh_knizhek_v_tsifru_kadrovikov_ozhidaet_dvoynoy_uchet/). 23.06.2020).***

***

«З 27 травня по 2 червня система захищеного доступу державних органів до мережі Інтернет заблокувала 25 DDoS-атак, переважна більшість з яких - на сайти Офісу Президента України…

"Системою кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури з 27 травня до 2 червня на об'єктах моніторингу зафіксовано 115459 підозрілих подій, що на 7% більше, ніж попереднього тижня", - йдеться у повідомленні.

Вказано, що переважна більшість зафіксованих підозрілих подій стосується виявлення нестандартних протоколів або подій (66%), спроб мережевого сканування (27%), виявлення мережевого трояна (3%), веб-атак (2%) та спроб отримання прав адміністратора (2%).

"Система захищеного доступу державних органів до мережі Інтернет заблокувала 10767 різних видів атак, що на 56% більше, ніж попереднього тижня. Переважна більшість (99%) з них - це мережеві атаки прикладного рівня. Також було заблоковано 25 DDoS-атак, переважна більшість з яких - на сайти Офісу Президента України", - йдеться у повідомленні.

Повідомляється, що урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 2451 кіберінцидент, що на 27% менше, ніж попереднього тижня. Переважна більшість опрацьованих інцидентів належить доменній зоні UACOM (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (94% від загальної кількості) та фішингу (4%)…». ***(Дар'я Панченко. Впродовж тижня зафіксували 25 DDoS-атак на держоргани, більшість з яких - на сайти ОПУ // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1872743-vprodovzh-tizhnya-zafiksuvali-25-ddos-atak-na-derzhorgani-bilshist-z-yakikh-na-sayti-opu). 02.06.2020).***

****

«Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA в середу повідомила про те, що система кібернетичного захисту державних інформаційних ресурсів і об'єктів критичної інфраструктури на об'єктах моніторингу в період з 3 по 9 червня зафіксувала 54,835 тис. кіберінцидентів, що на 53% менше у порівнянні з попереднім тижнем.

В повідомленні Держспецзв'язку відзначається, що переважна більшість зафіксованих підозрілих подій стосується виявлення нестандартних протоколів або подій (50%), спроб мережевого сканування (34%), виявлення мережевого трояна (7%), веб атак та спроб отримання прав адміністратора (по 4%).

Система захищеного доступу державних органів до мережі інтернет заблокувала 14890 різних видів атак, що на 28% більше, ніж на попередньому тижні. З них 99% - мережеві атаки прикладного рівня. Також були заблоковані 8 DDoS-атак (переважна більшість - на сайти Офісу Президента України).

В цей період зареєстрували та обробили 2878 кіберінциденти, що на 15% більше, ніж на попередньому тижні.

Переважна більшість оброблених інцидентів належить доменній зоні UACOM (близько 98%). Основна кількість інцидентів стосується поширення шкідливого ПО (94% загальної кількості) і фішингу (до 3%)…» ***(Кількість кіберінцидентів в Україні за тиждень скоротилася на половину // Дзеркало тижня. Україна (https://dt.ua/TECHNOLOGIES/kilkist-kiberincidentiv-v-ukrayini-za-tizhden-skorotilasya-na-polovinu-350468_.html). 10.06.2020).***

***

«Провайдер «Воля» звернувся до кіберполіції через DDoS-атаки на свої сервери, які тривали з 31 травня по 2 червня. Загалом повна відсутність доступу до сервісів тривала 12 хвилин 31 травня та 45 хвилин 1 червня. Також була зафіксована атака на веб-сайт volia.com, але її вдалося нейтралізувати. Про це провайдер повідомив 2 червня.

«Спочатку атаки були тільки на абонентські підсистеми, але пізніше вони перейшли на телекомунікаційну інфраструктуру. В результаті більше 100 000 абонентів відчули проблеми в користуванні інтернетом, IPTV, мультиекранними платформами і цифровим телебаченням», – йдеться в повідомленні.

Компанія має системи виявлення таких атак, блокує атакований хост на рівні ядра мережі тощо: «Незважаючи на це, в компанії не можуть бути впевнені, що атаки не повторяться знову, проте роблять все можливе, щоб цього уникнути».

За словами юристів компанії, ці дії мають ознаки кримінального правопорушення за ст. 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) ККУ, яка передбачає обмеження волі до 5 років.

«Атаки такого обсягу мають своїх замовників і виконавців. Іноді за ними слідує здирництво та інші спроби впливу на компанію. Тому ВОЛЯ твердо заявляє: ці атаки не допоможуть злочинцям досягти своїх цілей, адже компанія діє виключно в рамках законодавства, захищаючи свій сервіс і кожного абонента», – говорять у провайдера…» ***(«Воля» повідомила про кібератаку на свої сервери // ДЕТЕКТОР МЕДІА (https://detector.media/rinok/article/177686/2020-06-03-volya-povidomila-pro-kiberataku-na-svoi-serveri/). 03.06.2020).***

***

«Сайт украинского благотворительного фонда «Таблеточки» (предоставляет помощь онкобольным детям и их семьям) подвергся кибератаке. Со вчерашнего вечера и по состоянию на момент написания этой новости (10:18) сайт остается недоступен, а администраторы пока разбираются с инцидентом, устанавливая, какого рода данные могли быть похищены и насколько масштабной оказалась атака.

Об атаке администраторы фонда рассказали на своей страничке в Facebook.

Обнаружив подозрительную активность, администраторы моментально отключили сайт от хостинга, чтобы защитить данные сотен тысяч благотворителей. Сейчас технические партнеры занимаются расследованием инцидента, пытаясь

выяснить, к чему именно хакеры получили доступ. Пока неясно, смогли ли злоумышленники добраться до базы данных наших благотворителей — этот вопрос, а также возобновление работы сайта, сейчас в приоритете. Администраторы обещают предоставить ответы, как только сами все узнают, призывая следить за обновлениями на фейсбуке.

«Таблеточки» использует систему защиты от хакерских атак Cloudflare. Также в фонде отмечают, что осенью 2019 года сайт прошел аудит на уязвимость к атакам — тогда никаких критических уязвимостей проверка не показала». ***(Владимир Скрипин. Сайт фонда помощи онкобольным детям «Таблеточки» атаковали хакеры // ООО «ХОТЛАЙН» (https://itc.ua/news/sajt-fonda-pomoshhi-onkobolnym-detyam-tabletochki-atakovali-hakery/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 03.06.2020).***

***

«На Львівщині СБУ блокувала діяльність розгалуженої мережі «ботоферм», які керувались з території Російської Федерації…

Як зазначається у повідомленні, Служба безпеки України блокувала на території Львівської області діяльність розгалуженої мережі «ботоферм», які керувались з території країни-агресора.

Оперативники відділу кібербезпеки встановили, що організатори через відповідне телекомунікаційне обладнання та спеціалізоване програмне забезпечення керували електронними поштовими скриньками та обліковими записами у соцмережах з використанням фейкових персональних даних. Реєстрацію таких акаунтів в мережі «Інтернет», ділки здійснювали за допомогою SIM-карток українських та російських операторів зв'язку.

Загалом угруповання зареєструвало кілька тисяч активних акаунтів для поширення у соцмережах недостовірної інформації щодо ситуації в Україні, продовження гібридної війни проти нашої держави та здійснення впливу на свідомість людей з метою поширення негативного настрою в суспільстві та дискредитації української влади.

В рамках спільної спецоперації проведеної оперативниками СБ України на території нашої держави, схожа протиправна діяльність була виявлена та припинена в Києві, Сумах, Чернігові та Одесі.

Під час проведення обшуків слідчими та оперативниками СБУ виявлено і вилучено комп'ютерну техніку та спеціальне обладнання (GSM-модеми та шлюзи), понад 15 тисячі SIM-карток операторів стільникового мобільного зв'язку України та Росії.

В результаті проведених заходів перевіряється версія щодо причетності до організації вказаної протиправної діяльності спеціальних та розвідувальних органів РФ.

Операцію провели оперативники УСБУ у Львівській під процесуальним керівництвом Прокуратури Львівської області». ***(На Львівщині СБУ викрила і заблокувала російську «ботоферму», що керувалась з території Російської Федерації // То є Львів (https://inlviv.in.ua/lviv/lvivshhina/na-lvivshhyni-sbu-vykryla-***

i-zablokuvala-rosijsku-botofermu-shho-keruvalas-z-terytoriyi-rosijskoyi-federatsiyi). 16.06.2020).

***

Боротьба з кіберзлочинністю в Україні

«На Виноградівщині працівники відділу протидії кіберзлочинам в Закарпатській області, спільно з місцевими правоохоронцями, за процесуального керівництва Ужгородської прокуратури, викрили чоловіка, який незаконно отримував доступ до приватних даних своїх клієнтів. 39-річний житель села Олешник розробив шкідливе програмне забезпечення для злому акаунтів користувачів соцмереж. Придбавши програму через створений чоловіком канал у загальнодоступному месенджері, та встановивши на свій гаджет, клієнти отримували змогу зламувати мережеві акаунти користувачів соцмереж, а сам незаконний бізнесмен, здобував безперешкодний доступ до гаджетів своїх клієнтів.

Один з потерпілих, запідозривши, що придбаний інтернет-продукт може бути хакерським, звернувся до поліції. Він розповів правоохоронцям, що після того, як придбав застосунок для злому акаунтів, зрозумів, що до його комп'ютера має доступ інша людина.

Правоохоронці провели перевірку у ході якої і вийшли на 39-річноговиноградівця.

Під час проведення працівниками відділу кіберполіції в Закарпатській області санкціонованих обшуків за місцем проживання фігуранта, вилучено використовувану у злочинних цілях комп'ютерну техніку, мобільні телефони, банківські платіжні картки та флешносії інформації.

Наразі узгоджується питання вручення фігурантові повідомлення про підозру у двох злочинах, пов'язаних з виготовленням та розповсюдженням шкідливого програмного забезпечення та втручання у роботу ЕОМ, тобто за статтею 361 та 361-1 Кримінального кодексу України. Досудове розслідування триває». ***(Закарпатська поліція викрила хакера, який незаконно отримував доступ до персональної інформації користувачів // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/zakarpatska-policziya-vykryla-xakera-yakyj-nezakonno-otrymuvav-dostup-do-personalnoyi-informacziyi-korystuvachiv-1314/). 12.06.2020).***

***

«Співробітники кіберполіції у Дніпропетровській області спільно зі слідчими поліції області, під процесуальним керівництвом місцевої прокуратури, викрили чоловіка, який займався збутом шкідливих програмно-технічних та технічних засобів.

Поліцейські встановили, що до злочинних дій причетний мешканець міста Павлоград, 1984 року народження. Вказані технічні засоби фігурант збував за грошову винагороду у мережі Інтернет.

Основним призначенням таких засобів було незаконне подолання логічного захисту WI-FI мереж, пристроїв для подальшого несанкціонованого втручання в роботу комп’ютерів, мереж, з подальшим викраденням паролів, персональних даних осіб та їх незаконним використанням.

Правоохоронці провели обшук за місцем мешкання зловмисника. Поліцейські вилучили програмно-технічні засоби, призначені для взлому пристроїв WI-FI, жорсткі диски, накопичувачі інформації, а також мобільний телефон та чорнові записи.

За даним фактом відкрито кримінальне провадження за ч. 1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) та ч. 2 ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України.

Наразі вирішується питання щодо оголошення фігуранту про підозру. Йому загрожує покарання у вигляді позбавлення волі на строк від трьох до шести років. Слідчі дії тривають». ***(Кіберполіція викрила чоловіка у збуті шкідливих програмно-технічних засобів // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-cholovika-u-zbuti-shkidlyvyx-programno-texnichnyx-zasobiv-7876/). 11.06.2020).***

***

«Співробітники кіберполіції в Одеській області спільно зі слідчим управлінням поліції області, під процесуальним керівництвом обласної прокуратури припинили неправомірну діяльність державного реєстратора.

Кіберполіція встановила, що посадовець за допомогою спеціального електронного ключа скасував державну реєстрацію права власності на нерухоме майно на підставі неіснуючого рішення суду. Такими діями фігурант позбавив права власності законного власника, чим завдав шкоди на суму понад дев’ять мільйонів гривень.

Правоохоронці провели обшук за місцем мешкання фігуранта. Наразі чоловіку вже оголошено про підозру за ч. 3 ст. 362 (Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду) Кримінального кодексу України.

Санкція статті передбачає позбавлення волі на строк від трьох до шести років. Відносно державного реєстратора судом обрано запобіжний захід у вигляді цілодобового домашнього арешту». ***(Кіберполіція Одещини припинила неправомірну діяльність державного реєстратора // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-odeshhyny-prypynyla-nepravomirnu-diyalnist-derzhavnogo-reyestratora-2251/). 04.06.2020).***

***

«Співробітники Департаменту кіберполіції спільно з Головним слідчим управлінням НПУ, під процесуальним керівництвом Офісу генерального прокурора, викрили чоловіка у несанкціонованому доступі до облікових записів користувачі мережі Інтернет.

Кіберполіція встановила, що до такої діяльності причетний киянин, 1999 року народження. Фігурант самостійно створив шкідливе програмне забезпечення. За допомогою вказаної вірусної програми він отримував доступ до облікових записів електронних поштових сервісів, аккаунтів соціальних мереж, ігрових порталів та інших вебресурсів.

Крім цього, чоловік розповсюджував дане шкідливе програмне забезпечення на тематичному вебфорумі.

Правоохоронці провели обшук за місцем мешкання фігуранта. За результатами вилучено комп'ютерну техніку, флеш-накопичувачі, мобільний телефон та банківську картку.

За даним фактом відкрито кримінальне провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України.

Санкція статті передбачає позбавлення волі на строк від трьох до шести років. ***(Кіберполіція викрила чоловіка у несанкціонованому доступі до облікових записів користувачів мережі // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-cholovika-u-nesankczionovanomu-dostupi-do-oblikovyx-zapysiv-korystuvachiv-merezhi-2972/). 02.06.2020).***

****

«…Відділом протидії кіберзлочинам спільно з працівниками Мукачівського відділу поліції, під процесуальним керівництвом Мукачівської місцевої прокуратури, викрито мешканця Закарпатської області, який, перебуваючи на посаді спеціаліста по ломбардному кредитуванню одного із українських банків, незаконно привласнив приблизно 700 000 гривень. Поліцейські з'ясували, що, маючи право доступу до комп'ютерної програми, яка обробляє інформацію для ломбардної діяльності, закарпатець змінив інформацію, яка обробляється у вказаній програмі.

Внісши недостовірні відомості до заяв про приєднання до умов кредиту під заставу дорогоцінного металу, чоловік привласнив гроші клієнтів банку.

Фігуранту повідомлено про підозру за ч.1,3 ст. 191 та ч.1,3 ст. 362 КК України, тобто привласнення та розтрата майна, або заволодіння ним, шляхом зловживання службовим становищем та несанкціоноване використання інформації з ЕОМ.

Обвинувальний акт буде скеровано до суду. Фігуранту загрожує покарання у вигляді позбавлення волі строком від трьох до восьми років». ***(На Закарпатті поліція викрила працівника банку, що привласнив 700 тисяч гривень // Департамент кіберполіції Національної поліції України***

(https://cyberpolice.gov.ua/news/na-zakarpatti-policziya-vykryla-praczivnyka-banku-shho-pryvlasnyv--tysyach-gryven-978/). 16.06.2020).

***

«Сотрудники правоохранительных органов провели 36 обысков в десяти регионах в ходе спецоперации «Дата», целью которой было расследовать утечку и распространение персональных данных граждан из государственных и частных баз данных.

Об этом сообщил первый заместитель начальника Департамента киберполиции Нацполиции Сергей Кропива…

«За время проведения спецоперации мы возбудили 34 уголовных производства, а в течение десяти дней ее реализации провели 36 обысков. В результате установили и подтвердили преступную деятельность 25 человек. Восьми лицам было сообщено о подозрении, одного человека задержали», - сказал он.

Кропива уточнил, что спецоперацию под условным названием «Дата» провел Департамент киберполиции совместно со Службой безопасности.

Как рассказал чиновник, злоумышленники похитили базы данных компаний, занимающихся страхованием, предоставлением логистических услуг, а также базы государственных и частных банков. Кроме того, похищена информация о лицах, имевших доступ к государственным реестрам и базам данных государственных органов. Хакеры также достали базы данных водителей службы перевозок.

«Большую долю данных баз составлял частный сектор, а также информация о владельцах почтовых адресов и другой информации, которая может идентифицировать личность», - проинформировал Кропива.

Он уточнил, что за отдельную информацию хакеры требовали от тысячи гривен, а за целую базу данных - тысячу долларов…». ***(По делу об утечке данных граждан провели 36 обысков // ForUm (https://for-ua.com/article/1201493). 25.06.2020).***

***

«Киберполиция разоблачила «хакера», который взламывал личные кабинеты клиентов КП «Полтавааводоканал»…

Вероятным подозреваемым в несанкционированном вмешательстве в работу информационной системы коммунального предприятия является 44-летний полтавчанин. «Хакер» обходил степени защиты «Полтавааводоканала» с помощью вредоносного программного обеспечения.

Противоправную деятельность мужчины пресекли сотрудники отдела противодействия киберпреступности в Полтавской области совместно со следователями Полтавского отдела полиции и сотрудниками Службы безопасности Украины в Полтавской области под процессуальным руководством Полтавской прокуратуры.

Александр Ведмидский, начальник отдела противодействия киберпреступности в Полтавской области, отметил:

"Мужчина, используя вредоносное программное обеспечение, взламывал личные кабинеты клиентов «Полтававодоканала» и, используя их персональные данные, вносил изменения в показатели учета потребленной воды. Во время проведения санкционированных судом обысков по адресу проживания фигуранта, следователями изъяты ноутбук Lenovo, USB и SD накопители, USB-модем, sim-карты операторов мобильной связи и другие доказательства, подтверждающие факт сбора и хранения персональных данных жителей Полтавы".

По данному факту внесены сведения в Единый реестр досудебных расследований по ч. 1 ст. 361 (Несанкционированное вмешательство в работу электронно-вычислительных машин, компьютерных сетей) и ч.1 ст. 182 (Нарушение неприкосновенности частной жизни) Уголовного кодекса Украины. Решается вопрос о сообщении мошеннику о подозрении и избрании меры пресечения.

В случае доказательства вины мужчины, ему грозит штраф или ограничение свободы на срок от двух до пяти лет. Продолжаются следственные действия». ***(Артем Сереженок. Киберполиция задержала хакера, который взламывал личные кабинеты клиентов коммунального предприятия // Internetua (https://internetua.com/kiberpoliciya-zaderjala-hakera-kotoryi-vzlamyval-licsnye-kabinety-klientov-kommunalnogo-predpriyatiya). 28.06.2020).***

****

Коронавірус COVID-19 та питання кібербезпеки

«За первый квартал 2020 года количество кибернетических атак по сравнению с предыдущим кварталом возросло на 25%, — сообщает служба Beazley Breach Response (BBR).

Интернет ресурсу УкрСтрахование известно, что возросшее количество кибернетических инцидентов связано с карантинными ограничениями, вызванными пандемией Covid-19.

В частности, авторы отчета указывают одним из главных рисков кибератак стал переход на удаленный режим работы, прежде всего, предприятий финансового сектора и медицинских учреждений. На их долю пришлось более половины всех кибернетических инцидентов во втором квартале.

Согласно отчету Beazley, хакерские атаки были направлены не только на предприятия и организации, но и на их многочисленных клиентов. Повышенная кибернетическая уязвимость физических лиц в отчетном периоде объясняется повышенной тревожностью и снижением критического анализа поступающих электронных сообщений.

«Киберпреступники во время этой пандемии охотятся на людей с повышенной тревогой, заставляя их кликать и делиться ссылками, которые крадут информацию», — сказала Кэтрин Киф, глава BBR Services. По ее словам, работа на домашних компьютерах сопряжена с низкой IT-безопасностью, что успешно используется злоумышленниками». ***(Пандемия спровоцировала скачок***

кибернетических инцидентов // УкрСтрахование (https://www.ukrstrahovanie.com.ua/news/pandemiya-sprovoczirovala-skachok-kiberneticheskih-inczidentov). 10.06.2020).

***

«BI.ZONE поможет защитить медицинские учреждения, которые занимаются борьбой с коронавирусом, от атак киберпреступников. Компания присоединилась к глобальной инициативе Cyber4Healthcare, организованной международной некоммерческой организацией CyberPeace Institute, базирующейся в Швейцарии.

Борьба с COVID-19 идет в сложных условиях — не только из-за опасности вируса, но и из-за киберпреступников, которые пользуются обстановкой. Злоумышленники всё чаще устраивают кибератаки на медучреждения, пытаясь парализовать их работу и подвергая опасности тысячи человеческих жизней. Весной этого года жертвами хакеров стали множество организаций, которые стремятся победить COVID-19: больницы, исследовательские лаборатории, государственные подрядчики и даже Всемирная организация здравоохранения (ВОЗ). В апреле количество атак на ВОЗ выросло в пять раз с момента начала пандемии.

На помощь медработникам по всему миру приходит CyberPeace Institute — международная организация по развитию безопасного цифрового пространства. В июне 2020 года организация запустила проект Cyber4Healthcare, задача которого — помочь организациям здравоохранения повысить уровень киберустойчивости с помощью сервисов, предоставляемых партнерами инициативы. Любые больницы, клиники, лаборатории, производители медоборудования и другие медицинские учреждения, участвующие в борьбе с COVID-19, могут обратиться в CyberPeace Institute за бесплатной помощью в укреплении своей киберзащиты. Инициативу поддержали такие организации, как Microsoft, Unisys, Global Cyber Alliance, CybExer Technologies, FIRST и другие. BI.ZONE стала первым российским партнером проекта…». ***(BI.ZONE поможет медучреждениям в борьбе с COVID-19 // IKSMEDIA.RU (http://www.iksmedia.ru/news/5669011-BIZONE-pomozhet-meduchrezhdeniyam.html). 03.06.2020).***

***

«Правительства по всему миру используют решения по коронавирусным технологиям, такие как приложения для отслеживания контактов и интеллектуальные термометры, для принятия решений о повторном открытии. Но эксперты предупреждают, что их защиты и защиты конфиденциальности не хватает - что может помочь хакерам скомпрометировать личную информацию людей.

Исследователи утверждают, что разработчики приложений не внедрили надежную цифровую защиту, стандартную для других технологий, работающих с конфиденциальной личной информацией или информацией о здоровье. Многие пересылают данные третьим сторонам, что означает, что личная информация

людей может использоваться для целевой рекламы или отслеживать их через другие, не связанные приложения.

«Одна вещь, которая происходит с [коронавирусом], заключается в том, что люди отдают еще больше своей информации в ответ на кризис или загружают приложение», - говорит Адам Шварц, старший юрист в Electronic Frontier Foundation, группе по защите конфиденциальности. , «Нам не нужна защита».

Многие из приложений используются для автоматизации какой-либо формы отслеживания контактов - процесса, который позволяет пользователям выяснить, был ли у них контакт с кем-то, зараженным коронавирусом. Пользователи самостоятельно сообщают, заражены ли они, и приложения используют либо данные о местоположении, либо анонимные сигналы Bluetooth для проверки связи с другими пользователями, которые могли находиться поблизости и подвергаться воздействию. Цель также состоит в том, чтобы предоставить правительствам информацию о местных уровнях заболеваемости.

Из 17 приложений для отслеживания контактов Android - из 17 разных стран - только у одной трети было базовое шифрование.

Это согласно исследованию от компании GuardSquare кибербезопасности.

А плохая безопасность и конфиденциальность могут влиять на эффективность приложений: эксперты предупреждают, что приложения не будут привлекать достаточно большую базу пользователей, чтобы их можно было использовать для отслеживания контактов, если пользователи не доверяют приложениям для защиты своей конфиденциальности. «Если вы хотите, чтобы большое количество пользователей внедряло и устанавливало или использовало, им придется доверять этим приложениям», - говорит Грант Гуд, главный научный сотрудник GuardSquare.

В конце концов, говорит Гуд, «если они недостаточно защищены ... они становятся привлекательной целью для хакеров».

Другие эксперты обеспокоены тем, что приложения обмениваются данными с третьими сторонами без явного понимания или согласия пользователей.

В результате расследования , проведенного Международным советом по цифровой ответственности, независимой некоммерческой организацией, занимающейся вопросами конфиденциальности и наблюдения за потребителями, базирующейся в Бостоне, было обнаружено восемь приложений для коронавирусов по всему миру, которые передают информацию третьим сторонам, таким как компания мобильной аналитики Branch, принадлежащая Google Crashlytics и Facebook.

Разработчики обычно сотрудничают с этими компаниями, предлагающими программное обеспечение, помогающее оптимизировать производительность приложения, например, для сбора аналитических отчетов или отчетов о сбоях. Однако во многих случаях третьи стороны также получают доступ к личной информации и телефонным данным, которые можно использовать для целевой рекламы.

«Обоснование обеспокоенности по поводу участия [стороннего программного обеспечения] в некоторых из этих связанных с covid приложений означает, что существует риск большего сбора информации, чем ожидают

пользователи», - говорит президент IDAC Квентин Палфри. «Это может подорвать общественное доверие к использованию некоторых из этих инструментов, что в общественном доверии очень важно для эффективности этой меры общественного здравоохранения».

Три американских приложения, которые, по мнению IDAC, отправляли данные третьим сторонам, предоставляли данные Android, специально предназначенные для целевой рекламы. Это были приложения для регистрации симптомов Kencor Covid-19, Care19 и приложение интеллектуального измерителя Kinsa.

Палфри и другие исследователи говорят, что этот вид обмена данными может быть уместен в коммерческом контексте, но поднимает красные флажки для приложений, которые используются в ответных мерах общественного здравоохранения.

Например, Kinsa собирает собираемые им данные о лихорадке людей, которые можно использовать для прогнозирования горячих точек, чтобы чиновники здравоохранения могли реагировать соответствующим образом. Компания уже распространила около 700 000 термометров среди пользователей во время пандемии коронавируса через партнерские отношения с девятью городами и штатами США. (Приложение также позволяет пользователям самостоятельно сообщать о случаях применения covid-19, хотя эта информация не передается за пределы приложения, которое использует данные для предоставления рекомендаций по состоянию здоровья.)

Кинса сообщила, что ранее не знала, что Branch получает данные, которые могут быть использованы для целевой рекламы, и запретила доступ для телефонов Android на прошлой неделе после отчета IDAC.

Но Kinsa по-прежнему обменивается данными пользователей iPhone, включая IP-адреса и информацию об устройстве, и компания заявила, что не сможет отключить эту функцию, не сделав приложение бесполезным на устройствах Apple.

Компания подчеркивает, что Kinsa не передает данные о состоянии здоровья или личную информацию, например адреса электронной почты, филиалам.

Но пока третьи стороны могут получать доступ к информации, такой как IP-адреса и сборка устройства, пользователи практически не могут запретить сторонним пользователям создавать цифровые отпечатки пальцев для них и отслеживать их через несвязанные приложения, говорит Патрик Джексон, технический директор по конфиденциальности Приложение Disconnect.me.

«Это черный ящик, - говорит он. - Недостатком для потребителей является то, что если у Branch когда-нибудь будет утечка данных, которую пользователь никогда не узнает».

Здоровое совместное приложение Юты собирает аналогичные данные.

Политика конфиденциальности для приложения, выдвигаемого должностными лицами здравоохранения в штате, гласит, что оно «собирает [ы] информацию о вашем мобильном устройстве или компьютерной системе, включая MAC-адрес, IP-адрес и идентификатор мобильного устройства» - все сигналы, необходимые для цифрового отпечаток пальца, о котором предупреждают такие исследователи, как Джексон.

Политика конфиденциальности приложения не указывает, какие третьи стороны получают эти данные и почему. Но представитель Twenty, разработчика приложения, говорит, что оно использует Firebase Analytics и Crashlytics для анализа производительности и показателей вовлеченности.

Это просто показывает, насколько трудно решить проблему, говорит Шварц из EFF. «Если им нужны сводные данные, они должны делать это таким образом, чтобы это защищало общественность и их конфиденциальность», - сказал Шварц. «Мы не возражаем против использования действительно агрегированных данных, но если [приложение] рассылает информацию брокерам данных, которыми владеет клиент, то это не совсем агрегированные данные».

Именно такие потенциальные пробелы в конфиденциальности надеются устранить члены Конгресса.

Обе стороны представили свои собственные версии законодательства, которые регулировали бы использование данных, собранных для ответа на коронавирус.

«Технологии могут помочь нашей стране победить пандемию covid-19, но когда технические продукты собирают какие-либо личные данные, связанные с пандемией, они должны использоваться только для целей общественного здравоохранения», - сказала член палаты представителей Анна Г. Эшу (D-Калифорния). который ввел в действие Закон о конфиденциальности в чрезвычайных ситуациях в области общественного здравоохранения , который установит меры предосторожности в отношении того, как компании, работающие над мерами реагирования на пандемию, собирают и обмениваются личными данными, включая IP-адреса.

«Американцы не хотят, чтобы эти данные передавались третьим сторонам, использовались для таргетинга рекламы, продавались брокерам данных или использовались для каких-либо целей, кроме улучшения общественного здравоохранения», - продолжил Эшу». ***(Tonya Riley. The Cybersecurity 202: Privacy experts say many coronavirus apps aren't doing enough to safeguard users' information // The Washington Post (https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/06/22/the-cybersecurity-202-privacy-experts-say-many-coronavirus-apps-aren-t-doing-enough-to-safeguard-users-information/5eefae20602ff12947e91075/). 22.06.2020).***

****

«По данным Check Point, число фишинговых атак, связанных с темой коронавируса, значительно выше в тех регионах, где режим самоизоляции не отменен. Так, в Европе и Северной Америке, где бизнес возвращается к нормальной жизни, наблюдается резкое сокращение числа атак, связанных с коронавирусом. В то же время в странах Латинской Америки и Африки, которые все еще борются со вспышкой, наблюдутся частые случаи воздействия на организации вредоносных атак, связанных с Covid-19.

Новые тренды

Несмотря на то, что число атак на почве коронавируса снижается с послаблением режима самоизоляции, мошенники используют иные крупные инфоповоды для своих атак. Доказательством этому служит правозащитное движение «Black Lives Matter». В начале июня, когда глобальные протесты достигли своего пика, исследователи Check Point обнаружили активное распространение вредоносной спам-кампании, связанной с данным движением. В рассылку был вложен текстовый документ с темой «Give your opinion confidentially about Black Lives Matter» («Выскажись анонимно о движении Black Lives Matter), «Leave a review anon about Black Lives Matter» (Оставь анонимный отзыв о движении Black Lives Matter), «Vote anonymous about Black Lives Matter» («Отдай свой голос в поддержку движения Black Lives Matter»). В каждом из этих файлов был зашит банковский троян Trickbot.

«Если вы получаете письмо от неизвестного отправителя, будьте осторожны. Открыв вложение или кликнув по ссылке внутри, можно автоматически скачать вредоносный файл. Сейчас мы наблюдаем тенденцию в использовании для фишинговых атак такие доменные имена, как Microsoft Office 365. Они вызывают меньше подозрений у потенциальной жертвы, — рассказывает Василий Дягилев, глава представительства Check Point Software Technologies в России и СНГ. — Несмотря на то, что режим самоизоляции в некоторых регионах сходит на нет, число кибератак в ближайшем будущем будет только расти. Пандемия коронавируса стала катализатором другого глобального процесса — киберпандемии».

Динамика киберпреступности

По данным Check Point, количество еженедельных атак увеличилось в июне на 18% в сравнении с средним показателем мая. Тем не менее, количество атак, связанных с коронавирусом, сокращается. Так, в первую неделю июня мы зафиксировали 129 796, что на 24% меньше, чем ранее в мае. Кроме того, в первые две недели июня было зарегистрировано 2451 новых доменов, связанных с коронавирусом. Из них 4% (91) были признаны вредоносными и 3% (66)— подозрительными.

Как обезопасить компанию и сотрудников

1. Если в электронных письмах от незнакомых отправителей или на сайтах из этих писем содержатся ошибки, стоит насторожиться и внимательно проверить домен, с которого пришло письмо.

2. Будьте осторожны письмами, полученными по электронной почте от неизвестных отправителей, особенно если их автор запрашивает совершение определенного действия, которое вы обычно не делаете.

3. Убедитесь, что вы заказываете товары из оригинального магазина: не нажимайте на рекламные ссылки и баннеры в электронных письмах, вместо этого найдите нужный вам магазин в поисковой системе, которой вы привыкли пользоваться.

4. Остерегайтесь «специальных» предложений. «Эксклюзивное лекарство от коронавируса за 150 долларов» обычно не является надежной или заслуживающей доверия покупкой. На данный момент лекарство от коронавируса не существует, и даже если бы оно было, вы вряд ли узнали бы об этом по электронной почте.

5. Убедитесь, что вы везде используете уникальные сложные пароли». ***(Среднее число кибератак в неделю выросло на 18% // IKSMEDIA.RU (http://www.iksmedia.ru/news/5678998-Srednee-chislo-kiberatak-v-nedelyu.html). 29.06.2020).***

***

«…Отслеживание COVID-19 с помощью Интернета вещей может поставить вашу частную жизнь под угрозу. Прямо сейчас мы создаем инструменты общественного, рабочего и домашнего наблюдения не спрашиваем согласия перед их внедрением. Датчики, используемые на рабочих местах и дома, могут отслеживать звук, температуру, заполняемость пространства и движение, чтобы понять, что делает человек и какова окружающая его среда. Многие устройства оснащены камерами и микрофонами, которые дают обратную связь в облачный сервис.

В облаке хакеры могут получить доступ к изображениям, разговорам и сигналам окружающей среды. Помимо того просто подключенное устройство открывают сотрудникам компании-производителя окно в личную жизнь пользователей.

Для некоторых проблема с электронным наблюдением заключается только в том, что они не хотят создания записей о них. Для других это может представлять угрозу благополучию, поскольку правительство США всё чаще использует распознавание лиц и пытается собрать большие массивы электронных данных с помощью широких ордеров.

Как компании должны думать о согласии Интернета вещей? Прозрачность важна: любая компания, продающая подключённое устройство, должна видеть наперёд его возможности и то, что происходит с данными с устройства. Информирование пользователя — это первый шаг.

Компании также должны поощрять пользователей в информировании окружающих. Это может быть простая наклейка, предупреждающая посетителей о том, что дом находится под видеонаблюдением. А может — уведомление в приложении с просьбой объяснить возможности устройства соседям по дому или близким. Такое уведомление не поможет тем, чьи домочадцы используют подключённые устройства для абьюза и контроля, но оно напомнит любому, кто устанавливает устройство в своем доме, что девайс потенциально может следить.

Согласие может создать доверие к продукту или автоматизированной системе. Например, AdventHealth Celebration, больница в Орландо (штат Флорида) внедрила решение для отслеживания медсестер, которое мониторит их действия во время смены, чтобы определить оптимальные процессы в работе. Celebration не просто запустила систему, но прежде проинформировала медсестер, а потом обсудила с ними полученные результаты.

Мониторинг помог больнице изменить распределение пациентов по палатам таким образом, чтобы пациенты с высокими потребностями не находились рядом друг с другом и под крылом одной медсестры.

Привлечение медсестёр с самого начала имело решающее значение для успеха. Города, внедряющие распознавание лиц в школах или аэропортах, не

спрашивая об этом граждан, должны бы обратить внимание на успех системы Celebration. Неспособность спросить или проинформировать граждан свидетельствует о явном отсутствии озабоченности по поводу согласия.

Это означает, что наши правительства не стремятся к уважению и общению с людьми. И если это верно для правительств, то технологические компании это ли послание хотят отправить клиентам?» ***(Stacey Higginbotham. The Internet of Things Has a Consent Problem // IEEE Spectrum (https://spectrum.ieee.org/telecom/security/the-internet-of-things-has-a-consent-problem). 18.06.2020).***

***

«В начале июня нынешнего года операторы вымогательского ПО Netwalker атаковали Калифорнийский университет в Сан-Франциско (UCSF). Ведущее медицинское исследовательское учреждение, работающее над лекарством от COVID-19, приняло решение заплатить киберпреступникам выкуп в размере $1,14 млн.

Как сообщило издание BBC News, руководство университета вело переговоры с преступниками в даркнете. На первый взгляд, домашняя страница Netwalker в даркнете выглядит как обычный web-сайт обслуживания клиентов, с вкладкой часто задаваемых вопросов (FAQ), предложением «бесплатного» образца своего программного обеспечения и возможностью чата в реальном времени. Но там также есть специальный таймер, отсчитывающий время, когда хакеры либо удваивают цену своего выкупа, либо удаляют похищенные данные.

Представители UCSF вышли на связь с вымогателями и сначала попросили выделить больше времени и информации о взломанных данных. Отметив, что UCSF зарабатывает миллиарды в год, хакеры сначала потребовали $3 млн. Представитель UCSF пояснил, что пандемия коронавируса была «финансово разрушительной» для университета, и попросил их принять $780 тыс. После дня двусторонних переговоров UCSF собрала все имеющиеся деньги и могла заплатить $1,02 млн, но преступники отказались снижать размер выкупа ниже $1,5 млн. Несколько часов спустя UCSF вернулся с окончательным предложением в размере $1 140 895. На следующий день сумма в размере 116,4 биткойнов была переведена на электронные кошельки Netwalker, а программное обеспечение для дешифрования данных было отправлено в UCSF.

UCSF в настоящее время сотрудничает с ФБР в ходе расследования, одновременно работая над восстановлением всех затронутых систем.

«Зашифрованные данные являются важными для некоторой академической работы, которую мы проводим в университете ради общего блага. Поэтому мы приняли трудное решение выплатить часть выкупа, примерно $1,14 млн лицам, стоящим за кибератакой в обмен на инструмент для разблокировки систем и возврата полученных данных», — пояснили представители UCSF». ***(Обнародованы подробности переговоров Калифорнийского университета с операторами Netwalker // SecurityLab.ru (https://www.securitylab.ru/news/509557.php). 29.06.2020).***

***

«Секретар Ради національної безпеки і оборони України Олексій Данілов провів зустріч із Надзвичайним і Повноважним Послом Великої Британії в Україні Меліндою Сіммонс. Під час зустрічі сторони обговорили поточну безпекову ситуацію в Україні та світі, зокрема, в контексті російської агресії на Сході України, а також розширення співпраці у сфері кібербезпеки. Про це повідомляє УНН з посиланням на пресслужбу РНБО.

Так, торкаючись питання кібербезпеки, Данілов зазначив, що "наявність ядерної зброї сьогодні не є запорукою безпеки держав, а боротьба переноситься у кіберпростір, і ми маємо бути готові до цих викликів".

"Україна щодня відбиває кібератаки з сусідньої країни, і ми розуміємо, що цей кібернаступ буде спрямований не лише на Україну, але й на інші держави", - сказав секретар РНБО, додавши, що Україна готова ділитися цим досвідом зі своїми стратегічними партнерами.

У свою чергу, Сіммонс запевнила у незмінності підтримки України у її боротьбі за відновлення суверенітету та територіальної цілісності.

Вона висловила готовність Великої Британії надавати Україні підтримку, зокрема, під час розробки національної стратегії кібербезпеки, а також поглиблювати співпрацю у напрямку розбудови кібербезпекових спроможностей.

Повідомляється, що сторони домовились про подальшу активізацію співробітництва між державами…». ***(Наталія Рябцева. Данілов зустрівся з послом Великої Британії в Україні: про що говорили // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1874216-danilov-zustrivsya-z-poslom-velikoyi-britaniyi-v-ukrayini-pro-scho-govorili). 10.06.2020).***

***

«Міністерство оборони США повідомило про виділення військової підтримки Україні у розмірі 250 млн американських доларів. Ця допомога є кроком у розвитку американо-українського співробітництва, у якому важлива роль надається протистоянню агресії Російської Федерації…

Передбачається, що американська допомога покращить ситуацію у воєнно-морському флоті та з системами спостереження за повітряним простором, посприяє зростанню боєздатності сухопутних військ і ефективності медичної допомоги. Також окремим напрямком співробітництва стане сфера протидії кібератакам». ***(Пентагон виділить Україні чверть мільярда військової допомоги - "Важливому партнеру у протистоянні з Росією" // Знай.ua (https://chronicle.znaj.ua/317169-pentagon-vidilit-ukrajini-chvert-milyarda-viyskovoji-dopomogi-vazhlivomu-partneru-u-protistoyanni-z-rosiyeyu). 12.06.2020).***

***

«Секретарь Совета национальной безопасности и обороны Украины Алексей Данилов провел встречу с послом Японии в Украине Такаши Кураи. Они обсудили вопросы совместных долгосрочных экономических проектов и привлечения для их реализации соответствующих инвестиций, в частности, углубление сотрудничества между ведомствами по вопросам безопасности двух государств в области кибербезопасности. Об этом сообщает СНБО. 11 июня 2020 года состоялась встреча секретаря Совета национальной безопасности и обороны Украины Алексея Данилова с чрезвычайным и полномочным послом Японии в Украине Такаши Кураи…

Алексей Данилов отметил, что развитие партнерских отношений с Японией является важным элементом внешней политики Украины, имеющий целью дальнейшее углубление политического диалога и укрепления торгово-экономических отношений. “Кибербезопасность является дополнительной сферой двустороннего сотрудничества между Украиной и Японией, в которой мы могли бы добиться успеха”, — добавил Алексей Данилов…». ***(Данилов встретился с послом Японии в Украине: обсудили совместное сотрудничество в кибербезопасности // Информационный портал "ua.today" (http://ua.today/news/politics/danilov_vstretilsya_s_poslom_yaponii_v_ukraine_obsudili_sovmestnoe_sotrudnichestvo_v_kiberbezopasnosti). 12.06.2020).***

****

«Естонська Академія електронного управління (eGA) у співпраці з Мінцифри розпочала діяльність з удосконалення рівня кібербезпеки в установах українського державного сектору…

"Особливий фокус - на підвищенні спроможності державних органів щодо оцінювання безпеки своїх інформаційних систем та на впровадженні необхідних процедур тестування на безпеку.

У рамках проєкту "Підготовленість до кібербезпеки в українських державних органах влади" кібер-фахівці eGA допомагатимуть українським колегам у розробці, введенні в експлуатацію та проведенні тестів на безпеку та у навчанні керівників задля покращення розуміння ними необхідності таких тестувань", - йдеться у повідомленні.

Під час проєкту відібрані органи державної влади проведуть одноразові тестування критично важливих систем. За результатами тестів власники таких систем зможуть вжити належних заходів для запобігання реальним кібератакам.

eGA - некомерційна консалтингова організація. З 2002 року налагодила співпрацю з організаціями з більш ніж 130 країн і провела навчання для понад 4500 посадових осіб.

Починаючи з 2012 року, Академія електронного урядування допомагає розвивати сферу електронного урядування в Україні та проводить форуми для IT-директорів». ***(Естонська компанія займеться кібербезпекою українських держорганів // Економічна правда (https://www.epravda.com.ua/news/2020/06/22/662122/). 22.06.2020).***

****

«Декан Юридичного факультету Ірина Сопілко та доцент кафедри цивільного права і процесу Валерія Філінович провели онлайн-зустріч зі співзасновником Академії Кібербезпеки CSA (Грузія), головою правління неурядової організації «Internet Development Initiative» Владімєром Сванадзе.

Сторони наголосили на важливості розвитку співпраці між університетами щодо запровадження спільних навчальних програм (курсів), проведення спільних круглих столів, майстер-класів та семінарів, що сприятиме підготовці висококваліфікованих юристів у галузі кібербезпеки та протидії кіберзлочинам.

Обговорено питання підписання Меморандуму про міжнародне співробітництво між Національним авіаційним університетом та Академією Кібербезпеки CSA і Меморандуму про співробітництво між НАУ та неурядовою організацією «Internet Development Initiative».

За результатами онлайн-зустрічі досягнуто домовленостей про спільну організацію науково-методичних заходів та участь студентів нашого університету у грантових програмах. Вже у вересні представники Академії Кібербезпеки CSA проведуть для студентів ЮФ НАУ перший вебінар щодо протидії кіберзлочинам». ***(Початок співпраці з Академією Кібербезпеки CSA Грузії // Національний авіаційний університет (https://nau.edu.ua/ua/news/2020/cherven/pochatok-spivpratsi-z-akademieyu-kiberbezpeki-csa-gruzii.html). 25.06.2020).***

***

Світові тенденції в галузі кібербезпеки

«…Корпоративные клиенты Zoom получат доступ к разработанному к настоящему моменту сервису сквозного шифрования, пишет Bloomberg. Однако обеспечение такого уровня конфиденциальностью, не позволяющей расшифровывать сообщения третьими лицами, не распространится на обычных пользователей, заявил основатель компании Эрик Юань. «Мы хотим работать вместе с ФБР и местными правоохранительными органами в случае, если некоторые люди используют Zoom в плохих целях», — сказал он.

В настоящее время у Zoom есть 769 корпоративных клиентов, которые потратили более 100 тыс. долл. на продукты сервиса за последние 12 месяцев, что двое больше, чем год назад. Компания сообщила о резком росте продаж за три месяца, закончившихся 30 апреля. Продажи в текущем квартале составят 500 млн долл. В целом сервис рассчитывает получить в этом финансовом году до 1,8 млрд долл. , что почти втрое превышает размер бизнеса в прошлом году. Zoom, согласно собственным данным, завершил квартал с примерно 265 400 клиентами, что в четыре раза больше, чем за аналогичный период годом ранее.

Ранее рост популярности Zoom на фоне пандемии коронавируса обнажил дыры в безопасности компании. Тролли вторгались на видеоконференции, распространяли порнографию и выкрикивали слова ненормативной лексики или дискриминационные расовые эпитеты. Явление получило название Zoombombing. Компания создала инструменты для предотвращения виртуальных атак, такие как пароли и залы ожидания перед входом в конференцию.

Также имели место случаи, когда звонки направлялись через серверы в Китае, хотя на его территории не было ни одного участника. Помимо этого иногда метаданные при входе пользователей в систему отправлялись в Facebook Inc. Компания положила конец обеим практикам и пообещала улучшить конфиденциальность по всем другим вопросам в течение трех месяцев. Для этого Zoom купил компанию по безопасному обмену сообщениями Keybase и нанял экспертов по кибербезопасности для управления своими действиями в этой области…». ***(Zoom: «Хотим работать вместе с ФБР, сквозного шифрования не будет для обычных пользователей» // РосКомСвобода (https://roskomsvoboda.org/59522/). 03.06.2020).***

***

«Компания Check Point® Software Technologies Ltd. объявляет результаты исследования, в котором компании рассказывали о своем опыте обеспечения безопасности во время самоизоляции и делились приоритетами и опасениями о возможных проблемах по возвращении в нормальную жизнь.

Более 86% респондентов заявили, что их основной задачей во время пандемии стала организация безопасного удаленного доступа и обеспечение безопасности VPN соединений. В опросе приняли участие более 270 специалистов из области информационных технологий и информационной безопасности по всему миру. Основные результаты представлены ниже:

Главные сложности в обеспечении безопасности в начале пандемии. Когда в начале пандемии компании переводили сотрудников на удаленную работу, больше всего беспокойства вызывало обеспечение безопасного удаленного доступа и VPN - так ответили 62% респондентов. 47% опрошенных сообщили, что были обеспокоены вопросом предотвращения атак с использованием методов социальной инженерии, а 52% назвали одним из основных вызовов защиту конечных точек и домашних Wi-Fi сетей сотрудников.

Возвращение к нормальной жизни. С введением послаблений режима самоизоляции в разных странах 75% опрошенных заявили, что их офисы снова открыты для ограниченного числа сотрудников. Однако в среднем четыре из пяти дней сотрудники работают удаленно. Это значит, что угрозы удаленного доступа будут актуальны в течение еще длительного времени.

Уязвимости удаленного доступа. В то время как 65% респондентов заявили, что их компании блокируют доступ внешних компьютеров к корпоративным VPN, только 29% сообщают о развертывании систем защиты конечных устройств сотрудников, лишь 35% проводят проверку соответствия требованиям. Более того 42% ИТ- и ИБ-специалистов отмечают, что в их компаниях проводится обучение сотрудников вопросам кибербезопасности. Это показывает, насколько организации обеспокоены стремительными кибератаками пятого поколения, нацеленными на удаленных сотрудников.

Приоритеты в обеспечении безопасности после карантина. 79% респондентов заявили, что их главным приоритетом является усиление защиты и оперативное предотвращение атак, поскольку многие сотрудники продолжают работать в удаленном режиме. Более того, 43% опрошенных заявили, что

планируют внедрить решения для безопасности мобильных устройств, а 39% намерены консолидировать свои системы безопасности, чтобы устранить «слепые зоны» в новом расширенном периметре сети.

Угрозы безопасности на ближайший год. Более 75% респондентов выразили обеспокоенность ростом числа кибератак, в том числе с использованием фишинга и методов социальной инженерии. 51% специалистов заявили, что наибольшая угроза исходит от домашних устройств, 33% видят основную угрозу безопасности в мобильных устройствах сотрудников.

«Еще до введения режима самоизоляции многие компании разрешили сотрудникам работать удаленно. Как только режим вступил в силу, у организаций не осталось другого выхода, как в кратчайшие сроки организовать удаленный доступ для всех своих сотрудников. Безусловно, эти меры привели к возникновению новых возможностей для осуществления атак злоумышленниками, — рассказывает Василий Дягилев, глава представительства Check Point Software Technologies в СНГ. — Несмотря на то, что сейчас мы постепенно возвращаемся к прежней жизни, угроза кибератак отнюдь не снижается. Компаниям необходимо использовать комплексные решения для обеспечения безопасности нулевого дня, чтобы не пострадать от лавины кибератак нового поколения».

В апреле компания Check Point провела исследование, которое показало, что во время масштабирования своих систем и перевода сотрудников на удаленную работу многие организации подверглись участившимся атакам на почве коронавируса. Так, 71% респондентов сообщили об увеличении числа кибератак в феврале и марте 2020 года. 95% опрошенных заявили, что столкнулись с дополнительными проблемами ИТ-безопасности, связанными с обеспечением крупномасштабного удаленного доступа сотрудникам, а также управлением использования теневых ИТ». ***(Исследование Check Point: 75% специалистов обеспокоены ростом числа кібератак // IGate (https://igate.com.ua/news/24557-issledovanie-check-point-75-spetsialistov-obespokoeny-rostom-chisla-kiberatak). 11.06.2020).***

****

«Представлено масштабное исследование предпочтений системных администраторов, сетевых инженеров и самозанятых технических специалистов в области защиты сетевой инфраструктуры от кибер-угроз, проведенное по заказу российского представительства компании Zyxel Networks.

В опросе, проведенном в мае 2020 года, приняло участие 1804 специалиста из России и других стран постсоветского пространства.

Участникам опроса было предложено указать способы защиты своей сети, марку установленного в сети межсетевого экрана и перечислить функциональность, работающую на устройствах. При этом респондентам не раскрывалось, кто является заказчиком исследования.

Прежде всего мы выяснили какие средства используются для защиты сети. У 52% респондентов работает программная защита. Исключительно аппаратные компоненты используют 22% ответивших, облако используется в 7% случаев. 12%

применяют комбинацию из первых трех средств. Интересно, что 8% ответивших никак не защищают сеть от угроз.

Затем мы перешли непосредственно к перечислению марок используемого оборудования. Cisco является предпочтительным производителем для 33% ответивших, Zyxel – 13%, и замыкает тройку лидеров Huawei с 11%:

По данным исследования компании IDC в 2019 году мировой рынок устройств кибер-безопасности вырос на 9.4% по сравнению с 2018 годом и достиг объема в $4.8 миллиарда. Отгрузка в штуках также увеличилась: рост составил 21% до 1,3 миллионов устройств.

При этом, в исследовании J'son & Partners Consulting, касающегося исключительно России, проведенного в период с 2016 по 2018 год, отечественный рынок межсетевых экранов прибавил за это время лишь 10% в рублевом выражении, достигнув в 2018 году уровня чуть более 15 млрд. руб. в ценах вендоров.

Результаты по производителям прокомментировал руководитель канального направления Zyxel Networks Россия и СНГ Дмитрий Танюхин: «Несмотря на то, что 1804 участника исследования являются более-менее репрезентативной выборкой, я был приятно удивлен, увидев Zyxel на втором месте, между такими гигантами индустрии как Cisco и Huawei, опережая именитых CheckPoint, Fortinet и других. Несомненно, этому способствовала плодотворная работа Zyxel в регионе на протяжении более, чем 20 лет. И средства сетевой безопасности были и однозначно остаются в фокусе производителя в последние 10 лет».

Следующий вопрос, предложенный участникам опроса, касался набора функций, выполняющихся на устройствах. Три первых места поделили файрвол – 23%, обнаружение и предотвращение вторжений – 11% и антивирус с 10%:

Вместе с тем стало интересно, какие функции чаще всего используют те, кто предпочитает программную защиту или использует ее вместе с аппаратной. Здесь положения лидеров сохранились: антивирус – 22%, файрвол – 17% и замкнул тройку антиспам с 13%:

Те же, кто указал использование облачных сервисов предпочитают использовать аналогичные функциями: антивирус – 12%, антиспам – 11%, файрвол – 11%:

В целом результаты по трем категориям защит совпадают. Антивирус и файрвол активно применяются во всех трех случаях. При этом антивирус - лидер у поклонников ПО и облака. Однако при использовании аппаратных компонентов специалисты вместо антиспама предпочитают IDP функционал.

Цифры мы попросили прокомментировать специалиста в сфере информационной безопасности, автора книги «Наблюдайте, потом используйте» Владимира Иванова: «У российского бизнеса несколько специфичный взгляд на проблемы безопасности. Исходя из моего опыта, если в компании отсутствует выделенная служба ИТ-безопасности, то у большинства системных администраторов едва хватает времени и сил на установку антивируса и файрвола с настройками по умолчанию.»

«Большая часть времени у ИТ службы по-прежнему уходит на выполнение заявок, имеющих очень слабое отношение к ИТ-безопасности. Например,

пересадка пользователей или «консультации по использованию ПО», - добавляет Владимир Иванов.

Далее мы попросили респондентов определить свое положение в компании. Больше всего, 33%, оказались индивидуальными предпринимателями или самозанятыми. 23% - трудятся в компаниях от 10 до 100 человек, 20% - в компаниях 500+ человек, 17% обслуживают сети предприятий 100-500 человек и 8% - организации до 10 человек:

При этом 33% самостоятельно принимают решение о закупке оборудования, 40% могут советовать, что купить руководству и 27% никак не влияют на этот процесс:

Владимир Иванов продолжает: «Большинство руководителей компаний до момента нанесения существенного ущерба не хотят уделять внимание безопасности. Аргументы из серии: «А кому мы нужны?», «У нас честный бизнес, нам скрывать нечего!», — по-прежнему превалируют над осторожностью и здравым смыслом. А если для обеспечения этой самой безопасности надо потратить дополнительные деньги… тут вероятнее всего последует отказ. Поэтому приобретение антивируса и самого простого файрвола (вариант «возьмем старый сервер и что-нибудь на него поставим» — по-прежнему в силе) — это предел заботы о безопасности для многих российских компаний.»

«В некоторых случаях гораздо большее внимание уделяется локальным средствам защиты, например, блокировке USB-портов с целью препятствования использования флеш-накопителей, шифрование томов для хранения данных и так далее. Также неоправданно большой интерес вызывает контроль действий пользователей на рабочих местах, перемещений пользователя (включая учет соблюдения рабочего графика), перлюстрация переписки и контроль посещения Интернет-сайтов. У меня остается ярко выраженное впечатление, что в сознании российских руководителей до сих пор сохраняется советский образ мышления, и для них поиск «внутреннего врага» важнее технологического отставания. Разумеется, нельзя распространять какой-либо опыт на все организации. Существуют высокотехнологичные компании с технически грамотным руководством, где уделяют пристальное внимание всем аспектам ИТ-безопасности», - резюмирует Владимир Иванов.

В заключении выяснили, что для 54% ответивших важна поддержка производителя на русском языке, а 46% не считают это важным.

В этой связи интересным будут результаты исследования, проведенного по заказу Zyxel в январе 2019 года, на котором респондентам был задан только один вопрос: «При выборе производителя сетевого оборудования какие ПЯТЬ критериев из перечисленных вы считаете наиболее важными для принятия решения?»

«Позиции Zyxel усилились с появлением в линейке шлюзов серии ATP с функционалом так называемой «песочницы», позволяющей предотвращать «угрозы нулевого дня». Вышедшие на рынок в мае 2020 года решения USG FLEX являются обновлением зарекомендовавших себя ZyWALL USG, получившие более быструю аппаратную и программную платформу и более гибкую систему подписок. С 2021 года в этих шлюзах будет доступно не только локальное, но и облачное управление. Мы будем стараться удержаться на достигнутой высоте и постоянно

предлагать нашим клиентам самые современные решения по защите сетей», - сказал Дмитрий Танюхин в заключении.

Так же итоги своими мыслями по результатам исследования поделился Игорь Калинкин, продакт-менеджер компании Treolan: «У Zyxel хорошо налажена поддержка проектов, что позволяет нашим партнерам зарабатывать. Вендор активно развивает профессиональное сообщество, проводит вебинары, в том числе и технические. Я не удивлен, что производитель оказался в тройке лидеров по результатам исследования, ведь на его решениях можно построить достаточно серьезную систему информационной безопасности для предприятий и офисов разного уровня.» ***(Облачные сервисы для защиты сети от киберугроз по-прежнему непопулярны в России // IKSMEDIA.RU (http://www.iksmedia.ru/news/5669826-Stali-dostupny-rezultaty-masshtabno.html). 08.06.2020).***

***

«Развитие интернет-сферы приводит к новым вызовам – киберпреступлениям. Специалисты рассказали "ПолитЭксперту", как можно обезопасить себя от мошенников в Сети и не отказывать себе в онлайн-покупках…

След коронавируса

Количество киберпреступлений в России выросло на 85%. Использование мошенниками пластиковых карт – в шесть раз. Ежегодно рост киберпреступности составляет примерно 70%. Эта тенденция прослеживается с 2013 года, заявил генеральный директор компании "Интернет-розыск" Игорь Бедеров в интервью корреспонденту "ПолитЭксперта". За шесть лет количество преступлений в Сети выросло в 25 раз.

"В прошлом году 14,5% от всего числа преступлений в стране было совершено при помощи современных технологий. В 2020 году это будет уже около 30%. Раскрываемость же киберпреступлений постоянно снижается. В 2019 было раскрыто и передано в суд только 23% таких дел", – рассказал собеседник ПЭ.

Сейчас сложилась очень благоприятная среда для киберпреступлений, добавил российский разработчик ПО Иван Панченко. Онлайн-торговля на сегодняшний день переживает бум – многие компании не успевают адаптировать и модернизировать свои системы.

"С другой стороны, многие только делают первые шаги в онлайне и пока не обладают необходимыми навыками защиты, а также не понимают, почему подобные услуги и специалисты стоят так дорого", – уточнил сооснователь Postgres Professional.

Ограничения на фоне коронавируса также сыграли свою роль. Компании, которым в срочном порядке пришлось переводить работников на дистанционный режим работы, о защите конфиденциальной информации и персональных данных даже не задумывались. С опытом рынок адаптируется, считают специалисты.

Цифровая грамотность

Немаловажно, что киберпреступления стали предметом пристального внимания руководства правоохранительных органов, отметил член Комиссии по

правовому обеспечению цифровой экономики Московского отделения Ассоциации юристов России Борис Едидин. В прошлом году о создании специализированных подразделений по борьбе с киберпреступлениями заявили в Следственном комитете и в МВД.

"Защита от киберпреступлений в обществе – это повышение "цифровой грамотности". Индивидуально – необходимо пользоваться только проверенными сайтами, не поддаваться соблазнам сказочной выгоды или распродаж по невероятно низким ценам. Крайне осторожно надо подходить к предоставлению своих данных на сайтах. Подумайте, оправдано ли требование ваших персональных данных, номера или пин-кода банковской карты и других", – поделился Едидин.

Простой, но эффективный способ обезопасить свои деньги, предложил начальник отдела информационной безопасности Концерна "Автоматика" Госкорпорации Ростех Сергей Буларга. С этой целью достаточно завести банковскую карту для проведения транзакций с установленным лимитом расходования средств на необходимые покупки и поддерживать баланс карты на нуле, когда она не используется.

"Любой сайт может быть небезопасен, за исключением ресурсов, защищенных такими средствами, как TLS (Transport layer security) и WAF (Web application firewall). При этом речь идет о защите самого ресурса, а не устройства конечного пользователя. Сами пользователи могут выявить сомнительные сайты с помощью антивирусных программ", – добавил специалист.

В руки киберпреступников попали инструменты правительственных хакеров и инструменты манипуляции уязвимостью спецслужб, заявил директор по инфобезопасности холдинга TalentTech Иван Дмитриев. Если злоумышленник проник в информационный периметр, то он попытается остаться незамеченным и закрепиться там.

"Чтобы защитить себя, бизнесу нужно применять системный подход. Выстраивать эшелонированную и адаптивную систему защиты информации, постоянно развивать и совершенствовать ее", – подчеркнул эксперт.

Понимание кибербезопасности – один из ключевых навыков у сотрудников в 2020 году. Многие работодатели начали обучать этому свои команды. Главное – не отставать от киберпреступности ни на шаг. Основная сложность – это защита размытого информационного периметра. Легко контролировать только объект на расстоянии вытянутой руки.

"Никакая, даже самая технологичная, система защиты информации не сможет устоять под натиском действий сотрудников, которые не обладают диджитал-навыками и не соблюдают правила цифровой гигиены. От современного хакера защититься только техническими мерами невозможно", – предостерег Дмитриев.

Главное – быть бдительным

Защититься от нападений мошенников не всегда возможно – слишком много схем применяют специалисты, объяснил разработчик ПО Иван Панченко. По данным экспертов по кибербезопасности Cybersecurity Ventures, в 2019 году кибератаки совершались каждые 14 секунд. И темпы продолжают расти.

"Сфера интересов киберпреступников, с которыми сталкиваются пользователи, – мошенничество, кражи, незаконное распространение материалов, финансовые махинации", – перечислил собеседник ПЭ.

Главное – всегда сохранять бдительность. Социальная инженерия, получение конфиденциальной информации и фишинг, получение логина и пароля, – распространенное явление в интернете. Панченко перечислил семь правил, соблюдение которых поможет обезопасить себя от киберпреступников. Так, необходимо внимательно проверять URL-адрес. Злоумышленники изменяют расширение, например, com вместо ru, или заменяют буквы похожими цифрами. Также замечать наличие в протоколе https.

"S означает "secure" – передачу данных между сервером и сайтом по защищенным каналам", – пояснил разработчик ПО.

В браузере следует отключить автоматическую загрузку файлов, отслеживание, проверить настройки безопасности и конфиденциальности. Использовать сервис VirusTotal для проверки наличия угроз на сайте.

"Установите системы защиты сети – например, Avast с системой антифишинга. И узнайте, есть ли у вашего антивируса сертификат защиты от фишинга. Проверьте наличие обязательной информации на сайте – политики конфиденциальности", – обозначил эксперт.

И последнее – всегда можно установить владельца сайта при помощи сервиса WHOIS, где указывается информация вплоть до даты регистрации домена, подвел итог Иван Панченко…» ***(Ксения Емельянова. Специалисты посоветовали, как избежать встречи с кибермошенником // Политическая експертиза (https://politexpert.net/201463-specialisty-posovetovali-kak-izbezhat-vstrechi-s-kibermoshennikom). 19.06.2020).***

***

«Корпорация IBM сообщила, что покупает программные активы стартапа Spanugo, разработчика средств обеспечения кибербезопасности, автоматизирующих выявление, анализ угроз и защиту от них.

Новое приобретение IBM планирует использовать для улучшения безопасности своего публичного облака финансовых сервисов. Эта готовящаяся к выходу платформа была анонсирована в прошлом году. Её задача заключается в том, чтобы помогать клиентам из отрасли финансовых услуг обеспечивать соответствие стандартам и нормативным требованиям, безопасность и стабильность своего бизнеса.

Возможности определять профили соответствия, управлять средствами контроля и в режиме реального времени отслеживать соблюдение в рамках всей организации будут сосредоточены в центре управления безопасностью, который, по словам IBM, станет доступен клиентам раньше, чем было запланировано, благодаря активам, которые предоставит Spanugo…». ***(IBM дополнит публичное облако финансовых сервисов технологиями Spanugo // Компьютерное Обозрение (https://ko.com.ua/ibm_dopolnit_publichnoe_oblako_finansovyh_servisov_tehnologiyami_spanugo_133402). 16.06.2020).***

****

«Не в первый раз определенные технические термины называют устаревшими и откровенно расистскими. Поскольку протесты Black Lives Matter охватили США и даже расширились за ее пределы, некоторые на их фоне требуют, чтобы в технической отрасли и программировании такие слова, как blacklist, whitelist, Master/Slave ("хозяин и раб"), были немедленно изменены на менее оскорбительные.

Термин blacklist ("черный список") зачастую используется для описания списка, содержащего запрещенные или нежелательные элементы, такие как пароли, электронные письма со спамом, веб-сайты, приложения, телефонные номера и т.д. Некоторые считают этот термин откровенно "расистским", так как whitelist ("белый список") описывает все, что разрешено или хорошо, передает segodnya.ua.

Для опытных технических специалистов и программистов такие требования могут показаться откровенно странными. Но некоторые компании прислушались к требованиям. К примеру, Британский национальный центр кибербезопасности уже запретил термины blacklist и whitelist. Следом в Google тоже перестали использовать такие неэтические слова в браузере Chrome.

Термины master и slave были популярными среди системных администраторов и компьютерных энтузиастов на протяжении десятилетий. Они также являются частью терминологии в отрасли хранения баз данных, записи музыки, программного обеспечения, транспорта и многого другого. Как отмечает CNET, разработчики Python отказались от этих слов в 2018 году, а команда Drupal заменила их на primary/replica ("основной и реплика") в 2014 году. В 2013 году округ Лос-Анджелес попросил поставщиков и подрядчиков прекратить использование master и slave в компьютерном оборудовании.

Смерть Джорджа Флойда и последующие протесты Black Lives Matter подняли проблему использования неэтических слов в разных сферах. Некоторые считают, что проблема преувеличена, но сторонники замены слов на более толерантные уверены, что такая практика окажет положительный эффект». ***(В США запретили "расистские" термины в программировании // Вести-UA (https://vesti-ua.net/novosti/tehnologii/148047-v-ssha-zapretili-rasistskie-terminy-v-programmirovanii.html). 15.06.2020).***

****

Сполучені Штати Америки

«Более десятка американских чиновников направили письмо калифорнийскому провайдеру сетевых решений и решений для кибербезопасности Juniper Networks с целью спросить компанию о результатах расследования, начатого в 2015 году после обнаружения бэкдора в ее продуктах, сообщило издание SecurityWeek.

В конце 2015 года Juniper Networks в ходе проверки обнаружила неавторизованный код в операционной системе ScreenOS, послуживший причиной

появления двух уязвимостей (CVE-2015-7755 и CVE-2015-7754), позволяющих злоумышленникам удаленно получить доступ с правами администратора к устройствам Juniper NetScreen и расшифровать VPN-трафик.

Вторая проблема была связана с использованием Dual Elliptic Curve Deterministic Random Bit Generator (Dual EC DRBG), который ScreenOS использовал в качестве генератора псевдослучайных чисел. Dual EC DRBG содержала бэкдор, ответственность за появление которого предположительно лежит на Агентстве национальной безопасности США (АНБ).

«Прошло уже более четырех лет с тех пор, как Juniper Networks объявила о проведении расследования, однако компания до сих пор не сообщила, что именно она обнаружила. Американцы, а также компании и правительственные учреждения США, которые доверяли продуктам Juniper свои конфиденциальные данные, до сих пор не имеют информации о том, как Juniper допустила внедрение разработанного АНБ алгоритма шифрования с бэкдором», — сообщается в письме.

Власти предоставили Juniper Networks один месяц, чтобы ответить на восемь вопросов об инциденте, в том числе о решениях компании, касающихся Dual EC DRBG, результатах ее расследования, источнике несанкционированного кода, а также любых рекомендациях, сделанных и реализованных после исследования». ***(Власти США поинтересовались результатами расследования о бэкдоре в продуктах Juniper Networks // SecurityLab.ru (https://www.securitylab.ru/news/509165.php). 11.06.2020).***

***

«Согласно внутреннему отчёту бывшего директора ЦРУ Майка Помпео и его заместителя Джины Хаспел, в 2016 году из ЦРУ украли сверхсекретные компьютерные хакерские инструменты. Это стало результатом культуры на рабочем месте, в силу которой элитные компьютерные хакеры управления «отдавали приоритет созданию кибероружия за счет защиты своих собственных систем».

Процедуры обеспечения безопасности были «прискорбно слабыми», говорится в документе. Большинство чувствительных кибероружий не были разделены, пользователи делились паролями на уровне системных администраторов, эффективных средств управления съемными носителями не было, а исторические данные были доступны пользователям без ограничений по времени.

Хакерские инструменты были разработаны центром кибербразведки ЦРУ, где наиболее изощренные хакеры агентства разрабатывали способы получения доступа к труднодоступным сетям, чтобы, например, тайно активировать камеру и микрофон на планшете иностранного противника или украсть планы разработки передовых систем вооружения иностранного государства. По оценке оперативной группы было потеряно 34 Тбайт информации, или около 2,2 млрд страниц.

Нарушение, предположительно совершенное сотрудником ЦРУ, обнаружили только через год, когда информация о нём была опубликована WikiLeaks в марте 2017 года. Американские официальные лица заявили, что это была самая крупная утечка секретной информации в истории ЦРУ, в результате чего оно закрыло

некоторые разведывательные операции, а некоторые его иностранные противники узнали о шпионских методах органа.

Оперативная группа признала стремление заниматься растущими и критически важными потребностями миссии и слабость «повседневной практики обеспечения безопасности». Эти сотрудники управления находятся под постоянным давлением необходимости находить уязвимости в коммерческом программном обеспечении и других технологиях, сказал бывший сотрудник разведки, занимавший руководящую должность и знакомый с данными группы.

Внутренний отчёт был представлен в качестве доказательства в уголовном деле Джошуа Шульте, бывшего сотрудника ЦРУ, который обвиняется в краже хакерских инструментов и передаче их WikiLeaks.

Шульте не признал себя виновным, выводы оперативной группы помогли в его защите. Адвокаты Шульте утверждали на суде, что безопасность компьютерной сети была настолько плохой, что любой из сотен штатных или нанятых сотрудников мог иметь доступ к той же информации, что и Шульте.

В докладе говорится о разнице между «корпоративной информационно-технологической системой» ЦРУ, на которую приходится большая часть компьютерной сети управления, и специализированными «системами миссии», включая ту, в которой размещались хакерские инструменты.

Бывший сотрудник разведки в беседе с изданием сказал, что согласен с большинством выводов оперативной группы, но он возразил против утверждения, что ЦРУ не уделяло особого внимания компьютерной безопасности. Система миссии Центра располагалась в отдельном здании, а не в штаб-квартире ЦРУ, и доступ туда был строго ограничен, сказал он.

В 2014 году Конгресс дал Министерству внутренней безопасности полномочия требовать от федеральных органов соблюдения минимальных стандартов кибербезопасности, но освободил от этого разведку. Считалось, что хранители самых ценных секретов страны она будет проявлять дополнительную заботу о безопасности своих систем. «Теперь ясно, что освобождение разведывательных органов от базовых федеральных требований кибербезопасности было ошибкой», — написал сенатор Рон Уайден в письме директору Национальной разведки Джону Рэтклиффу.

Поскольку всё больше и больше данных размещалось в интернете, а барьеры в обмене разведданными между госорганами снижались после 11 сентября 2001 года, утечек становилось всё больше. В 2010 году аналитик армейской разведки Челси Мэннинг передала WikiLeaks сотни тысяч дипломатических телеграмм и военных файлов. В 2013 году Сноуден предоставил журналистам данные о секретных программах слежки.

«Можно было предположить, что эти инциденты станут тревожными сигналами для разведки и всех американских органов безопасности. Но похоже, что самые мощные и хорошо финансируемые разведывательные службы на планете не в состоянии остановить кровотечение своих собственных данных», — сказал Томас Рид, профессор информационной безопасности в Школе передовых международных исследований Университета Джона Хопкинса». ***(Ellen Nakashima, Shane Harris. Elite CIA unit that developed hacking tools failed to secure its own***

systems, allowing massive leak, an internal report found // The Washington Post (https://www.washingtonpost.com/national-security/elite-cia-unit-that-developed-hacking-tools-failed-to-secure-its-own-systems-allowing-massive-leak-an-internal-report-found/2020/06/15/502e3456-ae9d-11ea-8f56-63f38c990077_story.html). 16.06.2020).

***

«Почти четыреста организаций подписали открытое письмо , адресованное Конгрессу США, с просьбой защитить финансирование открытых проектов в условиях сложившейся в стране политически нестабильности. В числе подписавшихся значатся Фонд Викимедиа, Фонд электронных рубежей, Tor Project, Red Hat, Gnome, Digital Ocean, TunnelBear, Open Source Initiative, AccessNow, Human Rights Watch, и Центр по исследованию коррупции и организованной преступности (Organized Crime and Corruption Reporting Project, OCCRP). Письмо также подписали более 2,3 тыс. представителей открытых проектов и правозащитников.

Авторы письма просят Конгресс поддержать работу Фонда открытых технологий (Open Technology Fund, OTF) – американской некоммерческой организации, играющей роль связующего звена между правительством США и разработчиками ПО с открытым исходным кодом. С 2012 года OTF получает государственное финансирование через Агентство США по глобальным медиа (U.S. Agency for Global Media, USAGM) и распределяет его между разработчиками открытого ПО для защиты демократии и свободы слова по всему миру.

На прошлой неделе президент США Дональд Трамп сменил главу USAGM и уволил нескольких высокопоставленных должностных лиц из финансируемых агентством некоммерческих организаций. По данным CNN, с должностей были сняты руководители Middle East Broadcasting, Radio Free Asia, Radio Free Europe/Radio Liberty и Фонда открытых технологий. СМИ охарактеризовали действия Трампа как «вечернее побоище».

Как сообщает Motherboard, сейчас руководство USAGM планирует направить финансирование, изначально предназначенное для Фонда открытых технологий, на разработку ряда новых закрытых проектов, тем самым оставив широко использующиеся инструменты без финансирования в обозримом будущем.

К примеру, OTF участвовал в финансировании полного переписывания архитектуры WebExtensions и портирования в Chrome/Chromium. Кроме того, в настоящее время фонд финансирует разработку кросс-браузерной библиотеки для поддержки NoScript и других расширений для обеспечения приватности и безопасности.

По словам двух источников ZDNet, участвовавших в спонсируемых OTF проектах и пожелавших сохранить анонимность, есть риск того, что администрация Трампа может попытаться заменить проверенные технологии с открытым исходным кодом, предназначенные для защиты конфиденциальности, альтернативами с закрытым исходным кодом, в которых гораздо проще будет спрятать бэкдоры». ***(400 организаций просят Конгресс США не лишать***

открытые проекты финансирования // SecurityLab.ru (https://www.securitylab.ru/news/509406.php). 23.06.2020).

***

Країни ЄС

«В рамках программы исследований и инноваций Horizon 2020 Евросоюз выделяет 38 млн евро на защиту и совершенствование городов и наиболее важных объектов инфраструктуры.

Еврокомиссия выделяет более 38 млн евро на поддержку ряда инновационных проектов, направленных на развитие "умных городов" и обеспечение их безопасности, а также на защиту инфраструктуры ЕС от физических и киберугроз. Об этом говорится в сообщении, опубликованном на сайте Еврокомиссии в понедельник, 15 июня.

Финансирование проектов будет проходить в рамках программы Евросоюза по исследованиям и инновациям Horizon 2020, указано в документе. "ЕС принимает конкретные меры по защите наиболее важных инфраструктурных объектов, городов и граждан, поскольку мы сталкиваемся с целым рядом различных угроз в сфере кибербезопасности", – подчеркнул в этой связи комиссар ЕС по вопросам внутреннего рынка Тьери Бретон.

Проекты ЕС по защите инфраструктуры от киберугроз

Речь идет, в первую очередь, о проектах SAFETY4RAILS, 7SHIELD и ENSURESEC, которые должны обеспечить безопасность работы сетей метрополитена и железных дорог, наземной космической инфраструктуры и спутников, а также услуг в области электронной торговли и доставки.

Еще два проекта – IMPETUS и S4ALLCITIES – направлены на повышение устойчивости городских инфраструктур и систем услуг и защиту граждан в случае угрожающих безопасности инцидентов в общественных местах. Ожидается, что проекты будут запущены в период с июня по октябрь 2020 года. Рассчитаны они на два года». ***(ЕС совершенствует средства защиты от киберугроз // Информационное агентство GuildHall (https://ghall.com.ua/2020/06/16/es-sovershenstvuet-sredstva-zashhity-ot-kiberugroz/). 16.06.2020).***

***

Російська Федерація та країни ЄАЕС

«…Число компьютеров на операционной системе Windows, потенциально уязвимых для попыток доступа по протоколу RDP, с начала апреля к концу мая выросло в России на 230%, составив 101 тыс… Быстрый рост связан с тем, что на фоне самоизоляции высокими темпами росло и количество серверов, в том числе и открытых для интернета, цитирует «Ъ» мнение основателя и технического директора DeviceLock Ашота Оганесяна.

По словам Оганесяна, большинство компаний позволяют подключаться по протоколу удаленного стола только по технологии VPN (Virtual Private Network, виртуальная частная сеть). Но у некоторой доли серверов разрешена авторизация без пароля, а это представляет значительную опасность для корпоративных сетей, предупреждает Оганесян.

Директор экспертного центра Positive Technologies Алексей Новиков добавляет, что во всех популярных VPN-решениях также есть уязвимости, которые могут привести к несанкционированному доступу и отказу удаленной инфраструктуры. По его словам, быстрый переход на удаленку способствовал тому, что во главу угла ставилась работоспособность инфраструктуры, а не информационная безопасность.

По данным опроса, который Positive Technologies провела в середине апреля текущего года среди специалистов по информационной безопасности, более половины респондентов отметили, что в связи с пандемией удаленный доступ пришлось экстренно организовывать с нуля (11%) либо срочно масштабировать (41%).

По словам руководителя отдела расследования киберинцидентов JSOC CERT компании «Ростелеком» Игоря Залевского, с ростом количества целей (тех самых RDP) выросло число атак. Так, для подбора паролей к RDP число попыток возросло с 3–5 раз до 9–12. Сами атаки стали продолжаться дольше – от двух до трех часов. Для доступа в крупные компании с большим штатом отдела информационной безопасности злоумышленникам в среднем требуется полтора дня, рассказывает Игорь Залевский. Он рекомендует компаниям контролировать информацию о входах на сервер и заблаговременно копировать информацию, чтобы она не оказалась заблокирована в результате хакерских атак». ***(В России резко возросло число ПК, уязвимых к атакам через удалённый рабочий стол // РосКомСвобода (https://roskomsvoboda.org/59579/). 04.06.2020).***

***

«Голосование по поправкам к Конституции РФ может подвергнуться массированным кибератакам. Об этом заявил заместитель председателя комитета Совета Федерации по международным делам Андрей Климов.

Предполагаем, что будут попытки массированных кибератак. Мы такое наблюдали каждый раз перед выборами, которые проходили последние три года. Такие факты уже поступают в нашу комиссию, — цитирует РИА Новости сенатора.

Он добавил, что в полном объёме вся информация о возможных и уже совершённых кибератаках будет обобщена в ежегодном докладе, выпуск которого намечен на июль.

…около 40% всех кибератак в России приходится на московские организации, так как здесь сконцентрировано множество значимых организаций. Кроме того, в столице находится большинство центров обработки данных, которые являются одной из основных целей злоумышленников.

Так, во время проведения выборов мэра Москвы в 2018 году Solar JSOC зафиксировал более 200 различных попыток информационных воздействий на инфраструктуру выборов, в 2019 году — более 80. Все атаки были отражены.

Ранее секретарь Совета безопасности России Николай Патрушев заявлял, что спецслужбы иностранных государств ищут уязвимые места в информационной инфраструктуре России для совершения массированных кибератак.

В конце 2019 года вице-премьер Юрий Борисов, курирующий оборонную промышленность, дал поручение подготовить изменения в закон «О безопасности критической информационной инфраструктуры» для поэтапного замещения используемого иностранного оборудования на таких объектах. В ответ на это замминистра экономики Азер Талыбов предложил дополнить закон «О безопасности критической информационной инфраструктуры» нормой, обязывающей владельцев использовать только российское оборудование и софт, а также запретить иностранным компаниям «обеспечивать взаимодействие» с сетями и информационными системами критической инфраструктуры…». ***(В России ждут массовых кибератак по время голосования по Конституции // АНО "Информационно-аналитический центр "МедиаНьюс" (https://news.ru/politics/v-rossii-zhdut-massovyh-kiberatak-po-vremya-golosovaniya-po-konstitucii/). 18.06.2020).***

***

Інші країни

«Японский гигант электроники Sony объявил о запуске программы PlayStation Bug Bounty. Эта инициатива стала возможной благодаря партнерству с компанией по кибербезопасности HackerOne. Sony предлагает вознаграждение в размере до 50 000 долларов за тестирование игр, а также PlayStation 4 и PlayStation Network на критические уязвимости. Стоит отметить, что PlayStation 3 и другие старые устройства не нуждаются в тестировании. Для сравнения, в январе Microsoft начала платить до 20 000 долларов за обнаружение ошибок Xbox. И Sony, и Microsoft награждают “охотников за ошибками” 500 долларами за исправление уязвимостей низкого уровня. Ранее, Facebook установил партнерские отношения с HackerOne, чтобы запустить программу вознаграждений за обнаружение ошибок для проекта Libra. В конце мая компания HackerOne объявила о награждении белых хакеров наградами на сумму более 100 миллионов долларов. По оценкам, каждый час он платит своим пользователям около 6 000 долларов за поиск ошибок». ***(Сергей Ковалев. Sony запустила программу для вознаграждения белых хакеров // BitBetNews.com (https://www.bitbetnews.com/news-crypto/sony-zapustila-programmu-dlja-voznagrazhdenija-belyh-hakerov.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+bitbetnews+%28%D0%91%D0%BB%D0%BE%D0%B3+%D0%BE+%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0%D0%BB%D1%8E%D1%82%D0%B0%D1%85+bitbetnews.com%29). 25.06.2020).***

***

«Німеччина наполягає на запровадженні санкцій проти хакерів з РФ. Причина - кібератака на Бундестаг у 2015 році. У Берліні звинувачують у цьому російське ГРУ.

Анґела Меркель (Angela Merkel) відома своїм виваженим та сухим стилем ведення справ. Але у травні, під час виступу у Бундестазі, німецька канцлерка була незвично емоційною. Приводом для цього став депутатський запит депутатки від партії Зелених Табеї Реснер (Tabea Rösner) про те, які саме дані були викрадені з депутатського офісу канцлерки під час хакерської атаки на німецький парламент у 2015 році та з якою метою це було зроблено.

За словами Меркель, у неї склалося враження, що збиралися усі можливі дані. Вона також зазначила, що радіє рішенню німецької Генеральної прокуратури оголосити у розшук "конкретну особу". Після цього Меркель додала: "Я сприймаю ці речі дуже серйозно, бо я вірю, що там дуже добре все вивчили, і можу сказати - мені від цього боляче". Зокрема через те, що канцлерка, за її словами, намагається покращити відносини з Росією.

Читайте також: Пов'язані з ГРУ хакери намагалися зламати сервери компанії Burisma

Вона заявила про "вагомі докази" того, що російські відомства стоять за викраденням щонайменше 16 гігабайт даних, документів та електронних листів з мережі Бундестагу. Серед цих даних - і листування з депутатського офісу самої Меркель. Тому канцлерка пов'язала кібератаку із "російською стратегією гібридної війни - війни, яка включає в себе дезорієнтацію супротивника у кіберпросторі та спотворення фактів".

Відкрите звинувачення Росії

Виступ Меркель став поворотним пунктом для визнання російської провини у кібератаках. Йому передувало рішення генеральної прокуратури - її очільник Петер Франк (Peter Frank) наприкінці квітня оголосив у міжнародний розшук Дмитра Бадіна. Слідчі впевнені, що 29-річний росіянин стоїть за ефектною атакою на ІТ-системи німецького Бундестагу навесні 2015 року. Шпигунська програма хакерів так глибоко укорінилася у мережі, що її довелося повністю виключати. Після викрадення даних, система, до якої було підключено майже 6000 комп'ютерів, була вибудувана з нуля.

Німеччина довго ухилялася від того, аби публічно звинуватити в атаці російські спецслужби. Але це змінилося після ордеру з Карлсруе, де розташоване відомство Генеральної прокуратури, та після промови канцлерки, розповідає Юлія Шютце (Julia Schütze). Шютце працює менеджеркою проєкту "Міжнародна політика кібербезпеки" у берлінському аналітичному центрі "Фонд нової відповідальності". Для експертки звинувачення Бадіна продемонструвало "витримку Німеччини, коли йдеться про те, аби отримати юридично вагомі докази для подібних звинувачень, які потім можуть призвести до політичних кроків".

Режим кіберсанкцій ЄС

І політичні заходи вже на підході. Наприкінці травня російського посла викликали у міністерство закордонних справ Німеччини. Сергій Нечаєв мусив не

лише вислуховувати слова про те, що німецький уряд "найгостріше" засуджує хакерську атаку. Нечаєву також повідомили про те, що уряд вимагатиме "у Брюсселі запровадження режиму кіберсанкцій ЄС проти відповідальних за атаку на німецький Бундестаг, зокрема й проти пана Бадіна".

Сам механізм кіберсанкцій був ухвалений Європейською Радою 17 травня 2019 року. Завдяки цьому, після кібератак, які мали "істотні наслідки", ЄС може запроваджувати санкції проти осіб та організацій, які є відповідальними за ці атаки. Серед іншого йдеться про загрозу заборони на в'їзд до ЄС, пояснює Шютце, чи також замороження рахунків. Експертка з питань кібербезпеки вбачає важливість цих заходів у їхньому "політичному стратегічному символізмі".

Те, про що було оголошено російському послу, поступово приводиться у дію. Німецький уряд "зробив пропозиції санкційного списку з огляду на хакерську атаку та перебуває щодо цього у тісному спілкуванні із своїми партнерами по ЄС". Так на запит DW відповіли у МЗС Німеччини. Цей процес розпочинається у робочій групі при Європейській Раді у Брюсселі. Як повідомляє низка ЗМІ, німецькі дипломати представили свої пропозиції щодо санкцій 3 червня. Із впевненістю можна сказати, що Дмитро Бадін має бути у цьому списку на особливо почесному місці.

Прописка у спецслужбі

На плакатах американського ФБР із розшукуваними ним особами Бадіна можна знайти одразу двічі. З цих постерів коротко стрижений блондин дивиться на нас із серйозним виразом обличчя.

ФБР також висуває вагомі звинувачення проти цього уродженця Курська, розташованого за 500 кілометрів на південь від Москви. Бадін, вірогідно, належав до осіб, які викрали та оприлюднили електронне листування Гілларі Клінтон та Демократичної партії під час передвиборчої кампанії у США 2016 року, таким чином вплинувши на результат виборів на користь Дональда Трампа.

Також доповідь журналістів-розслідувачів з Bellingcat пов'язує Бадіна з російською військовою розвідкою ГРУ. Наприклад, адреса його прописки збігається із офіційною адресою частини ГРУ під номером 26165, свідчать дані Bellingcat.

Цей підрозділ широко відомий під різними іменами: передусім - Fancy Bear, але також Sofacy, Pawn Storm чи Sednit. ІТ-експерти, а також німецьке Федеральне відомство з охорони конституції надають перевагу більш технічному терміну - APT28. APT означає "Advanced Persistent Threat", що перекладається як "розвинута стійка загроза" - вираз під яким здебільшого розуміють цільову та добре сплановану кібератаку.

APT28 й справді є стійкою. Компанія з кібербезпеки FireEye спостерігає за хакерами на службі російської держави вже з 2007 року. У компанії пов'язують їх не лише із атаками на Бундестаг чи американськими виборами, але також і низкою інших кібератак, зокрема на Всесвітнє антидопінгове агентство (WADA), ОБСЄ та НАТО.

Допомога з Нідерландів

У будь-якому разі, звинувачення у кібератаках, або так звана атрибуція, є важкою справою. У віртуальному просторі можна легко заплутувати сліди. Втім часто все ж знаходяться технічні докази і підстави для обґрунтованих підозр. Для

спецслужб цього достатньо, аби зробити належну оцінку того, що відбулося. Але судам потрібні однозначні докази.

Важливу допомогу німецькі слідчі отримали з Нідерландів. Там навесні 2018 року контррозвідка змогла запобігти атаці на Організацію із заборони хімічної зброї (ОЗХЗ). Тоді в руки нідерландців потрапила велика кількість технічного обладнання. Це й дало німецькій прокуратурі чіткі докази, які привели її до Бадіна та ГРУ, розповідає Шютце.

Генеральна прокуратура нагадує, що кібератаки можуть відбуватися з будь-якого напрямку. "До найбільш відомих випадків належать розслідування через підозру у шпигуванні за мобільним телефоном канцлерки ФРН, Анґели Меркель з боку американських розвідувальних служб, - зазначається на вебсторінці відомства. - Для цієї підозри не вдалося знайти доказів, які б могли задовольнити суд. Розслідування було припинене у червні 2015 року".

Але у випадку Бадіна та ГРУ Німеччина, вірогідно, використає своє головування у Раді ЄС, яке розпочнеться з 1 липня, аби хакерська атака на Бундестаг не залишилася без наслідків». ***(Маттіас фон Гайн, Олександр Голубов. Хакерська атака на Бундестаг. Чи запровадить ЄС санкції проти РФ // Deutsche Welle(https://www.dw.com/uk/%D1%85%D0%B0%D0%BA%D0%B5%D1%80%D1%81%D1%8C%D0%BA%D0%B0-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0-%D0%BD%D0%B0-%D0%B1%D1%83%D0%BD%D0%B4%D0%B5%D1%81%D1%82%D0%B0%D0%B3-%D1%87%D0%B8-%D0%B7%D0%B0%D0%BF%D1%80%D0%BE%D0%B2%D0%B0%D0%B4%D0%B8%D1%82%D1%8C-%D1%94%D1%81-%D1%81%D0%B0%D0%BD%D0%BA%D1%86%D1%96%D1%97-%D0%BF%D1%80%D0%BE%D1%82%D0%B8-%D1%80%D1%84/a-53812641?maca=ukr-rss-MetaUA-ukr-V_Mire-3051-xml-mrss). 16.06.2020).***

***

«Німецьке слідство має докази того, що громадянин Росії разом з іншими особами здійснив хакерську атаку на Бундестаг для розвідки РФ. Про це заявив міністр закордонних справ Німеччини Хайко Маас заявив в інтерв'ю італійській газеті La Repubblica…

"Існують конкретні і достовірні докази з боку слідчих і судових органів про те, що громадянин Росії скоїв хакерську атаку на бундестаг Німеччини для російської спецслужби навесні 2015 року — разом з іншими людьми", — заявив міністр.

За його словами, на цій підставі слідчі судді Федерального суду видали ордер на арешт зазначеного громадянина.

"Не може бути й мови про політичні забобони, як неодноразово заявляла російська сторона. Ми також будемо працювати в Брюсселі, щоб використовувати режим кіберсанкцій ЄС для тих, хто несе відповідальність за атаку, наприклад, щоб заморозити активи або ввести обмеження на в'їзд. У той же час очевидно, що ми хочемо продовжувати конструктивно-критичний діалог з Москвою в інших

областях зовнішньої політики, таких як конфлікт на сході України або в Лівії і Сирії", — додав Маас…». ***(Саша Картер. Німеччина заявила про наявність доказів причетності РФ до хакерської атаки на Бундестаг // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1873198-nimechchina-zayavila-pro-nayavnist-dokaziv-prichetnosti-rf-do-khakerskoyi-ataki-na-bundestag). 04.06.2020).***

***

«Хакери з Ірану і Китаю намагалися взяти під контроль комп'ютерні системи передвиборчих штабів президента США Дональда Трампа і його ймовірного суперника на виборах Джо Байдена

Про це в своєму Twitter повідомив керівник відділу Google з кібербезпеки Шейн Хантлі.

За його словами, у хакерів могли бути зв'язки з владою своїх країн.

"Якщо ви працюєте над кампанією в цьому циклі виборів, ваші особисті облікові записи можуть бути зламані. Використовуйте кращий захист, який тільки зможете. Двофакторна аутентифікація або підвищений захист дійсно можуть змінити ситуацію", - зазначив Хантлі.

Він додав, що Google повідомив про ці випадки користувачів, яких могла торкнутися ця ситуація, а також співробітників правоохоронних органів.

Байден є найбільш імовірним кандидатом від Демократичної партії на президентських виборах, які відбудуться в листопаді 2020 року.

Кандидатуру Байдена повинні затвердити на з'їзді Демпартії 17 серпня.

Згідно з останніми опитуваннями, електоральна перевага демократа перед президентом Трампом становить до 10%». ***(Хакери з Китаю та Ірану атакували передвиборчі штаби Трампа і Байдена) // Espreso.tv (https://espreso.tv/news/2020/06/05/khakery_z_kytayu_ta_iranu_atakuvaly_peredvyborchi_shtaby_trampa_i_baydena). 05.06.2020).***

***

«Компанія Facebook заявила, що не знайшла на своїх платформах доказів скоординованого втручання з-за кордону, спрямованого на протести у США на своїх платформах. «Ми активно шукаємо і поки не бачимо втручання з-за кордону, або скоординованої неавтентичної поведінки, яка б походила із США, спрямованих на протести», - заявив Натаніель Гляйхер, голова політики з кібербезпеки Facebook, повідомляє «Голос Америки».

Натаніель Гляйхер також закликав не робити передчасних висновків без чітких доказів втручання з-за кордону.

Раніше міністр юстиції США Вільям Барр заявив, що «екстремістські агітатори», пов'язані з ліворадикальним рухом «Антіфа», і угруповання, які діють в інтересах іноземних держав, спробували скористатися загальнонаціональними протестами для загострення обстановки в США. За словами Барра, іноземні угруповання зараз проводять дезінформаційні кампанії у соціальних мережах, на зразок кампаній, які проводилися російською владою під час президентських

виборів в США в 2016 році. Мета іноземців, за словами Барра, - посіяти ворожнечу в американському суспільстві.

«Деякі з іноземних хакерів і угруповань, пов'язаних з іноземними урядами, зосереджуються на ситуації, яка у нас тут складається, і намагаються загострити її всіма можливими способами», - заявив міністр юстиції США.

За кілька днів до заяви Барра видання The Nation повідомило, з посиланням на внутрішні документи Федерального Бюро Розслідувань, що у ФБР «немає розвідданих, які б вказували на участь, або присутність» членів руху «Антіфа» у насильницьких діях, які мали місце у столиці США, Вашингтоні 31-го травня». ***(У Facebook не знайшли доказів закордонного втручання, пов'язаного із протестами у США // Конфликты и законы (https://k-z.com.ua/myr/54028-u-facebook-ne-znayshli-dokaziv-zakordonnogo-vtruchannya-povyazanogo-iz-protestami-u-ssha). 06.06.2020).***

***

«Не исключено, что ответом палестинской стороны на аннексию части Западного берега, планируемую премьер-министром Израиля Биньямином Нетаниягу (Benjamin Netanyahu), станут многочисленные кибернетические атаки.

О возможности именно такого развития событий предупреждает бывший глава ШАБАКа Юваль Дискин (Yuval Diskin), который убежден, что оборонному ведомству следует быть готовым к отражению ударов кибернетического характера.

Свои замечания господин Дискин озвучил после того, как основанный им стартап «Opora» привлек семь миллионов долларов США в качестве стартового капитала от фонда «Jerusalem Venture Partners» и частных инвесторов-меценатов. При основании стартапа в 2018 году партнерами Юваля Дискина стали бывшие коллеги Ноам Йоллес (Noam Jolles) и Цафир Кац (Tsafrir Katz), а также предприниматель Крис Белл (Chris Bell)». ***(Кибератаки могут стать ответом на аннексию // ISRAland Online Ltd (http://www.isra.com/news/246456). 12.06.2020).***

***

«Рада ЄС продовжила санкції за кібератаки до 18 травня 2021 року

Україна приєдналася до погодженого ЄС пакету санкцій проти третіх країн за здійснення навмисних кібернетичних атак проти ЄС або проти його країн-членів.

Про це йдеться у декларації Високого представника ЄС від імені усього Євросоюзу, яка оприлюднена на сайті Європейської Ради.

«14 травня 2020 року Рада ЄС ухвалила рішення (CFSP) 2020/651. Рішення Ради продовжує існуючі обмежувальні заходи на наступні 12 місяців, до 18 травня 2021 року. Країни-кандидати Туреччина, Республіка Північна Македонія, Чорногорія і Албанія, країна Процесу стабілізації і асоціації та потенційний кандидат Боснія і Герцеговина, країни Європейської зони вільної торгівлі Ісландія і Норвегія, члени Європейського економічного простору, а також Україна і Грузія приєдналися до цього рішення Ради», - йдеться у документі.

Як зазначається в декларації, згадані треті країни зобов'язалися забезпечити відповідність національної політики цьому рішенню Ради ЄС. Європейський Союз взяв до уваги ці зобов'язання та привітав їх.

Згадане рішення Ради ЄС прийнято у розвиток рішення Європейської Ради від 17 травня 2019 року стосовно обмежувальних заходів проти кібернетичних атак, що загрожують Європейському Союзу або його країнам-членам. Документ визначає рамкові умови для застосування дипломатичних заходів проти країн, які здійснюють агресивні та навмисні кібернетичні атаки проти ЄС, які потягнули важкі наслідки для країн-членів або для критично важливої європейської інфраструктури.

ЄС розглядає ці санкції як потенційну можливість, тому що до цього моменту до переліку фізичних або юридичних осіб третіх країн, які можуть бути причетними до такої кібернетичної агресії, не внесено жодного конкретного суб'єкта…». ***(Україна приєдналася до санкцій ЄС за кібератаки // Українські медійні системи (https://glavcom.ua/news/ukrajina-prijednalasya-do-sankciy-jes-za-kiberataki-688062.html). 19.06.2020).***

***

«Прем'єр-міністр Скотт Моррісон заявив, що уряд Австралії і ряд інших організацій в різних областях стали об'єктами кібератаки з боку неназваною країни.

За словами Моррісона на брифінгу в Канберрі, ці атаки були спрямовані на всі рівні уряду, політичні організації, постачальників основних послуг і інших операторів стратегічної інфраструктури.

"Беручи до уваги характер і масштаби атак, ми прийшли до висновку, що це досвідчений зловмисник, який діяв за підтримки іншої країни", – повідомив Моррісон.

За словами Моррісона, хоча загроза постійна, частота атак збільшилася в останні кілька місяців. Він вказав на те, що дії були здійснені із значним потенціалом.

Міністр оборони Австралії Лінда Рейнольдс заявила, що в результаті хакерської атаки не було виявлено великих витоків даних». ***(Лиза Солнцева. Прем'єр-міністр Моррісон заявив, що Австралія є метою кібератак з іншої країни // ІА "ЄУРАБОТА" (https://news.eurabota.ua/uk/australia/developments/prem-ier-ministr-morrison-zajaviv-shho-avstralija-ie-metoju-kiberatak-z-inshoi-kraini/). 19.06.2020).***

***

«Днем в воскресенье, 21 июня, был взломан интернет-сайт издания The Jerusalem Post.

Хакеры, которые идентифицировали себя просто как «Турецкие и мусульманские хакеры», заменили контент сайта одной страницей со звездой и полумесяцем турецкого флага, наряду со стихами из Корана и исламистской пропагандой.

«Не забывай! Аль-Кудс - наша красная линия!», - частично читается на странице, а также: «Свободные мусульмане, и свободная Палестина, и свободный Восточный Туркестан».

Внизу страницы хакеры выставили Израиль как «главного дьявола», сравнивая еврейское государство с Европейским союзом, Организацией Объединенных Наций, США и Китаем. Сайт был позже восстановлен.

В начале этого месяца исламистские хакеры запустили «OpIsrael» - ежегодное мероприятие, представляющее собой кибератаки, нацеленные на израильские и еврейские цели.

Во время «OpIsrael» в этом году хакерам удалось украсть личную информацию сотен израильтян». ***(Сайт The Jerusalem Post взломали исламистские хакеры // STMEGI Media Group (https://stmegi.com/posts/81054/sayt-the-jerusalem-post-vzlomali-islamistskie-khakery/). 21.06.2020).***

***

Створення та функціонування кібервійськ

«Министерство обороны Великобритании создало 13-й Сигнальный полк в составе Королевского корпуса связи британских вооруженных сил, отвечающий за обеспечение защиты от цифровых атак. Новое подразделение будет защищать жизненно важные оборонные сети в стране и во время проведения операций за рубежом.

«Это новый шаг в модернизации вооруженных сил Великобритании, которые должны быть готовы к информационной войне. Кибератаки столь же смертоносны, как и те, с которыми сталкиваются на физическом поле битвы, поэтому мы должны подготовиться к защите от любых источников угроз, и 13-й Сигнальный полк является жизненно важным дополнением к этой защите», — пояснил глава ведомства Бен Уоллес (Ben Wallace).

Специализированное подразделение обеспечит основу для нового Центра операций по информационной безопасности армии, уделяя особое внимание защите домена ведомства, и будет сотрудничать с Королевским военно-морским флотом и Королевскими военно-воздушными силами для обеспечения безопасных сетей всех военных коммуникаций». ***(Минобороны Великобритании создало киберполк для защиты от цифровых атак // SecurityLab.ru (https://www.securitylab.ru/news/508944.php). 05.06.2020).***

***

Захист персональних даних

«Пять миллиардов долларов штрафа грозит компании Google. Крупнейшую в мире поисковую систему обвиняют в тайном сборе персональных данных.

Американская корпорация попадается на нарушениях далеко не в первый раз. Коллективный иск против холдинга Alphabet, куда входит Google, подан в федеральный суд Калифорнии. По данным Reuters, планируется взыскать около 5 тысяч долларов за каждого пользователя. Незаконный сбор данных велся с помощью сервиса статистики, рекламного менеджера и других приложений, установленных на смартфонах». ***(Google грозит штраф на 5 миллиардов долларов за незаконный сбор данных пользователей // Новости США на русском языке (https://usa.one/2020/06/google-grozit-shtraf-na-5-milliardov-dollarov-za-nezakonnyj-sbor-dannyx-polzovatelej/). 04.06.2020).***

***

«В апреле 2020 года пользователи Nintendo стали массово жаловаться на компрометацию своих учтенных записей. Неизвестные лица входили в чужие аккаунты из самых разных стран мира, и многие пострадавшие теряли деньги в результате таких компрометаций. В некоторых случаях хакеры покупали игры Nintendo за чужой счет, но чаще всего приобретали игровую валюту Fortnite через привязанную к профилю Nintendo карту или аккаунт PayPal.

Когда количество жалоб и публикаций в СМИ достигло критической точки, компания Nintendo подтвердила, что неизвестные злоумышленники действительно взломали учтенные записи примерно 160 000 пользователей.

Как выяснилось, проблема заключалась не в массовых credential stuffing атаках и переборе наиболее распространенных комбинаций учтенных данных. Игровая компания утверждает, что хакеры эксплуатировали интеграцию с NNID, то есть Nintendo Network ID, чтобы получить доступ к чужим профилям. NNID – это устаревшая логин-система, используемая для управления учетными записями на старых платформах Wii U или Nintendo 3DS. На новых устройствах Nintendo пользователи так же могут связать свои старые учетные записи NNID с профилем Nintendo.

Тогда представители Nintendo не уточнили, что именно произошло, но заявили, что более NNID не поддерживается, и войти таким образом в основной профиль Nintendo не выйдет.

Теперь, спустя полтора месяца после этих событий, Nintendo сообщила, что специалистам компании удалось выявить еще примерно 140 000 нарушений, то есть суммарно от апрельских атак пострадали около 300 000 пользователей…

Компания еще раз принесла извинения пользователям и пообещала повысить безопасность, чтобы подобное больше повторилось. В настоящее время всем пострадавшим сбросили пароли, а также специалисты Nintendo уверяют, что почти закончили возвращать пострадавшим их средства». ***(Мария Нефёдова. Nintendo признала, что от атак хакеров пострадали 300 000 пользователей // Xakep (https://xakep.ru/2020/06/11/nintendo-nnid-hack/). 11.06.2020).***

***

«Эксперты компании IntSights обнаружили, что в последнее время в даркнете отмечается рост интереса к учетным данным от YouTube-каналов, а также, в качестве "побочного эффекта", это стимулирует деятельность по

проверке данных. На хакерских форумах и сайтах, где торгуют учетными данными, можно найти все больше предложений такого рода.

При этом нужно отметить, что киберпреступников давно интересует YouTube, ведь сайт предоставляет им новую аудиторию, которую можно использовать самими разными способами, от мошенничества до рекламы. К тому же нередко злоумышленники «угоняют» популярные каналы у их законных владельцев, а затем требуют выкуп за возвращение доступа.

Данные о YouTube-каналах в основном собирают с зараженных малварью компьютеров, в результате фишинговых кампаний и так далее. После ворованную информацию сортируют на конкретные логины и пароли от определенных сервисов, а затем продают на черном рынке.

Стоимость выставленных на продажу списков с учтенными данными от YouTube-каналов пропорциональна количеству их подписчиков. Исследователи приводят несколько примеров. Так, в одном случае цена за канал с 200 000 подписчиков начиналась от 1000 долларов и возрастала с шагом 200 долларов.

В другом случае исследователи обнаружили рекламу аукциона, в рамках которого продавали данные от 990 000 активных каналов, и цена начиналась от 1500 долларов (тот, кто заплатит 2500 долларов, получал список без торга). Очевидно, продавец надеялся быстро заработать, продав данные, так как опасался, что его жертвы заметят компрометацию, обратятся в поддержку и вернут доступ к своим аккаунтам.

Еще один набор из 687 учетных записей YouTube, с сортировкой по количеству подписчиков, был выставлен на продажу по начальной цене в 400 долларов (цена возрастала с шагом в 100 долларов, а за 5000 долларов «лот» можно было забирать сразу).

Специалисты IntSights полагают, что хакеры, скорее всего, собирают материал для таких списков с учетными данными от каналов на YouTube, проверяя БД с ворованными логинами и паролями (в поисках данных от учетных записей Google) и данные, полученные с зараженных компьютеров.

Эксперты IntSights пишут, что в прошлом злоумышленники использовали сложные фишинговые кампании и наборы инструментов с обратным прокси, чтобы обманывать двухфакторную аутентификацию Google. Теперь продавцы редко упоминают 2ФА вообще, и скорее всего, это говорит о том, что угнанные аккаунты не были защищены двухфакторной аутентификацией.

Издание Bleeping Computer отмечает, что пользователи, пострадавшие от взлома и угона аккаунта на YouTube, часто жалуются, что их обманом вынудили загрузить малварь…». ***(Мария Нефёдова. На хакерских форумах растет спрос на учетные данные от YouTube-каналов // Xakep (https://xakep.ru/2020/06/05/youtube-credentials/). 05.06.2020).***

***

«Специалисты из ИБ-компании RiskIQ сообщили о трех скомпрометированных web-сайтах, принадлежащих компании Endeavor Business Media. Одна из группировок Magecart использовала некорректно

настроенные бакеты Amazon S3 для внедрения JavaScript-кода на web-сайты с целью кражи данных кредитных карт.

На уязвимых ресурсах размещался контент, связанный с аварийными службами, и форумы чатов, предназначенные для пожарных, полицейских и специалистов по безопасности. Эксперты сообщили Endeavour Business Media о своих находках, однако компания не отреагировала на уведомление.

Помимо JavaScript-кода, специалисты также обнаружили дополнительный код, получивший название jqueryapi1oad. Преступники использовали его в ходе длительной вредоносной кампании, которая началась в апреле 2019 года и, по имеющимся данным, заразила 277 уникальных хостов.

Код устанавливает выполняет проверку на наличие ботов и устанавливает cookie-файл jqueryapi1oad с датой истечения срока действия, основанной на результатах проверки, а также создает DOM-элемент на странице. Затем происходит загрузка дополнительного JavaScript-кода, который, в свою очередь, загружает cookie-файл, связанный с системой управления трафиком (Traffic Distribution System, TDS) Keitaro, для перенаправления трафика на мошеннические объявления в рамках вредоносной рекламной кампании HookAds…». ***(Одна из группировок Magecart атаковала сайты, связанные с экстренными службами // SecurityLab.ru (https://www.securitylab.ru/news/509017.php). 09.06.2020).***

***

«Исследователи из Университета Карнеги-Меллона подсчитали, что только треть пользователей меняют свои пароли после компрометации данных. Интересно, что этот доклад, представленный в рамках воркшопа IEEE 2020 по технологиям и защите потребителей, основывается не на данных опросов, а на фактическом трафике браузеров.

Эксперты изучили реальный трафик, собранный с помощью университетской Security Behavior Observatory, исследовательской группы, в которую пользователи добровольно вступают и делятся полной историей браузера с целью проведения академических исследований. Так, данные для этого анализа были собраны с домашних компьютеров 249 участников эксперимента за период с января 2017 года по декабрь 2018 года. Информация включала не только веб-трафик, но также пароли, сохраненные в браузере.

Как выяснилось, из 249 пользователей только 63 имели учетные записи на различных взломанных доменах (учитывались только те компании, которые публично объявили о взломе и утечке данных).

Из этих 63 пользователей только 21 человек (33%) посетил взломанные сайты, чтобы изменить пароль, а из этих 21 только 15 пользователей сменили пароли в течение трех месяцев после объявления о компрометации.

В общей сложности на указанных выше доменах было изменено 23 пароля. Так, среди сменивших пароли участников эксперимента было только 18 пользователей Yahoo!; еще 31 пользователь Yahoo! (из 49 в общей сложности) не меняли свои пароли, хотя все пострадали в результате утечки данных. Еще 2 пользователя сменили свои пароли от Yahoo! дважды, по одному разу после каждого сообщения о компрометации. 2 пользователя сменили свои пароли на

взломанном домене в течение одного месяца после объявления о взломе, 5 человек поменяли пароли по истечении двух месяцев и 8 человек спустя три месяца.

Так как, помимо прочего, исследователи собирали данные о паролях участников эксперимента, команда смогла проанализировать и сложность их новых паролей. Среди пользователей, которые изменили пароли (суммарно 21 человек), только треть (9 человек) сменила их на более надежные. Остальные члены контрольной группы придумали более слабые пароли или пароли аналогичной силы. Обычно новые пароли создавались либо путем повторного использования последовательностей символов из предыдущего пароля, либо люди попросту изменял пароль на другой, но уже использующийся для других учетных записей и тоже хранившийся в браузере.

Исследователи утверждают, что большая часть вины за происходящее лежит на самих взломанных сервисах, поскольку те «почти никогда не объясняют людям, что еще нужно сбрасывать похожие и идентичные пароли для других учетных записей». ***(Мария Нефёдова. Пользователи редко меняют пароли даже после утечек данных // Xakep (https://xakep.ru/2020/06/03/passwords-security/). 03.06.2020).***

***

«Всього в минулому місяці відбулося 105 інцидентів, з яких на один припадає рекордна витік в 8,3 млрд. Записів. Британська компанія IT Governance, що займається поставками рішень для інформаційної безпеки та оцінкою кіберрісков, підготувала список з усіма публічними витоками даних, що відбулися в травні 2020 року. У список потрапили лише ті витоку, інформація про яких стала публічною – на ділі ж витоків могло бути і більше.

Наймасовіша витік стався в результаті всього одного інциденту з мереж тайського оператора мобільного зв'язку AIS – в інтернеті з'явилося 8,3 млрд. Записів журналів DNS-запитів і NetFlow клієнтів. Користувач, який знайшов дані у відкритому доступі, спробував зв'язатися з AIS безпосередньо, але компанія проігнорувала всі повідомлення. Тільки звернувшись в національну комп'ютерну групу реагування на надзвичайні інциденти ThaiCERT, вдалося домогтися приховування даних.

Інші випадки витоків меркнуть на тлі першого – в результаті 104 інцидентів було отримано доступ до 460 млн. Записів. Велика частина з них не представляла велику цінність для хакерів, проте деякі були вельми чутливі для користувачів. Наприклад, в Північній Ірландії були розкриті особистості 250 жертв насильства.

Найчастіше до даних отримували доступ в результаті кібератак, атак з використанням здирницькі ПО, а також в результаті незахищених розміщення даних в інтернеті». ***(У травні стався рекордний витік даних в 8,3 млрд. записів // Portaltele (https://portaltele.com.ua/news/internet/u-travni-stavsya-rekordnij-vitik-danih-v-8-3-mlrd-zapisiv.html). 04.06.2020).***

***

«Более 300 000 канадских бухгалтеров и других пользователей ресурсов ассоциации дипломированных профессиональных бухгалтеров Канады (CPA

Canada) пострадали от утечки данных. Организация опубликовала заявление, в котором говорится, что неизвестные лица получили доступ к персональной информации, взломав сайт.

Около 329 000 членов ассоциации и других пользователей оказались под угрозой компрометации персональных данных. Скомпрометированная информация относится главным образом к профессиональному изданию ассоциации — CPA Magazine, и включает имена, адреса, почтовые адреса и имена сотрудников. Организация заявила, что пароли и данные кредитных карт были зашифрованы, хотя и не сообщается по какому алгоритму. Пользователи подвергшихся атаке ресурсов предупреждены о возможности повторных атак». ***(Канадская ассоциация бухгалтеров подверглась кибератаке // SecureNews (https://securenews.ru/canadian-accountants-association-attacks-cyber-attack/). 08.06.2020).***

***

«Крупнейший американский оператор пассажирских железнодорожных перевозок, компания Amtrak, заявила о взломе информационной системы и утечке некоторых данных своих клиентов.

Вечером 16 апреля сотрудники Amtrak заметили, что некто получил неавторизованный доступ к некоторым учетным записям (Amtrak Guest Rewards). Неизвестные использовали где-то раздобытые учетные данные, чтобы получить доступ к аккаунтам, и им это удалось — некоторые данные могли быть просмотрены. Однако в компании заверяют, что номера кредитных карт и социального страхования, а также финансовая информация не были подвергнуты риску.

ИТ-отдел в течение нескольких часов полностью прекратил неавторизованный доступ. Учетные данные атакованных аккаунтов были сброшены. Были наняты эксперты извне, чтобы урегулировать инцидент и наладить безопасность.

На данный момент неизвестно, каким образом злоумышленники завладели авторизационными данными, с помощью которых получили доступ к аккаунтам. Они могли быть получены из других утечек и использовались хакерами для множественных попыток войти на разные сайты». ***(Утечка данных в крупной американской железнодорожной компании // SecureNews (https://securenews.ru/large-us-railroad-company-data-leak/). 01.06.2020).***

***

«Утечка коснулась профилей, несколько лет назад созданных на AliExpress, Ebay, Sony PlayStation Network, Steam, Blizzard Entertainment и многих других онлайн-сервисах

Эксперты по кибербезопасности из Cyble Research Team обнаружили выставленную на продажу базу данных, содержащую сведения о миллионах пользователей сети, о чём сообщается на сайте компании. В базе содержится информация об аккаунтах на разных сайтах. Большинство профилей, данные которых выставлены на продажу, было зарегистрировано несколько лет назад. К

примеру, в базе оказались сведения о 300 миллионах пользователей AliExpress, создавших свои аккаунты в 2014 году.

Кроме того, злоумышленники выставили на продажу личную информацию 145 миллионов пользователей Ebay, 77 миллионов пользователей Sony PlayStation Network, 35 миллионов пользователей Steam (Valve), 14 млн. клиентов Blizzard Entertainment и многих других.

Специалисты дали несколько советов о том, как не стать жертвами мошенников. Они порекомендовали никогда не отправлять личные данные по электронной почте или SMS, использовать сложные пароли, включить автоматические обновления программ на компьютере и телефоне, а также пользоваться антивирусом». ***(В сеть утекли данные миллионов интернет-покупателей // РосКомСвобода (https://roskomsvoboda.org/60025/). 16.06.2020).***

***

«Задумывались ли вы, почему онлайн-реклама вещей появляется сразу как только вы о них подумали?

Здесь нет никакой магии. Рекламные технологии могут быть очень точными. Технический гигант Oracle — одна из немногих компаний в Силиконовой долине, которая практически усовершенствовала искусство отслеживания людей через Интернет. Компания потратила десятилетие и миллиарды долларов на покупку стартапов, чтобы создать собственную базу данных о просмотре веб-страниц пользователями.

Один из таких стартапов, BlueKai, который Oracle купил в 2014 году немногим более 400 миллионов долларов , едва известен за пределами маркетинговых кругов, но он собрал один из крупнейших банков данных веб-отслеживания за пределами федерального правительства.

BlueKai использует файлы cookie на веб-сайте и другие технологии отслеживания, чтобы следить пользователями Интернета. Зная, какие веб-сайты вы посещаете и какие электронные письма открываете, маркетологи могут использовать этот огромный объем отслеживаемых данных, чтобы сделать как можно больше выводов о пользователе: его доходах, образовании, политических взглядах и интересах, — используя потом эти жанные, чтобы сделать целевую рекламу более точной, которая соответствует определенным вкусам. Если пользователь открывает ссылку, рекламодатели делают деньги.

Но какое-то время эти данные веб-трекинга раздавались в открытом доступе в интернете, потому что сервер оставался незащищенным и без пароля, открывая миллиарды записей для любого, кто мог их найти.

Исследователь безопасности Анураг Сен нашел базу данных и сообщил о своих находках в Oracle через посредника — Роя Карти, руководителя фирмы по кибербезопасности Hudson Rock.

Среди данных, предоставленных Сеном, найдены имена, домашние адреса, адреса электронной почты и другая персональная информация в базе данных. Данные также показали, что пользователи просматривают различные веб-страницы начиная от покупок до отмены подписки на рассылку.

«На самом деле невозможно сказать, насколько раскрытыми могут быть некоторые из этих данных», — сказал TechNetCrunch Беннетт Сайферс, штатный технолог из Electronic Frontier Foundation.

«Oracle осведомлена об отчете Рои Карти из Hudson Rock, касающемся определенных записей BlueKai, которые могут быть представлены в Интернете», — сказала представитель Oracle Дебора Хеллингер. «Хотя первоначальная информация, предоставленная исследователем, не содержала достаточного количества информации для идентификации уязвимой системы, исследование Oracle впоследствии установило, что две компании неправильно настроили свои услуги. Oracle предприняла дополнительные меры, чтобы избежать повторения этой проблемы».

Oracle не назвал компании и не сказал, что это были за дополнительные меры, и отказался от комментариев.

Но из-за огромного размера выставленной базы данных это одна из самых больших уязвимостей в системе киберезопасности в этом году.

Больше данных в открытом доступе BlueKai просеивает бесконечный поток данных из различных источников, чтобы понять тенденции и доставить наиболее точную рекламу в интересах заказчика.

Маркетологи могут либо использовать огромный банк данных Oracle, который он получает от кредитных агентств, аналитических фирм и других источников данных о потребителях, включая миллиарды ежедневных отметок геолокация, чтобы нацелить свои объявления. Маркетологи также могут загружать свои собственные данные, полученные непосредственно от потребителей, такие как информация, которую вы передаете при регистрации учетной записи на веб-сайте или при подписке на новостную рассылку компании.

BlueKai также использует более скрытую тактику, например, позволяет веб-сайтам встраивать невидимые пиксельные изображения для сбора информации о пользователн, как только он откроет веб-страницу — оборудование, операционную систему, браузер и любую информацию о сетевом подключении.

Такие данные, известные как «пользовательский агент» веб-браузера, могут не показаться конфиденциальными, но при их объединении они могут создать уникальный «отпечаток пальца» устройства человека, который можно использовать для отслеживания конкретной личности во время работы в Интернете.

BlueKai также может привязать привычки потребителя при просмотре веб-страниц на мобильных устройствах к активности на рабочем столе, позволяя им следить за пользователем через Интернет независимо от того, какое устройство он использует.

Скажем, маркетолог хочет провести кампанию, пытаясь продать новую модель автомобиля. В случае BlueKai у него уже есть категория «автолюбителей» — и многие другие, более конкретные категории — которые маркетолог может использовать для таргетинга рекламы. Любой, кто посетил веб-сайт автопроизводителя или блог, содержащий пиксель отслеживания BlueKai, может быть отнесен к категории «автолюбителей». Со временем этот человек будет

разделен на различные категории в профиле, который узнает как можно больше о потребителе, чтобы нацелить на него такие объявления.

Технология далека от совершенства. Ранее в этом году Harvard Business Review обнаружило, что качество информации, собираемой такими брокерами, как Oracle, может сильно различаться. Но некоторые из этих платформ оказались пугающе точными.

В 2012 году Target отправила купоны по беременности и родам учащейся средней школы после того, как внутренняя аналитическая система выяснила, что она беременна — еще до того, как она рассказала своим родителям — из-за данных, полученных из ее просмотра веб-страниц.

Некоторые могут возразить, что именно для этого предназначены эти системы. Джонатан Майер, профессор науки в Принстонском университете, говорит, что BlueKai является одной из ведущих систем для связи данных.

«Если у системы есть браузер, отправляющий адрес электронной почты и файл cookie для отслеживания одновременно, это то, что нужно системе для создания таршетинговой ссылки», — сказал он.

Конечная цель: чем больше BlueKai собирает данных, тем больше он может повлиять на плльзователя, упрощая рекламный таргетинг, который может соблазнить поьребителч на такой волшебный клик по зарабатыванию денег.

Но маркетологи не могут просто войти в BlueKai и загрузить множество личной информации со своих серверов, говорит специалист по маркетингу. Данные очищаются и маскируются так, чтобы маркетологи никогда не видели имена, адреса или любые другие личные данные.

Как объяснил Майер: BlueKai собирает личные данные; но не делится ими с маркетологами.

«Не разглашать»

За кулисами BlueKai постоянно принимает и сопоставляет как можно больше необработанных персональных данных с профилем каждого человека, постоянно дополняя эти данные профиля, чтобы обеспечить их актуальность.

Так один отчет показал, как одна из крупнейших инвестиционных компаний Турции использовала BlueKai для отслеживания пользователей на своем веб-сайте. В записи подробно рассказывается, как один человек, живущий в Стамбуле, заказал в магазине мебели для дома на сумму 899 долларов. Это стало известно, потому что в его записи содержались все эти данные, включая имя покупателя, адрес электронной почты и прямой веб-адрес заказа, для чего не требовался логин.

Также рассмотрена запись, в которой подробно описывается, как один человек, отписавшийся от рассылки электронной почты, которую ведет потребитель электроники, отправил ее на свой адрес iCloud. Запись показала, что человека, возможно, интересовала конкретная модель автомобильной видеорегистратора. На основании его аккаунтп теперь можно даже сказать, что его iPhone устарел и нуждается в обновлении программного обеспечения.

По словам Сена, который обнаружил базу данных, данные собирались месяцами. По его словам, некоторые журналы датируются августом 2019 года.

«Детализированные записи привычек просмотра веб-страниц людьми могут выявить хобби, политическую принадлежность, уровень дохода, состояние

здоровья, сексуальные предпочтения и — как видно здесь — привычки азартных игр», — сказал Сайферс из EFF. «Поскольку мы живем большую часть своей жизни в Интернете, такие данные составляют все большую часть того, как мы проводим наше время».

Oracle отказалась сообщить, информировала ли она тех, чьи данные были раскрыты, об ошибке безопасности. Компания также отказалась сообщить, предупредила ли она США или международные регуляторы об инциденте.

В соответствии с законодательством штата Калифорния, такие компании, как Oracle, обязаны публично раскрывать информацию о подобных инцидентах, но Oracle до сих пор не объявила об этом.

В соответствии с Европейским общим регламентом о защите данных, компании могут быть оштрафованы на сумму до 4% от своего глобального годового оборота за нарушение правил защиты и раскрытия данных.

Трекеры и повсеместное отслеживание

BlueKai повсюду — даже когда вы не можете его увидеть.

Согласно одной из оценок, BlueKai отслеживает более 1% всего веб-трафика — непостижимый объем ежедневного сбора данных — и отслеживает некоторые из крупнейших в мире веб-сайтов: Amazon, ESPN, Forbes, Glassdoor, Healthline, Levi's, MSN.com, Rotten Tomatoes и Нью-Йорк Таймс .

Но BlueKai не одинок. Почти каждый веб-сайт, который вы посещаете, содержит какую-то форму невидимого кода отслеживания, который наблюдает за вами, когда вы заходите в Интернет.

Несмотря на то, что невидимые трекеры подают данные о каждом веб-просмотре в гигантскую базу данных в облаке, эти самые данные сохраняют Интернет в значительной степени свободным в течение столь длительного времени.

Чтобы оставаться свободными, веб-сайты используют рекламу для получения дохода. Чем более таргетинована реклама, тем выше должен быть доход .

Хотя большинство веб-пользователей ещё достаточно наивны, чтобы думать, что интернет-слежения не существует, лишь немногие сторонние маркетинговые круги понимают, сколько данных собирается и что с ними делается.

К примеру, нарушение данных Equifax в 2017 году, которое вызвало резкую критику со стороны законодателей после того, как было собрано миллионы данных потребителей без их явного согласия. Equifax, как и BlueKai, полагается на то, что потребители пропускают длительные политики конфиденциальности, определяющие, как их отслеживают веб-сайты.

В любом случае, у потребителей нет иного выбора, кроме как принять эти условия. Отслеживаться или покинуть сайт. Это компромисс с бесплатным интернетом.

Но существует опасность сбора данных о веб-отслеживании миллионов людей.

«Всякий раз, когда существуют подобные базы данных, всегда существует риск, что данные окажутся в чужих руках и могут нанести кому-нибудь вред», — говорит Сайферс.

Сайферс сказал, что данные, если они попадут в руки злоумышленников, могут способствовать краже персональной информации, фишингу или подделке.

«Это также является ценной целью для правоохранительных органов и правительственных учреждений, которые хотят использовать возможности сбора данных, которые Oracle уже делает», — сказал он.

По словам Сайферса, даже когда данные остаются на своих местах, эти обширные базы информации позволяют «манипулировать рекламой для таких вещей, как политические проблемы или эксплуатационные услуги и дают возможность маркетологам адаптировать свои сообщения для конкретных уязвимых групп населения», — сказал он.

«У всех есть разные вещи, которые они хотят держать в секрете, и разные люди, которых они хотят держать в секрете», — сказал Сайферс. «Когда компании собирают необработанные данные о просмотре веб-страниц или покупках, тысячи мелких деталей о жизни реальных людей накапливаются»…» ***(Oracle отслеживает всех через Интернет для таргетинговой рекламы // Goodnews.ua (https://goodnews.ua/technologies/oracle-otslezhivaet-vseh-cherez-internet-dlya-targetingovoj-reklamy/). 20.06.2020).***

***

«Исследователи информационной безопасности предупреждают пользователей игры Stalker Online, что 1.3 миллиона пользовательских записей были проданы на форумах дарквеба. Имена, пароли, email адреса, телефонные номера и IP-адреса были обнаружены исследователями из компании CyberNews. Исследователи уточнили, что пароли хранились в виде хешей, зашифрованных по алгоритму MD5, а не в открытом виде. Тем не менее, это слабейший из алгоритмов хеширования.

Всего на подпольных площадках были найдены две базы данных. Одна содержала 1.2 миллиона записей, вторая 136 000. После того, как подлинность данных, содержащихся в базах, была подтверждена, исследователи попробовали связаться с австралийскими разработчиками BigWorld Technology, а также владеющей BWT на данный момент компанией Wargaming. Ответа пока не поступило». ***(Утечка данных в Stalker Online: более 1.3 миллионов учетных записей // SecureNews (https://securenews.ru/stalker-online-data-leak-over-1-3-million-accounts/). 22.06.2020).***

***

«Компания Delivery Hero подтвердила утечку данных клиентов сервиса по доставке еды Foodora — дочерней компании Delivery Hero. Стало известно, что данные 727 000 клиентов сервиса из 14 стран были выложены на нескольких хакерских форумах. Данные включают полные имена, телефонные адреса, номера, захешированные пароли (по алгоритму MD5). Предположительно, некоторые данные были украдены еще в 2016 году. Это подтверждает и компания, говоря, что многие записи действительно соответствуют их текущим и прошлым рынкам.

В настоящее время компания проводит расследование инцидента. Ее представители связываются с властями, чтобы получить помощь в расследовании, а также оповещают клиентов, данные которых оказались доступны злоумышленникам. Известно, что некоторым из них поступают подозрительные

письма от неизвестных отправителей». ***(Утечка данных у сервиса по доставке еды // SecureNews (https://securenews.ru/data-leak-at-food-delivery-service/). 17.06.2020).***

***

«Специалисты компании Comparitech, занимающейся информационной безопасностью, провели любопытное исследование. Они создали базу данных, которую заполнили бесполезными данными, имитирующими ценную информацию. Базу оставили доступной онлайн на 11 дней и не защитили паролем. То есть, сымитировали довольно распространенную ситуацию, из-за которой случаются утечки информации.

Первая атака случилась через 8 с половиной часов — еще до того, как база была проиндексирована поисковиками Shodan и BinaryEdge (поисковики интернета вещей). Это говорит о том, что хакеры активно используют инструменты проактивного сканирования.

Всего за время наблюдений было зарегистрировано 175 атак. Это в среднем 18 за день. Самое большое количество атак в сутки, 22, произошло сразу же после индексирования базы поисковиком Shodan. Причем первые две в течение минуты после этого. Больше всего атак происходило из Румынии, США и Китая. Большинство пытались получить больше информации о базе и ее настройках.

Некоторые хакеры пытались использовать уязвимости Elasticsearch 2015 года, чтобы установить ПО для майнинга криптовалюты, украсть пароли или изменить настройки сервера, чтобы украсть или удалить данные. А через несколько дней после завершения эксперимента все еще незащищенная база была атакована ботом, который удалил все содержимое базы и оставил сообщение о выкупе.

Проведенный эксперимент говорит о том, как мало времени есть у организаций, которые по ошибке оставили без защиты базу данных». ***(Незащищенная база данных подвергается атаке 18 раз в день // SecureNews (https://securenews.ru/an-unprotected-database-is-attacked-18-times-a-day/). 15.06.2020).***

***

«В Сети стали появляться жалобы пользователей Firefox на то, что без их разрешения Microsoft автоматически перенесла все данные их браузеров в Edge.

Судя по всему, проблема появилась после обновления до Windows 10 2004. По словам пользователей, после установки новой ОС с улучшенным Edge появляется функция-мастер для запуска Edge с единственной возможной опцией «Начать». Закрыть мастер можно только через диспетчер задач, однако при этом все данные из Firefox автоматически переносятся в Edge, браузер прикрепляется к панели задач, а на рабочем столе появляется иконка. Более того, при следующем переходе по ссылке пользователю нужно снова выбирать браузер по умолчанию.

Согласно некоторым сообщениям пользователей, в Edge переносятся данные не только из Firefox, но также из других браузеров…». ***(Edge импортирует***

данные из Firefox без согласия пользователей // SecurityLab.ru (https://www.securitylab.ru/news/509427.php). 23.06.2020).

***

«Группа активистов под названием DDoSecrets опубликовала в Сети 296 ГБ данных, которые, по их утверждению, были похищены у более чем 200 полицейских участков и центров охраны правопорядка по всей территории США.

Утечка данных, получившая название BlueLeaks, была опубликована на общедоступном портале и содержит более миллиона файлов, таких как отсканированные документы, видео, электронные письма, аудиофайлы и пр.

Согласно DDoSecrets, большинство файлов представляют собой отчеты полиции и ФБР, бюллетени по безопасности и руководства для правоохранительных органов за последние 24 года. Некоторые из файлов также предположительно содержат конфиденциальную и личную информацию, такую как имена, номера банковских счетов и номера телефонов.

Как утверждает DDoSecrets, данные BlueLeaks были «любезно предоставлены участниками движения Anonymous». Данные были похищены в результате взлома систем техасской компании Netsential, обслуживающей ряд государственных правоохранительных ресурсов по обмену данными.

Ассоциация National Fusion Center Association (NFCA) подтвердила подлинность утечки во внутреннем предупреждении безопасности». ***(Злоумышленники опубликовали в Сети данные 200 полицейских участков в США // SecurityLab.ru (https://www.securitylab.ru/news/509399.php0. 23.06.2020).***

***

«У відомстві кажуть, що зловмисники викрадали реквізити банківських електронних рахунків громадян США, Європи, України, а також викрадали їхні персональні дані.

У Харкові співробітники Служби безпеки викрили групу хакерів, які викрадали гроші з банківських рахунків. Про це пишуть на офіційному сайті СБУ.

За даними слідства, група з 15 осіб використовувала шкідливе програмне забезпечення, за допомогою якого викрадала реквізити банківських електронних рахунків громадян США, Європи, України, а також їх персональні дані. Зокрема, через електронні платіжні сервіси, в тому числі заборонені в Україні російські ресурси, вони переводили викрадені гроші на власні рахунки в українських та російських банках.

Зазначають, що правоохоронці провели в Харкові 16 обшуків за місцем розташування хакерського центру і за місцем проживання фігурантів.

Під час обшуків було виявлено більше 40 пристроїв з фотографіями і реквізитами іноземних банківських карток і іншими доказами злочинів. Також були вилучені банківські картки, готівка та цінності на суму більш ніж 12 млн грн, а також документи на рухоме і нерухоме майно в Україні та за кордоном…» ***(СБУ затримала групу хакерів, які обкрадали банківські рахунки // MediaSapiens***

(https://ms.detector.media/kiberbezpeka/post/24931/2020-06-24-sbu-zatrimala-grupu-khakeriv-yaki-obkradali-bankivski-rakhunki/). 24.06.2020).

***

«Причиной самой большой утечки данных в истории ЦРУ стала халатность специализированного подразделение агентства. Как сообщается во внутреннем отчете ЦРУ, опубликованном сенатором-демократом США Роном Уайденом (Ron Wyden), высококвалицифированные ИБ-специалисты ведомства «были сосредоточены на создании кибероружия в ущерб обеспечению безопасности собственных компьютерных систем».

Хакерские инструменты были похищены в результате взлома систем Center for Cyber Intelligence (CCI) в 2016 году. Точный объем украденных данных остается неизвестным, но по предварительным оценкам может составлять около 34 ТБ. Кража была обнаружена примерно через год, в марте 2017 года, когда WikiLeaks опубликовал крупнейшую подборку документов ЦРУ под названием Vault 7, в которых подробно описывались некоторые из самых современных хакерских инструментов агентства.

«Большая часть нашего секретного кибероружия не была разделена, пользователи обменивались паролями уровня администратора, не было эффективных средств управления съемными носителями, а важные данные были доступны пользователям на неопределенный срок... Если бы эти данные были украдены в интересах вражеского государства и не были опубликованы, мы бы могли так и не узнать об утечке», — сообщается в документе». ***(Кибероружие ЦРУ было похищено в результате халатности сотрудников // SecurityLab.ru (https://www.securitylab.ru/news/509261.php). 17.06.2020).***

***

«Специалисты ИБ-подразделения ElevenPaths испанской телекоммуникационной компании Telefónica обнаружили новую киберпреступную операцию, целью которой является похищение конфиденциальных данных тайваньских пользователей.

По словам исследователей, злоумышленники рассылают избранной группе жертв фишинговые письма, искусно подделанные под уведомления от Центров по контролю заболеваний Тайваня. Письма адресованы сотрудникам этих же центров.

В прошлом месяце в течение недели злоумышленники рассылали жертвам письма, в которых сообщалось, что они якобы должны пройти новый тест на коронавирус. Во вложении к письму содержался хакерский инструмент для удаленного похищения учетных данных и взлома web-камер. Как считают в ElevenPaths, жертвы и тип избранного киберпреступниками инструмента свидетельствует о том, что их интересует информация, в частности правительственная. Увенчались ли попытки фишинговых атак успехом, неизвестно.

За атаками предположительно стоят хакеры из группировки Vendetta, появившейся всего два месяца назад. Группировка выдает себя за госучреждения разных стран, рассылая жертвам фишинговые письма от их имени. Согласно отчету

ИБ-компании Qihoo 360 за май 2020 года, Vendetta выдавала себя за государственные управления Австрии, Австралии и Румынии, пытаясь установить на системах жертв инструменты для удаленного взлома. Как минимум в одном случае ее целью было похищение конфиденциальных деловых документов.

Скорее всего, число жертв Vendetta на Тайване небольшое. Подобные группировки не проводят массовых кибератак, а тщательно выбирают своих жертв.

Центры по контролю заболеваний не единственные цели киберпреступников на Тайване. В другой, не связанной с Vendetta кампании злоумышленники атаковали Министерство здравоохранения и социального обеспечения с целью установить вредоносное ПО LokiBot для похищения данных». ***(Vendetta атакует управления здравоохранения на Тайване // SecurityLab.ru (https://www.securitylab.ru/news/509256.php). 17.06.2020).***

***

«Более 10 тыс. человек подали коллективный иск против британской авиакомпании EasyJet после того, как в результате хакерской атаки данные примерно 9 млн ее клиентов стали доступны злоумышленникам…

Адвокаты потерпевших отмечают, что к иску присоединились клиенты EasyJet из более чем 50 стран. Это одна из крупнейших групповых судебных жалоб в Великобритании, связанных с утечкой персональной информации.

По данным Financial Times, дело против авиаперевозчика ведет лондонская юридическая фирма PGMBM.

Представители авиакомпании заявили, что им известно об исковой инициативе, а также о том, «что другие подобные фирмы рекламируют свои услуги в этом же отношении».

«Это не редкость, и тот факт, что фирмы занимаются рекламой, не означает наличие у них серьезных претензий», — заявили в EasyJet.

19 мая EasyJet сообщила о кибератаке, после которой взломщики получили доступ к базе данных электронных адресов и сведений о поездках 9 млн клиентов, а также к информации о кредитных картах 2,2 тыс. из них». ***(Против EasyJet подали коллективный иск после утечки данных 9 млн ее клиентов // Полит.ру (https://polit.ru/news/2020/06/24/easyjet/). 24.06.2020).***

***

«Представители Twitter связываются с бизнес-клиентами сервиса, чтобы предупредить, что их данные могут оказаться под угрозой. Сказано, что email адрес, телефонный номер и последние 4 цифры банковской карты могут оказаться известны посторонним из-за того, что эта информация сохраняется в кэше браузера. Впервые эту уязвимость обнаружили 20 мая, после чего немедленно предприняли действия по ее исправлению и стали связываться с клиентами. Стоит отметить, что по информации BBC уязвимость не затрагивает обычных пользователей сервиса.

Это уже не первый случай, когда Twitter заявляет, что данные, оказывающиеся в распоряжении платформы, оказываются в опасности. За месяц до текущего инцидента компания предупреждала, что некоторая непубличная

информация может сохранятся в кэше браузера Firefox. Подобные уязвимости опасны для тех, кто пользуется сервисом, используя общественные компьютеры или к чьим личным компьютерам могут иметь доступ другие люди». ***(Twitter уведомляет клиентов об угрозе их персональным данням // SecureNews (https://securenews.ru/twitter-notifies-customers-of-a-threat-to-their-personal-data/). 24.06.2020).***

***

«В марте исследователей встревожило обнаруженное ими нарушение конфиденциальности более чем четырьмя десятками iOS-приложений, включая TikTok (китайская соцсеть для обмена видео, покорившая интернет). Несмотря на обещание сделать работу над ошибками, TikTok всё ещё имеет доступ к некоторым наиболее чувствительным данным пользователей Apple — таким как пароли, адреса криптовалютных кошельков, ссылки на сброс учётных записей и личные сообщения. Еще 53 приложения, выявленные в марте, тоже не оставили подобную практику.

Вторжение в частную жизнь — результат чтения приложениями текстов, которые случайно оказались в буферах обмена, используемых компьютерами и другими устройствами для хранения данных из менеджеров паролей и почтовых программ.

Исследователи Талал Хадж Бакри и Томми Миск обнаружили, что, не имея на то прав, приложения намеренно вызывают интерфейс программирования iOS, который извлекает текст из буфера обмена пользователя.

Универсальная слежка

Во многих случаях скрытое считывание не ограничено данными, хранящимися на локальном устройстве. Если iPhone или iPad использует тот же идентификатор Apple ID, что и другие устройства Apple, и находится примерно в 10 футах (чуть более трёх метров — прим. ред.) друг от друга, все они имеют общий универсальный буфер обмена. Поэтому содержимое может быть скопировано из приложения одного устройства и вставлено в приложение на другом.

Это открывает возможность приложению на iPhone считывать конфиденциальные данные на планшетах других подключённых устройств. Такими данными могут быть биткойн-адреса, пароли или сообщения электронной почты, которые временно хранятся в буфере обмена ближайшего компьютера Mac или iPad. Несмотря на работу на отдельном устройстве, приложения iOS могут легко считывать чувствительные данные, хранящиеся на других машинах.

«Это очень, очень опасно. Эти приложения читают буфер обмена без какой-бы то ни было цели. Приложение, у которого нет текстового поля для ввода текста, не имеет причин читать текст из буфера обмена», — сказал Миск о беспорядочном считывании данных из буфера обмена приложениями.

Видео ниже демонстрирует универсальное чтение буфера обмена.

TikTok в центре внимания

СМИ сосредоточили особое внимание на TikTok в значительной степени из-за его огромной базы активных пользователей (сообщается, что она составляет 800

млн, из них только в первой половине 2018 года приложение было установлено 104 млн раз на iOS, что делает его самым загружаемым приложением за этот период).

TikTok привлёк к себе внимание ещё и по другим причинам. В марте провайдер видеохостинга сообщил британскому изданию The Telegraph, что прекратит слежку в ближайшие недели. Миск сказал, что приложение не прекращало мониторинг никогда. Более того, выяснилось, что чтение буфера обмена происходит каждый раз, когда пользователь вводит знак препинания или нажимает пробел, составляя комментарий. Это означает, что чтение буфера обмена может происходить примерно каждую секунду, что гораздо быстрее, чем показало мартовское исследование, говорившее, что мониторинг происходит при открытии приложения.

Okay so TikTok is grabbing the contents of my clipboard every 1-3 keystrokes. iOS 14 is snitching on it with the new paste notification pic.twitter.com/OSXP43t5SZ

— Jeremy Burge (@jeremyburge) June 24, 2020

Представители TikTok написали:

«После выхода бета-версии iOS14 22 июня пользователи получили уведомления при использовании ряда популярных приложений. У TikTok это было вызвано функцией выявления повторяющегося спам-поведения. Мы уже представили обновленную версию приложения в App Store, удалив функцию защиты от спама, чтобы исключить возможную путаницу.

TikTok стремится защитить конфиденциальность пользователей и быть прозрачным в своей работе. Мы с нетерпением ожидаем увидеть сторонних экспертов в нашем Центре прозрачности позже в этом году».

Ранее пресс-секретарь говорил, что TikTok для Android никогда не реализовывал функцию защиты от спама.

Не только TikTok

В целом исследователи обнаружили, что следующие приложения iOS считывали данные из буфера обмена пользователей, не имея на то чёткой цели, каждый раз, когда приложение открывалось.

• App Name — BundleID

Новости

• ABC News — com.abcnews.ABCNews
• Al Jazeera English — ajenglishiphone
• CBC News — ca.cbc.CBCNews
• CBS News — com.H443NM7F8H.CBSNews
• CNBC — com.nbcuni.cnbc.cnbcrtipad
• Fox News — com.foxnews.foxnews
• News Break — com.particlenews.newsbreak
• New York Times — com.nytimes.NYTimes
• NPR — org.npr.nprnews
• ntv Nachrichten — de.n-tv.n-tvmobil
• Reuters — com.thomsonreuters.Reuters
• Russia Today — com.rt.RTNewsEnglish
• Stern Nachrichten — de.grunerundjahr.sternneu
• The Economist — com.economist.lamarr
• The Huffington Post — com.huffingtonpost.HuffingtonPost
• The Wall Street Journal — com.dowjones.WSJ.ipad
• Vice News — com.vice.news.VICE-News

Игры

• 8 Ball Pool™ — com.miniclip.8ballpoolmult
• AMAZE!!! — com.amaze.game
• Bejeweled — com.ea.ios.bejeweledskies
• Block Puzzle —Game.BlockPuzzle
• Classic Bejeweled — com.popcap.ios.Bej3
• Classic Bejeweled HD — com.popcap.ios.Bej3HD
• FlipTheGun — com.playgendary.flipgun
• Fruit Ninja — com.halfbrick.FruitNinjaLite
• Golfmasters — com.playgendary.sportmasterstwo
• Letter Soup — com.candywriter.apollo7
• Love Nikki — com.elex.nikki
• My Emma — com.crazylabs.myemma

• Plants vs. Zombies™ Heroes — com.ea.ios.pvzheroes
• Pooking – Billiards City — com.pool.club.billiards.city
• PUBG Mobile — com.tencent.ig
• Tomb of the Mask — com.happymagenta.fromcore
• Tomb of the Mask: Color — com.happymagenta.totm2
• Total Party Kill — com.adventureislands.totalpartykill
• Watermarbling — com.hydro.dipping

Социальные сети

• TikTok — com.zhiliaoapp.musically
• ToTalk — totalk.gofeiyu.com
• Tok — com.SimpleDate.Tok
• Truecaller — com.truesoftware.TrueCallerOther
• Viber — com.viber
• Weibo — com.sina.weibo
• Zoosk — com.zoosk.Zoosk

Другие

• 10% Happier: Meditation — com.changecollective.tenpercenthappier
• 5-0 Radio Police Scanner — com.smartestapple.50radiofree
• Accuweather — com.yourcompany.TestWithCustomTabs
• AliExpress Shopping App — com.alibaba.iAliexpress
• Bed Bath & Beyond — com.digby.bedbathbeyond
• Dazn — com.dazn.theApp
• Hotels.com — com.hotels.HotelsNearMe
• Hotel Tonight — com.hoteltonight.prod
• Overstock — com.overstock.app
• Pigment – Adult Coloring Book — com.pixite.pigment
• Recolor Coloring Book to Color — com.sumoing.ReColor
• Sky Ticket — de.sky.skyonline
• The Weather Network — com.theweathernetwork.weathereyeiphone

После публикации отчёта TikTok обещал остановить слежку, но так и не сделал этого, сказал Миск. Ни одно приложение не сделало этого.

Правильное чтение буфера обмена

В некоторых случаях чтение буфера обмена может сделать приложения намного полезнее. Так, приложение UPS для iPhone извлекает текст из буфера обмена и в случае, если текст соответствует характеристикам номера отслеживания, предлагает пользователю отслеживать соответствующий пакет. Google Chrome тоже извлекает текст и, если это URL-адрес, предлагает пользователю перейти к нему. Фоторедактор Pixelmator считывает данные изображений и предлагает пользователю открыть его для редактирования. Во всех трёх случаях чтение данных имеет чёткую цель и прозрачность.

TikTok и другие оскорбительные приложения, напротив, получают доступ к буферу обмена без видимой причины и каких-либо объяснений того, что они это делают. Миск рассказал, что Apple планирует использовать данные исследования для создания нового уведомления буфера обмена в iOS 14. Он считает, что это хорошее начало, но в итоге Apple и Google должны сделать больше. Они могут сделать запрос на доступ к буферу обмена стандартным, как к микрофону или камере. Либо потребовать от разработчиков приложений точно раскрывать, какие данные буфера обмена считываются и что приложение делает с ними.

Пока же пользователи должны помнить, что любые данные, хранящиеся в буфере обмена, несмотря на то что они незаметны невооруженным глазом, постоянно могут быть доступны приложениям, которые во многих случаях даже не установлены на самом устройстве. Если вы сомневаетесь, очистите данные буфера обмена, скопировав символ, слово или другой фрагмент обычного текста». ***(TikTok and 53 other iOS apps still snoop your sensitive clipboard data // Condé Nast***

(https://arstechnica.com/gadgets/2020/06/tiktok-and-53-other-ios-apps-still-snoop-your-sensitive-clipboard-data/). 27.06.2020).

***

«**Данные 5 млн учащихся и сотрудников онлайн-школы английского языка Skyeng выставлены на продажу в интернете за 40 тыс. руб.** В самой компании факт утечки не подтверждают. Эксперты предполагают, что базу мог слить кто-то из увольняющихся сотрудников компании, и прогнозируют рост таких случаев в связи с текучкой кадров.

Данные 5 млн учащихся онлайн-школы английского языка Skyeng выставлены на продажу в интернете, обнаружил Telegram-канал In4security. В базе содержатся сведения о пользователях сервиса из стран СНГ, включая телефоны, адреса электронной почты и идентификаторы в Skype. Данные продаются за 40 тыс. руб., уточняет основатель DeviceLock и сервиса разведки утечек DLBI Ашот Оганесян. В том числе в базе 270 тыс. записей о российских пользователях — учителях, учениках и всех работниках компании, говорит он…

В Skyeng не подтвердили факт утечки или взлома. Нет оснований считать, что указанная в сообщении база имеет отношение к Skyeng, заявил управляющий партнер этой платформы Александр Ларьяновский.

Судя по формату предоставленных продавцом образцов, база утекла в результате открытого доступа к серверу MongoDB примерно три месяца назад, полагает Ашот Оганесян. Подобные ситуации нередки в последнее время и приводят к тому, что базы, выставленные в открытый доступ, попадают в продажу или бесплатно публикуются на хакерских форумах, указывает он.

Характер базы говорит о том, что либо был взломан ресурс школы, либо базу унес сотрудник, предполагает ведущий аналитик Infosecurity a Softline Company Александр Вураско.

Базу мог вынести кто-то из инсайдеров, чтобы попытаться «слить» злоумышленникам или конкурентам, соглашается менеджер по развитию направления DLP Solar Dozor компании «Ростелеком-Солар» Алексей Кубарев, прогнозируя рост случайных и умышленных утечек данных в связи с возросшей текучкой кадров. Среди возможных сценариев утечки он также называет внешнюю атаку на сервер, где хранятся данные пользователей, либо сбор данных от онлайн-кабинетов пользователей с помощью фишингового сайта, похожего на сайт сервиса-жертвы.

Сотрудники компаний воруют данные, когда не уверены в завтрашнем дне, их доход снизился и они получили доступ к корпоративной информации из дома и могут скопировать ее быстро и бесконтрольно, полагает руководитель аналитического центра Zecurion Владимир Ульянов.

По данным Zecurion, в обычных условиях менее половины сотрудников намерены копировать корпоративные данные, но при угрозе увольнения или сокращения доля таких желающих возрастает почти вдвое.

Вполне вероятно, что базу украл увольняющийся сотрудник, полагает господин Ульянов, неспроста подобные работники попадают в группу особого контроля со стороны службы безопасности.

В Infosecurity a Softline Company во время пандемии фиксировали до десяти новых утечек баз с данными граждан — клиентов интернет-магазинов, посетителей сайтов и др. На этой неделе в интернете обнаружилась база данных 5 млн пользователей предположительно с сайта SuperJob (в компании опровергли утечку)…

База может использоваться для спама и в этой роли будет интересна конкурентам Skyeng, которых в последнее время появилось много, считает Ашот Оганесян. Конкурирующие сервисы могут использовать ее для целевой рекламы с помощью интернет-сервисов, например контекстной или таргетированной рекламы, соглашается Владимир Ульянов. Кроме того, использующие методы социальной инженерии мошенники могут выведать информацию непосредственно для получения денег, добавляет он. Мошенники могут предложить клиентам оплатить несуществующие программы и фейковые услуги, уточняет Алексей Кубарев». ***(Юлия Степанова. Информация об учащихся онлайн-школы Skyeng выставлена на продажу // Газета "Коммерсантъ" (https://www.kommersant.ru/doc/4396472). 27.06.2020).***

***

Кібербезпека Інтернету речей

«Эксперты по кибербезопасности заявили о наличии сразу нескольких угроз, связанных с «умным домом». Так, например, 112 тысяч устройств в 20 тысячах умных домов Zipato дают возможность хакеру открывать двери и делать все, что ему угодно. Кроме того хакеры научились управлять розетками, а через них и подключенными устройствами. Эксперты по безопасности также обнаружили уязвимость в выпрямителе для волос, который хакеры могли разогревать выше 230 градусов. В 2020 году исследователи Check Point обнаружили уязвимость в «умных» лампочках: через нее можно было получить доступ к сети Wi-Fi.

В связи с выявленными угрозами в Роскачестве советуют использовать надежные пароли и двухфакторную аутентификацию, а также пользоваться на компьютере антивирусом, защищать Wi-FI и сеть VPN (Virtual Private Network, «виртуальная частная сеть»). Если это возможно, то лучше использовать более одного маршрутизатора, чтобы ваши устройства IoT находились в сети, отличной от сети вашего основного ПК. Это защитит информацию на вашем ПК в случае, если ваши IoT-устройства будут скомпрометированы, советуют в Роскачестве». ***(Иван Гридин. Роскачество заявило о небезопасности «умных домов» // РИА «Новый День» (https://newdaynews.ru/technology/694977.html). 17.06.2020).***

***

«Крупнейший интернет-провайдер в Австрии A1 Telekom стал жертвой кибератаки. Инсайдер, использующий псевдоним Libertas, сообщил блогеру Кристиану Хащеку (Christian Haschek) подробности о кибератаке, произошедшей в ноябре 2019 года.

Команда безопасности A1 Telekom обнаружила вредоносное ПО только через месяц после атаки, однако устранить вредонос оказалось намного труднее, чем первоначально предполагалось. С декабря 2019 года по май 2020 года специалисты боролись с операторами вредоносного ПО, пытаясь удалить все их замаскированные бэкдор-компоненты и прогнать злоумышленников из сети компании.

Вредоносное ПО заразило только компьютеры в офисной сети, а не всю IT-систему, состоящую из более чем 15 тыс. рабочих станций, 12 тыс. серверов и тысяч приложений. Злоумышленники предположительно вручную управляли вредоносным ПО с целью распространить заражение на другие системы в сети компании. Преступникам удалось взломать некоторые базы данных и даже выполнить запросы к базе данных, чтобы изучить внутреннюю сеть компании.

Как отметили представители A1 Telekom, несмотря на довольно длительную борьбу с вредоносом, которая длилась более шести месяцев, злоумышленнику не удалось похитить какие-либо конфиденциальные данные клиентов. Компания осуществила сброс паролей для учетных записей всех своих 8 тыс. сотрудников и изменила пароли и ключи доступа для всех серверов.

По словам блогера, кибератаку осуществила киберпреступная группировка Gallium, специализирующаяся на взломе телекоммуникационных провайдеров по всему миру». ***(Хакеры взломали системы крупнейшего австрийского провайдера A1 Telekom // SecurityLab.ru (https://www.securitylab.ru/news/509181.php). 11.06.2020).***

***

«Журналисты Bleeping Computer предупредили, что недавно мошенники захватили три YouTube-канала, дали им новые названия, связанные с компанией SpaceX, а затем запустили фейковые «трансляции» с Илоном Маском, в ходе которых проводили фиктивные раздачи биткоинов. Таким образом злоумышленники выманили у пользователей более 150 000 долларов в криптовалюте всего за два дня.

Уже много лет разные мошенники время от времени выдают себя за Илона Маска и компанию SpaceX, прикрывая тем самым свои вредоносную деятельность. В частности, преступники любят проводить от имени Маска фейковые раздачи криптовалют, обещая пользователям огромные прибыли, если те сначала отправят им немного биткоинов.

Теперь журналисты сообщают, что недавно неизвестные злоумышленники взломали каналы Juice TV, Right Human и MaximSakulevich, а затем переименовали их в SpaceX Live и SpaceX. Один из угнанных каналов имел 230 000 подписчиков, а

другой —131 000 подписчиков. При этом настоящий канал SpaceX на YouTube насчитывает 4,33 миллиона пользователей.

Все захваченные каналы транслировали интервью и различные выступления Илона Маска или конференции SpaceX, выдавая эти записи за живые стримы. На таких стримах мошенники рекламировали фейковые раздачи биткоинов и просили зрителей прислать им небольшое количество криптовалюты, чтобы поучаствовать в раздаче и получить обратно уже удвоенную сумму.

К сожалению, на удочку скамеров попалось множество пользователей. Bleeping Computer пишет, что одну из трансляций смотрело примерно 80 000 человек, и начиная с 8 июня 2020 года мошенники сумели «заработать» таким образом примерно 150 000 долларов в биткоинах.

Так, один канал просил пользователей отправлять биткоины на адрес 1ELonMUSK14JSGNYAcPJNqubuFByZPyjcj. Как можно видеть, мошенники получили более 30 переводов на общую сумму 5,51 BTC. Эта сумма эквивалентна 53 600 долларам США по текущему курсу.

Другой канал использовал адрес 3EtrSPskMRgwEEE9onLdmwcAFqaH9jj9rM и был даже успешнее первого: на этот адресу поступило 85 транзакций на общую сумму 11,25 BTC, то есть 109 606 долларов США.

В настоящее время все три взломанных канала уже были удалены или заблокированы, а журналисты в очередной раз напоминают пользователям о «золотом правиле» — избегать любых раздач криптовалюты и рекламных акций, если их организаторы обещают удвоить (утроить и так далее) любую сумму, которую им отправят». ***(Мария Нефёдова. Фальшивые каналы SpaceX на YouTube выманили у пользователей более 150 000 долларов // Xakep (https://xakep.ru/2020/06/10/fake-spacex/). 10.06.2020).***

***

«Несколько заводов корпорации Honda затронула масштабная кибератака. Из-за инцидента заводы в Бразилии и Индии были вынуждены на некоторое время приостановить работу. Пресс-служба Honda сообщает, что кибератака была направлена на внутренние серверы компании. Хакеры распространили вирус в компьютерной системе компании.

В заявлении добавляют, что после кибератаки заводы в Индии, Бразилии и Турции были вынуждены остановить производство. Завод в Турции уже возобновил деятельность, в отличие от двух других. "Служба безопасности компании Honda ведет расследование этого дела", - говорят представители корпорации.

Согласно информации СМИ с США, кибератака затронула 11 заводов Honda, 5 в Америке. Все заводы в США уже возобновили привычный график. Согласно предварительным данным, остановка заводов минимально повлияет на мировой рынок и бизнес компании в мире». ***(Мощная кибератака против Honda: Несколько заводов остановили свою работу // AvtoBlog.ua – Автомобильный портал (https://avtoblog.ua/news/moschnaja-kiberataka-protiv-honda-neskolko-zavodov-ostanovili-svoju-rabotu). 10.06.2020).***

***

«Специалисты команды IBM X-Force обнаружили целенаправленную фишинговую операцию против неназванной немецкой компании. Как пояснили исследователи, компания входит в рабочую группу, созданную правительством Германии для бесперебойного обеспечения медицинского персонала средствами индивидуальной защиты (СИЗ).

В период пандемии COVID-19 СИЗ востребованы, как никогда ранее, и страны мира соревнуются между собой в закупках масок и других средств защиты для медперсонала, имеющего дело с больными. Как и многие другие страны, Германия заручилась помощью некоторых крупнейших своих компаний для оказания помощи в закупках.

По мнению специалистов IBM X-Force, обнаруженная ими вредоносная операция направлена именно на эту компанию как раз потому, что она входит в правительственную рабочую группу по обеспечению медработников СИЗ (атаки начались сразу же после того, как компания вошла в состав группы). Более того, операция является частью плана неизвестной киберпреступной группировки по срыву поставок СИЗ в Германии.

По словам исследователей, атакующие тщательно продумали, какой отдел компании и когда атаковать. В настоящее время атаки находятся на ранней стадии – злоумышленники только рассылают фишинговые письма с целью выманить у сотрудников их учетные данные. Как они будут действовать дальше, перехватывать коммуникации сотрудников, продвигаться по корпоративным сетям или и то, и другое, пока неясно.

Кто стоит за операцией, рядовые киберпреступники или хакеры, финансируемые правительством какой-либо страны, также неизвестно. Тем не менее, проникнув в сети компании, правительственные хакеры могут добыть ценные сведения о закупках Германией средств индивидуальной защиты. Эта информация может обеспечить стороннему государству преимущество при осуществлении собственных закупок.

Однако есть еще одна возможная причина атак на компанию, считает специалист IBM X-Force Ник Россман (Nick Rossman). Не исключено, что хакеров интересуют не СИЗ, а нечто более существенное – вакцина против коронавируса.

«Укрепившись в сетях этих организаций, они, вероятно, смогут получить доступ к конфиденциальным данным, касающимся ресурсов компаний и/или национальных ресурсов COVID-19, стратегий реагирования и даже, возможно, прогресса в области разработки вакцин», - сообщил Россман». ***(Хакеры атакуют немецких производителей средств индивидуальной защиты // SecurityLab.ru (https://www.securitylab.ru/news/509101.php). 10.06.2020).***

****

«Специалисты Wordfence предупредили о масштабной кампании, нацеленной на WordPress-сайты. В минувшие выходные хакеры атаковали старые уязвимости в плагинах и попытались скачать с сайтов файлов конфигурации.

Исследователи сообщают, что атакующие использовали старые эксплоиты для скачивания или экспорта файлов wp-config.php с уязвимых сайтов, извлечения учетных данных от БД, а затем использовали полученные имена пользователей и пароли для захвата баз данных.

Аналитики Wordfence пишут, что на эту кампанию пришлось около 75% всех попыток использования уязвимостей в плагинах и темах для WordPress. Фактически атаки на захват файлов конфигурации утроились из-за произошедшего.

Wordfence заблокировала более 130 000 000 попыток эксплуатации различных уязвимостей, которые были нацелены более чем на 1 300 000 сайтов WordPress. Но нужно учитывать, что статистика компании охватывает только сайты данные ее собственной сети, а атаки явно были направлены и на другие сайты за ее пределами.

Атаки осуществлялись с 20 000 различных IP-адресов, большинство из которых ранее использовались в другой крупномасштабной кампании, так же нацеленной на сайты WordPress и активной в начале мая текущего года.

Так, во время первой кампании хакеры использовали ряд XSS-уязвимостей и пытались создать на уязвимых сайтах новых пользователей-администраторов и внедрить бэкдоры. Эта кампания была не менее масштабной, чем нынешняя, так как XSS-атаки неизвестной группы перевешивали все остальные XSS-аткки, проводимые другими хакерами вместе взятыми (см. иллюстрацию ниже). В общей сложности группировка попыталась взломать более 900 000 сайтов.

Теперь эксперты Wordfence считают, что обе кампании – это дело рук одной и то же хакерской группы, которая попросту пробует разные подходы». ***(Мария Нефёдова. Замечена масштабная кампания по взлому сайтов на WordPress // Xakep (https://xakep.ru/2020/06/04/wordpress-campaign-2/). 04.06.2020).***

***

«Каліфорнійський університет в Сан-Франциско зазнав кібератаки з використанням здирницького ПЗ.

Кіберзлочинність угруповання, відомі своїми атаками на установи охорони здоров'я, атакували Каліфорнійський університет в Сан-Франциско (UCSF) за допомогою здирницького ПЗ. Адміністрація університету підтвердила журналістам Bloomberg, що стала жертвою «незаконного вторгнення», але не уточнила, яка частина IT-інфраструктури постраждала.

Фахівці UCSF займають лідируючі позиції в США в області тестування антитіл і розробки лікування коронавірусної інфекції. За словами глави відділу зі зв'язків з громадськістю університету Пітера Ферлі (Peter Farley), дослідження за участю пацієнтів не були порушені кібератакою. Адміністрація UCSF повідомила про подію правоохоронним органам і звернулася за допомогою до експертів з кібербезпеки.

«З їх допомогою ми проводимо ретельну оцінку інциденту, в тому числі з'ясовуємо, яка інформація могла бути скомпрометована», – повідомив Ферлі, додавши, що не може розкрити ніяких подробиць, поки триває слідство.

Схоже, зловмисники зашифрували дані UCSF і зажадали викуп за їх відновлення. Оплата повинна бути здійснена до 8 червня цього року, і в разі

несплати вимагачі пообіцяли опублікувати «секретні дані» UCSF. Яку суму зажадали кіберзлочинці і яку здирницьку програму використовували, не уточнюється. Імовірно, університет міг стати жертвою здирницького ПЗ Netwalker, яка активно використовується кіберзлочинцями з вересня минулого року». ***(Лужна Софія. Лідируючий в США розробник вакцини проти COVID-19 став жертвою кібератаки // TechnoPortal.com.ua (https://technoportal.com.ua/programy/50410). 04.06.2020).***

***

«Сообщается, что компания Westech International подверглась кибератаке. Компания занимается предоставлением услуг по инженерному сопровождению и поддержанию работоспособности американских ядерных ракет Minuteman III. Это баллистические ракеты шахтного базирования с радиусом поражения более 9500 км.

Компания подтвердила, что подверглась кибератаке. Хакеры из группировки MAZE получили доступ к сети компании, зашифровали и украли некоторые данные, хранившиеся на компьютерах, и потребовали выкуп. Украденными файлами оказались электронный письма, платежные ведомости и другая «персональная информация» по выражению источника. На данный момент компания не сообщает, когда была совершена атака, а также каким образом она оказалась возможной. Сейчас проводится расследование, в том числе привлечены сторонние специалисты по информационной безопасности». ***(У компании, обслуживающей американские ядерные ракеты, украли данные // SecureNews (https://securenews.ru/us-nuclear-missile-service-company-stole-data/). 04.06.2020).***

***

«Дословно BEC переводится как «компрометация деловой электронной почты», и является разновидностью мошеннических схем, которые используют электронные переводы. Обычно BEC начинается с киберпреступников, которые взламывают корпоративную почту и подделывают электронные письма, чтобы выдать себя за одного из топ-менеджеров компании, обычно генерального или финансового директора. Иногда хакеры притворяются поставщиками. Оказавшись внутри корпоративной сети, киберпреступник запрашивает, казалось бы, законную оплату. Письмо выглядит очень правдоподобно, и кажется, что оно получено от руководителя, поэтому сотрудник подчиняется. Как правило, злоумышленники запрашивают перевод денег или чеки на хранение. Не зная об этом, сотрудник переводит средства на выбранный банковский счет, который принадлежит хакерам.

В случае BEC-атак злоумышленники используют тактику социальной инженерии, чтобы обмануть ничего не подозревающих сотрудников и руководителей. Как уже было сказано, они имитируют роль генерального директора или любого другого руководителя, уполномоченного делать или запрашивать электронные переводы. Кроме того, мошенники тщательно исследуют поведение и долго наблюдают за своими потенциальными жертвами и их компаниями, отслеживая все предстоящие сделки.

Обычно подобные аферы осуществлялись одним человеком. Однако в последнее время исследователи CheckPoint отмечают, что эти мошенничества становятся все более изощренными, и классифицируют их как организованную преступность. В апреле 2020 года исследователи Check Point опубликовали статью о том, как они раскрыли схему, в которой кибер-банда, которую исследователи назвали «флорентийским банкиром», выручила 1,3 миллиона долларов между тремя частными акционерными компаниями. В течение нескольких месяцев члены группы изучали электронные письма своих жертв, манипулируя корреспонденцией, регистрируя похожие домены и сразу обналичивая деньги. Экстренное вмешательство Check Point IncidentResponse привело к взысканию чуть более половины украденной суммы, оставшаяся часть была потеряна навсегда.

Исследователи Check Point считают, что коммерческие организации и венчурные компании являются основными целями BEC-атак, поскольку хакеры знают, что крупные организации часто переводят значительные денежные суммы. Поэтому этим организациям нужно хорошо понимать, как именно хакеры могут ими воспользоваться. Какие этапы можно выделить в подобной атаке?

Наблюдение. После того, как злоумышленники получат контроль над учетной записью электронной почты жертвы, они начнут читать электронные письма. Киберпреступники могут проводить дни, недели или даже месяцы, занимаясь разведкой, терпеливо составляя карту бизнес-схем и стандартных процедур, прежде чем активно вмешаться в общение

Контроль и изоляция. Злоумышленники начинают изолировать жертву от третьих лиц и коллег, создавая вредоносные правила почтовых ящиков. Эти правила электронной почты перенаправляют любые электронные письма с отфильтрованным содержимым или темами в папку, отслеживаемую хакерами, по сути создавая атаку «человек посередине».

Схожая настройка. Злоумышленники регистрируют похожие домены, те, которые визуально похожи на легитимные домены лиц, участвующих в той переписке, которую они хотят перехватить. Злоумышленник начинает отправлять электронные письма с похожих доменов. Они либо создают новый диалог, либо продолжают существующий, тем самым обманывая цель, полагая, что источник сообщения является законным.

Запрос на перевод денег. Злоумышленники начинают вводить информацию о своем банковском счете с помощью двух методов: перехват обычных, законных переводов и создание новых запросов на банковский перевод.

Перевод денег. Киберпреступники контролируют переписку, пока третье лицо не утвердит новые банковские реквизиты и не подтвердит транзакцию. Если банк отклоняет транзакцию из-за несоответствия в валюте счета, имени получателя или по любой другой причине, злоумышленники стараются максимально быстро исправить все ошибки, пока деньги не попадут в их собственные руки…

Включите многофакторную аутентификацию для учетных записей деловой почты. Этот тип аутентификации требует ввода нескольких частей информации для входа в систему, например, таких как пароль. Внедрение многофакторной аутентификации затрудняет доступ к электронной почте сотрудников киберпреступнику.

Не открывайте электронные письма от неизвестных отправителей. Если вдруг случайно вы это сделали, не нажимайте на ссылки и не открывайте вложения, поскольку они часто содержат вредоносные программы, которые получают доступ к вашей системе.

Дважды проверьте адрес электронной почты отправителя. Поддельный адрес электронной почты часто выглядит очень похоже на адрес электронной почты коллег или партнеров.

Всегда проверяйте требование перевода перед отправкой денег или данных. Разработайте стандартную рабочую процедуру для сотрудников, чтобы подтверждать запросы по электронной почте для банковского перевода или конфиденциальной информации.

Выбирайте опцию «переслать», а не «отвечать», отвечая на деловые письма. При пересылке электронного письма правильный адрес должен быть введен вручную или выбран из адресной книги. Переадресация гарантирует, что вы используете правильный адрес электронной почты получателя». ***(Удаленная работа провоцирует BEC-атаки // IKSMEDIA.RU (http://www.iksmedia.ru/news/5669227-Udalennaya-rabota-provociruet-BECat.html). 04.06.2020).***

***

«Исследователи Check Point идентифицировали киберпреступника, который написал в Твиттере, что его личная цель — взломать 5000 веб-сайтов по всему миру. Практически этого он и достиг, распространяя антиправительственные сообщения на веб-сайтах официальных ведомств, исследовательских учреждений и коммерческих организаций.

Исследователи Check Point раскрыли личность хакера-одиночки, ответственного за порчу тысяч официальных правительственных веб-сайтов по всему миру. Хакер работал с 2013 года под псевдонимом ‘VandaTheGod’.

Исследователи Check Point утверждают, что хакер руководствуется не деньгами, а хактивизмом — организацией кибератак, направленных на распространение определенной идеологии. VandaTheGodсосредоточился на социальной несправедливости и распространял сообщения, связанные с антиправительственными лозунгами. Например, хакер испортил веб-сайт правительства Бразилии с помощью хэштега #PrayforAmazonia в ответ на поджоги дождевого леса Амазонки, якобы проведенного правительством Бразилии.

США заняли первое место в списке хакеров

Соединенные Штаты занимают первое место в списке целей хакеров. Фактически, на веб-сайты США хакер совершил 57% своих кибератак (всего 612 веб-сайтов), в том числе, на официальный веб-сайт штата Род-Айленд и города Филадельфия. Хакерская деятельность также вышла за рамки хактивизма и включала в себя кражу кредитных карт и личных данных. Хакер попытался взломать аккаунты общественных деятелей, университетов и даже больниц. Так, VandaTheGod заявил в социальных сетях, что у него есть доступ к 1 миллиону медицинских карт пациентов из Новой Зеландии, при этом он предложил продавать каждый контакт по 200 долларов.

VandaTheGod рассказывал о своих успехах в социальных сетях, в первую очередь в Twitter. Зарегистрировавшись под несколькими псевдонимами, такими как «Vanda de Assis» и «SH1N1NG4M3», хакер написал, что его цель — взломать более 5000 веб-сайтов. VandaTheGod почти достиг своей цели: исследователи Check Point связали 4820 взломанных сайтов именно с этим хакером. Тем не менее, именно активность в социальных сетях обернулась против VandaTheGod, поскольку исследователи Check Point сначала обратили внимание именно на это.

Исследователи Check Point изучали учетные записи VandaTheGod в Twitter и Facebook, чтобы собрать улики, понять, кто стоит за этим. После тщательного изучения публикаций и твитов за несколько лет, эксперты CheckPoint обнаружили личность хакера. Им оказался человек, живущий в Уберландии, Бразилия. Эксперты CheckPoint передали полученные данные в соответствующие правоохранительные органы.

Лотем Финкелстин, руководитель группы по анализу угроз Check Point: «Мы видим уровень правонарушений, которые может создать на международном уровне даже один человек. Хотя первоначальным мотивом VandaTheGod была борьба против предполагаемой несправедливости, грань между хактивизмом и киберпреступностью тонкая. Мы часто видим, как хакеры начинают с цифрового вандализма, а дальше совершенствуют свои методы и переходят к краже учетных данных и краже денег. Раскрытие личности человека и передача этой информации правоохранительным органам должны положить конец его обширной подрывной и преступной деятельности». ***(Хактивист испортил сайты в более чем 40 странах // IKSMEDIA.RU (http://www.iksmedia.ru/news/5669020-Xaktivist-isportil-sajty-v-bolee.html). 03.06.2020).***

***

«Киберпреступники нашли новый способ вымогательства в университетах - кража конфиденциальной информации, а затем угроза поделиться ею в темной сети, если не будет выплачена награда.

За последние две недели хакеры успешно использовали три таких учреждения. Первым был Университет штата Мичиган , затем Университет Калифорнии, Сан-Франциско и, совсем недавно, Колумбийский колледж в Чикаго.

Ни одно из учреждений не сообщило, сколько было запрошено выкупа. Все они были атакованы с использованием вредоносного программного обеспечения, известного как NetWalker, и им был предоставлен срок оплаты в шесть дней.

Сообщается, что блог, поддерживаемый киберпреступниками за NetWalker, может похвастаться тем, что украденная информация из учреждений включает номера социального страхования и другую конфиденциальную информацию. Пользователи Twitter, такие как Ransom Leaks, поделились снимками экрана с примерами данных, которые публикуются в блоге, включая паспорта и банковские реквизиты.

Университет штата Мичиган публично заявил, что не будет платить выкуп хакерам на прошлой неделе - необычное заявление, так как многие учреждения не хотят обнародовать свой ответ на требования о выкупе. По сообщениям, 4 июня

хакеры начали публиковать данные, которые они украли в штате Мичиган, чтобы они были доступны для загрузки в темной сети.

«Выплата этим преступникам позволяет только увековечивать эти преступления и преследовать других жертв», - сказал в электронном письме временный руководитель службы информационной безопасности штата Мичиган Дан Айала. Он добавил, что решение о невыплате соответствовало руководству правоохранительных органов и было принято при поддержке попечительского совета и президента университета.

Атака штата Мичиган была ограничена подразделением физики и астрономии учреждения. В настоящее время неизвестно, сколько информации хакеры смогли получить, и сколько утекли сейчас, когда крайний срок хакера прошел. Айала сказал, что не смог поделиться многими подробностями о нападении, чтобы «защитить целостность текущего расследования».

По словам Айяла, студенты, преподаватели и сотрудники получают обновленную информацию о ситуации, которая разворачивается…

Решение не выплачивать выкуп было «в целом поддержано сообществом МГУ, особенно при том понимании, что выплата таких сумм увековечивает практику», сказала Айала. Но студенты по понятным причинам обеспокоены тем, какая информация могла быть украдена, сказала Брианна Айелло, вице-президент по академическим вопросам в Ассоциированных студентах Мичиганского государственного университета, организации студенческого самоуправления…

Платить или не платить?

Колумбийский колледж в Чикаго и Калифорнийский университет в Сан-Франциско, похоже, по-разному реагируют на атаки, говорит Бретт Каллоу, аналитик по угрозам в компании Emsisoft, занимающейся решениями кибербезопасности. «Их данных больше нет в блоге NetWalker, что говорит о том, что они либо заплатили выкуп, либо договорились о том, чтобы эту информацию убрали», - сказал он.

Ни одно из учреждений не ответило на вопросы о том, заплатили ли они выкуп, требуемый хакерами, или не рассмотрели масштаб нарушений. Как и в штате Мичиган, оба учреждения заявили, что не могут делиться большой информацией, так как расследование продолжается.

Калифорнийский университет в Сан-Франциско поделился заявлением, в котором подтвердил, что «незаконное вторжение в определенную область нашей ИТ-среды» было выявлено 1 июня.

Калифорнийский университет в Сан-Франциско является одним из научно-исследовательских учреждений, возглавляющих усилия в США по поиску возможных способов лечения COVID-19. В нескольких сообщениях СМИ высказывалось предположение, что это исследование и потенциально прибыльная связанная с ним интеллектуальная собственность, возможно, сделали учреждение привлекательной целью для хакеров.

Университет не подтвердил цель атаки.

«Мы считаем, что наши действия изолировали вторжение в область, на которую было нацелено», - говорится в заявлении университета. «Важно отметить,

что наши операции по оказанию медицинской помощи пациентам не затрагиваются, и инцидент не влияет на нашу общую сеть кампуса».

«Мы наняли фирму по информационной безопасности и обратились в правоохранительные органы. С их помощью мы проводим тщательную оценку инцидента, включая определение того, какая, если таковая имеется, информация могла быть скомпрометирована », - говорится в заявлении. «Чтобы сохранить целостность расследования, нам нужно будет ограничить то, что мы можем поделиться в это время»…

Высшие учебные заведения по закону обязаны защищать информацию о студентах, но имеют давнюю историю «действительно серьезных нарушений информации», с которыми не всегда обращаются хорошо, сказала Амелия Вэнс, директор по вопросам конфиденциальности молодежи и образования на форуме Future of Privacy…

По словам Вэнса, один из способов, с помощью которого учреждения могут попытаться предотвратить утечку конфиденциальных данных, - это обеспечить, чтобы они не держали информацию, в которой они не нуждаются. «Нам нужны учреждения, чтобы постоянно соблюдать правила гигиены данных», - сказала она.

Другим вариантом было бы для колледжей шифровать конфиденциальную информацию, которую они должны хранить. Это сделало бы украденную информацию практически бесполезной в темной сети, поскольку преступникам потребовалось бы время и деньги, чтобы взломать шифрование, сказал Вэнс. Проблема с шифрованием всего на институциональном уровне заключается в удобстве использования. «Если система слишком сложна, люди просто обойдутся, какой бы она ни была», - сказал Вэнс. «Трудно найти баланс, чтобы найти правильный путь для учреждений».

Университеты, в отличие от многих компаний, необычны тем, что они часто пытаются поддерживать относительно открытые сети для поощрения совместной работы и простоты использования, сказал Майк Стэнфилд, старший аналитик по безопасности в Центре прикладных исследований в области кибербезопасности в Университете Индианы. По его словам, поддерживать открытость при попытке защитить сеть невероятно сложно…

Многие атаки вымогателей являются результатом фишинговых писем, когда пользователи щелкают ссылку и непреднамеренно загружают вредоносное программное обеспечение. В последние месяцы фишинговые электронные письма использовали страх и путаницу, связанные с пандемией COVID-19, в своих интересах. По словам Стэнфилда, чтобы не допустить успеха фишинговых писем, учреждения могут обучать сотрудников колледжа распознавать подозрительные письма. По его словам, двухфакторная идентификация также является важной защитой.

Брайан Келли, директор по кибербезопасности в Educause, согласился, что это важные шаги, но они не обязательно защищают от атак NetWalker. Публично, ИТ-директора могут не делиться большой информацией о том, как происходят эти атаки, и о тех индикаторах, которые они ищут, но есть сети, где ИТ-лидеры обмениваются информацией, такие как сеть REN-ISAC, базирующаяся в

университете Индианы. «Мы можем помогать друг другу, не предупреждая хакера о том, что мы им помогаем», - сказала Келли.

Келли и Стэнфилд сошлись во мнении, что для высокопоставленных ИТ-руководителей важно следить за этими сетями и общаться со своими коллегами. Кибератаки постоянно развиваются, и неспособность идти в ногу с новым интеллектом может иметь ужасные последствия.

«Это постоянная игра в кошки-мышки», - сказала Келли. «Как только мы понимаем одну угрозу, возникает новая». ***(Lindsay McKenzie. Cyberextortion Threat Evolves // Inside Higher Ed (https://www.insidehighered.com/news/2020/06/11/colleges-face-evolving-cyber-extortion-threat). 11.06.2020).***

***

«**Эксперты Positive Technologies проанализировали кибератаки в I квартале и выяснили, что число киберинцидентов значительно выросло по сравнению с предыдущим кварталом.** Около 13% фишинговых атак были связаны с темой COVID-19, и все больше операторов шифровальщиков требуют выкуп за неразглашение похищенной информации.

По данным исследования, в первой четверти было выявлено на 22,5% больше кибератак, чем годом ранее. В течение квартала высокую активность проявляли 23 APT-группировки, атаки которых были направлены преимущественно на государственные учреждения, промышленные предприятия, финансовую отрасль и медицинские организации.

Как показал анализ, более трети (34%) всех атак на юридические лица с использованием вредоносного ПО составили атаки троянов-шифровальщиков. Эксперты отмечают, что некоторые операторы шифровальщиков создали собственные сайты, на которых публикуют похищенные у жертв файлы в случае отказа платить выкуп. Каждая десятая атака шифровальщиков была направлена на промышленность. При этом в начале года внимание многих специалистов по кибербезопасности привлек новый шифровальщик Snake, который умеет удалять теневые копии и останавливать процессы, связанные с работой промышленных систем управления.

Специалисты отмечают, что актуальность заражения вредоносами растет. При этом киберпреступники не ограничиваются одним типом зловредов: используют многофункциональные трояны либо загружают на скомпрометированные устройства несколько разновидностей. Чтобы предотвратить заражение, эксперты рекомендуют проверять вложения из электронных писем на предмет вредоносной активности с помощью решений класса sandbox.

По сравнению с последним кварталом прошлого года существенно выросла доля атак на госучреждения с использованием вредоносов (81 против 66%) и методов социальной инженерии (79 против 66%). По мнению экспертов Positive Technologies, этому могла способствовать ситуация с эпидемией: многие злоумышленники рассылали в госучреждения разных стран письма с вредоносными вложениями на тему коронавирусной инфекции.

Злоумышленники подхватили тему всеобщего беспокойства по поводу пандемии и стали использовать ее для фишинговых писем. По оценкам специалистов, около 13% всех фишинговых рассылок в I квартале были связаны с темой COVID-19. Чуть менее половины из них (44%) пришлись на частных лиц, а каждая пятая рассылка была направлена на государственные организации».

«Рост числа фишинговых рассылок на тему COVID-19 наши эксперты фиксируют со второй половины января, – отметил Алексей Новиков, директор экспертного центра безопасности Positive Technologies (PT Expert Security Center). – Эпидемией пользовались как для проведения массовых вредоносных кампаний, так и для сложных целенаправленных атак (APT-атак). Под видом официальной информации о статистике заражений, мерах профилактики и вакцине, рассылаемой якобы от имени государственных органов и медицинских учреждений, в I квартале распространялось вредоносное ПО Emotet, Remcos, AZORult, Agent Tesla, LokiBot, TrickBot и множество других троянов. Рассылки писем с вредоносными вложениями на тему эпидемии проводили группы TA505, Hades, Mustang Panda, APT36, SongXY, а также южнокорейская группировка Higaisa». ***(В первом квартале количество кибератак выросло почти на четверть // Компьютерное Обозрение (https://ko.com.ua/v_pervom_kvartale_kolichestvo_kiberatak_vyroslo_pochti_na_chetvert_133415). 17.06.2020).***

***

«Специалисты международного разработчика антивирусного программного обеспечения, эксперта в области киберзащиты – компании ESET обнаружили новые целенаправленные атаки на пользователей социальной сети LinkedIn, для осуществления которых злоумышленники использовали методы фишинга и выдавали себя за других людей, сообщает пресс-служба компании ESET. «Очевидно, что целью киберпреступников был не только шпионаж, но и финансовая выгода. Атаки с использованием образца вредоносного программного обеспечения «Inception.dll» происходили в сентябре-декабре 2019 года. А основными целями злоумышленников стали аэрокосмические и военные компании в Европе и на Ближнем Востоке», - говорится в сообщении.

Согласно сообщению, для заражения целей киберпреступники использовали приемы социальной инженерии в LinkedIn, маскируясь под привлекательными, но фальшивыми предложениями о работе. «Сообщение было вполне правдоподобным предложением о работе якобы от имени известной компании в соответствующем секторе. Конечно, профиль LinkedIn был поддельным, а файлы, отправленные в ходе общения — вредоносными», — приводит пресс-служба слова исследователя компании ESET Доминика Брайтенбахера. По данным ESET, хакеры отправляли файлы с помощью мессенджера в LinkedIn или через сообщения электронной почты, которые содержали ссылку на OneDrive. Для последнего варианта киберпреступники создали учетные записи электронной почты, которые соответствовали их поддельным профилям в LinkedIn. После открытия файла пользователь видел, казалось бы, обычный PDF-документ с информацией о заработной плате, связанной с фальшивым предложением работы. Однако на самом

деле злоумышленники заражали компьютер жертвы вредоносным программным обеспечением.

В пресс-службе ESET добавили, что среди инструментов злоумышленников были сложные многомодульные вредоносные программы, которые часто маскировались под легитимное программное обеспечение, а также модифицированные версии инструментов с открытым исходным кодом. Кроме того, киберпреступники несанкционированно использовали существующие в операционной системе Windows стандартные утилиты для выполнения различных вредоносных операций. «Атаки, которые мы исследовали, показали все признаки шпионажа, которые указывают на возможную связь с известной группой киберпреступников Lazarus. Однако исследования и анализ вредоносных программ не позволили понять, на какие именно файлы нацелены преступники», — цитирует пресс-служба Брайтенбахера. Кроме шпионажа, киберпреступники использовали скомпрометированные учетные записи для выманивания денег у других компаний. Как сообщал УНИАН, ранее специалисты ESET обнаружили новые атаки группы хакеров Gamaredon на пользователей Microsoft Outlook и Office. По данным ESET, в Украине ежедневно фиксируется около 300 тыс. новых киберугроз для информационной безопасности. При этом, найти хакеров-злоумышленников крайне сложно, компаниям остается лишь проводить ежеминутные мониторинги на предмет выявления киберугроз с целью их дальнейшего блокирования. Компания ESET – ведущий разработчик решений в области компьютерной безопасности и эксперт в сфере IT-безопасности. Компания была основана в 1992 году в Словакии и на сегодня представлена более, чем в 180 странах мира». ***(Специалисты по кибербезопасности обнаружили новые хакерские атаки на пользователей LinkedIn // УНИАН (https://www.unian.net/science/specialisty-po-kiberbezopasnosti-obnaruzhili-novye-hakerskie-ataki-na-polzovateley-linkedin-novosti-11039444.html). 17.06.2020).***

****

«Исследователи из Check Point раскрыли сложную фишинговую кампанию, нацеленную на сбор корпоративных данных, которые хранятся в учетных записях Microsoft Office 365. Для того, чтобы избежать обнаружения программами безопасности, злоумышленники использовали названия известных организаций – Оксфордского университета, Adobe и Samsung.

Чтобы рассылать своим жертвам вредоносные письма, хакеры взломали почтовый сервер Оксфордского университета. В электронных письмах содержались ссылки, которые перенаправляли жертв на сервер Adobe – ранее он использовался компанией Samsung. Это позволяло хакерам создать видимость легитимного домена Samsung – это повышало доверие у жертв. Таким образом, жертвы перенаправлялись как бы на страничку ввода учетных данных для входа в Office 365.

В начале апреля исследователи Check Point стали просматривать электронные письма, отправленные жертвам с темой «Голосовая почта Office 365». Электронные письма сообщали, что для прослушивания письма нужно перейти по ссылке. Если

жертва нажимала на ссылку, ее перенаправляли на фишинговую страницу, маскирующуюся под страницу входа в Office 365.

Письма приходили с нескольких сгенерированных адресов, которые принадлежали настоящим поддоменам разных отделов Оксфордского университета. Заголовки электронной почты показывают, что хакеры нашли способ злоупотребить одним из Оксфордских SMTP-серверов (простой протокол передачи почты), основными функциями которого является отправка, получение и/или ретрансляция исходящей почты. Использование законных Оксфордских SMTP-серверов позволило хакерам пройти проверку репутации, которую требуют меры безопасности для домена отправителя.

За прошедший год открытые перенаправления Google и Adobe использовались фишинговыми кампаниями для придания легитимности URL-адресам, используемым в спам-письмах. Открытое перенаправление – URL-адрес на веб-сайте, который может использоваться любым лицом для перенаправления пользователей на другой сайт. В этом случае ссылки в сообщении электронной почты будут перенаправлены на сервер Adobe, ранее использовавшийся компанией Samsung во время маркетинговой кампании киберпонедельника 2018 г. Другими словами, ссылка, встроенная в исходное фишинговое электронное письмо, является частью доверенного домена Samsung, по которому, не зная об этом, жертвы перенаправляются на веб-сайт, размещенный хакерами. Используя определенный формат ссылок Adobe Campaign и законный домен, злоумышленники увеличили шансы своей электронной почты на обход защитных решений на основе репутации, черных списков и шаблонов URL.

Компания Check Point проинформировала Оксфордский университет, компании Adobe и Samsung о своих выводах». ***(Взломанный почтовый сервер Оксфордского университета использовался для фишинга // Компьютерное Обозрение(https://ko.com.ua/vzlomannyj_pochtovyj_server_oksfordckogo_universiteta_ispolzovalsya_dlya_fishinga_133473). 22.06.2020).***

***

«Как показала статистика «Лаборатории Касперского», в апреле количество ежедневных попыток перейти на зараженные сайты, эксплуатирующие игровую тему, в мире выросло на 54% по сравнению с январем. Чаще всего злоумышленники использовали название игры Minecraft, чтобы привлечь внимание пользователей. Оно фигурировало в более чем 130 тыс. атак.

Также использовалось название одной из самых популярных игровых платформ – Steam. Число попыток переходов на фишинговые страницы с отсылками к ней в апреле выросло на 40% по сравнению с февралем.

Приманками для пользователей также становились обещания бесплатных версий популярных игр, обновлений и расширений, а также читов. По ссылкам распространялись разные типы вредоносного ПО – от программ для кражи паролей до вымогателей и майнеров.

Чтобы не стать жертвой кибератаки, эксперты рекомендуют: использовать для защиты игрового аккаунта сложные длинные пароли и, где это возможно,

двухфакторную аутентификацию; помнить о том, что злоумышленники часто используют для распространения вредоносного ПО читы и пиратские копии видеоигр; использовать защитное решение, которое умеет распознавать киберугрозы, блокировать фишинговые сайты и предотвращать переходы на вредоносные страницы; не выключать защитное решение в процессе игры. Чтобы оно потребляло меньше ресурсов, можно включить специальный игровой режим». ***(Для привлечения внимания геймеров кибер-преступники чаще всего используют название игры Minecraft // Компьютерное Обозрение (https://ko.com.ua/dlya_privlecheniya_vnimaniya_gejmerov_kiber-prestupniki_chashhe_vsego_ispolzuyut_nazvanie_igry_minecraft_133447). 19.06.2020).***

***

«Amazon объявила, что в середине февраля этого года её службе AWS Shield удалось остановить крупнейшую из когда-либо зарегистрированных атак методом распределённого отказа в обслуживании (DDoS).

Об этом инциденте, в котором поток данных, сгенерированных ботнетом достиг 2,3 терабит в секунду, рассказывается в подробностях в опубликованном Amazon отчёте AWS Shield Threat Landscape.

В нападении на неназванного клиента AWS, заставившем компанию ввести для персонала AWS Shield 3-дневный режим повышенной готовности, были задействованы взломанные веб-серверы CLDAP. Протокол CLDAP (Connection-less Lightweight Directory Access Protocol) это альтернатива устаревшему LDAP, которая применяется для подключения к доступным из Интернета каталогам, для поиска и модификации хранящейся в них информации.

Первые попытки злонамеренного использования CLDAP отмечены в конце 2016 г. Серверы CLDAP с тех пор стали желанной целью для оркестраторов DDoS-атак благодаря их способности увеличивать вредоносный трафиик в 56-70 раз.

До сих пор крупнейшей считалась атака с объёмом DDoS-трафика 1,7 Тб/с, которую NETSCOUT Arbor блокировала в марте 2018 года. В ней использовалась сеть из скомпрометированных серверов Memcached.

После этого массовые атаки DDoS, стали редкостью из-за согласованной работы Интернет-провайдеров, сетей доставки контента и других ведущих сетевых игроков над повышением безопасности уязвимых систем Memcached.

Последние годы крупными считались атаки с пиковым трафиком порядка 500 Гб/с, поэтому инцидент с AWS стал неприятным сюрпризом для всей сетевой индустрии, тем более, что он может указывать на новую тенденцию. Подтверждением тому является вчерашнее сообщение Akamai о DDoS-атаке с трафиком 1,44 Тб/с, остановленной в первую неделю июня 2020 г.» ***(AWS отразила величайшую атаку DDoS в истории // Компьютерное Обозрение(https://ko.com.ua/aws_otrazila_velichajshuyu_ataku_ddos_v_istorii_133435). 18.06.2020).***

***

«Исследователи информационной безопасности предупреждают о фишинговой кампании, осуществляемой из Северной Кореи в адрес многих стран. Атака нацелена на извлечение выгоды из мер поддержки, оказываемых правительствами населению и бизнесу.

Кампания проводится знаменитой Пхеньянской группировкой Lazarus, выдающей себя за правительственные учреждения, департаменты и торговые ассоциации, которым поручено следить за выплатой помощи.

Стартап Cyfirma, работающий в области кибербезопасности и поддерживаемый Goldman Sachs, заявил, что по их данным атака запланирована для развертывания в США, Великобритании, Индии, Японии, Сингапуре и Южной Корее.

Исследователи утверждают, что впервые обнаружили свидетельства операции в начале месяца. Ими стали семь шаблонов электронных писем, от имени якобы правительственных департаментов и учреждений, таких как Банк Англии, Министерство трудовых ресурсов Сингапура, Министерство финансов Японии и Министерство сельского хозяйства США.

По всей видимости, группа будет использовать для рассылки миллионы адресов и деловых контактов. Одна из приманок, используемых в письмах — сообщение о новой государственной выплате в поддержку бизнеса». ***(Северная Корея проводит массовую фишинговую кампанию // SecureNews (https://securenews.ru/north-korea-conducts-a-massive-phishing-campaign/). 23.06.2020).***

***

«В 2019 году зафиксировано 248 случаев утечек из облачных хранилищ, что привело к компрометации 8,35 млрд записей персональных и платежных данных в мире и 122 млн в России. Соответственно, это более 56% всех утекших за год записей данных в мире и 68% в России. Экспертно-аналитический центр группы компаний InfoWatch опубликовал отчет об утечках конфиденциальной информации из незащищенных серверов на облачных сервисах.

Экспертно-аналитический центр группы компаний InfoWatch опубликовал отчет об утечках конфиденциальной информации из незащищенных серверов на облачных сервисах.

По итогам 2019 года аналитики отмечают рост утечек из незащищенных серверов на облачных сервисах в 3,5 раза по сравнению с 2018 годом. В ходе исследования на основании сведений из публичных источников аналитики рассчитали, что, в среднем каждый выявленный незащищенный сервер приводил к утечке 33,7 млн записей в глобальном масштабе и 1,85 млн записей в России.

В последние годы отмечается стабильный рост рынка сервисов на основе публичных облаков. Согласно отчету Gartner, в 2019 г. объем данного рынка составил $227,8 млрд, а в 2020 году он может вырасти на 17% и превысит $266 млрд. Квартет мировых лидеров в области услуг на базе публичных облаков составляют Amazon, Microsoft, Google и Alibaba – в сумме на них приходится 72% рынка. Российский рынок облачных сервисов менее зрелый, относительно слабо консолидирован, имеет большой потенциал роста и с задержкой на один-два года

повторяет структурные изменения, сложившиеся в мире. «Все больше отечественных компаний доверяют хранение своих данных, в том числе довольно критичных, провайдерам «облачных» услуг. Одно из исключений – финансовый сектор, который не готов к миграции на облачные сервисы по ряду технологических причин, из-за требований регуляторов в области ИБ, а также из-за вполне осязаемых и понятных рисков кибербезопасности», - отмечает Андрей Арсентьев, руководитель направления аналитики и спецпроектов ГК InfoWatch.

В России в 2019 году зарегистрировано 66 утечек данных с облачных серверов, что в 22 раза превышает показатель 2018 г., скомпрометированными оказались более 122 млн записей ПДн и платежной информации. Стоит отметить, что почти 90% утечек из хранилищ в незащищенных облачных сервисах в России пришлись на персональные данные, при этом более 40% случаев произошли в хайтек-индустрии. По результатам исследования одной из самых уязвимых российских вертикалей оказалось здравоохранение. Аналитики связывают это с набирающей ход цифровизацией государственных клиник и развитием во многих регионах направления коммерческой медицины. Однако при переходе на облачные услуги медучреждения порой не уделяют должного внимания контролю конфигурации используемых ресурсов. Впрочем, проблема безопасности конфиденциальных данных, хранящихся на серверных мощностях в публичных облачных сервисах, сегодня в той или иной степени актуальна для всех отраслей как в России, так и во всем мире.

«Стараясь сократить капитальные затраты на инфраструктуру, предприятия ищут удобные и гибкие способы хранения своих данных, мигрируют на облачные сервисы, забывая об элементарных правилах безопасности. Изученные в ходе исследования случаи позволяют говорить о том, что компании все чаще переносят в «облака» данные высокого уровня важности: широкий спектр клиентской информации, коммерческие сведения, даже медицинские данные, потеря которых весьма чувствительная для любого человека. Как показывает мировая практика, на случайно открытый сервис может зайти не только пытливый исследователь безопасности или другой человек без недобрых намерений, но и злоумышленник, владеющий современными автоматизированными инструментами изучения подключенных к Сети ресурсов. При поиске уязвимых сервисов одной из мотиваций для киберпреступников служат случаи проявления халатности со стороны операторов облачных ресурсов. Неправильная конфигурация таких ресурсов – прямой путь к утечке», - говорит Андрей Арсентьев.

Исследование показало, что, несмотря на значительный рост рынка облачных сервисов и повышение доверия к ним со стороны заказчиков, в данном ИТ-направлении сохраняются многие проблемы в области кибербезопасности. Особое внимание необходимо уделить защите облачных сервисов на основе свободного ПО, также компании должны регулярно проводить аудит подключенных к Сети хранилищ и заботиться о повышении квалификации администраторов, обслуживающих облачные серверы». ***(Более половины конфиденциальной информации в мире утекает из облачных сервисов // IKSMEDIA.RU (http://www.iksmedia.ru/news/5673089-Bolee-poloviny-konfidencialnoj-info.html). 18.06.2020).***

****

«Издание The Register сообщает, что специалисты компании Emsisoft обнаружили весьма интересную атаку. Операторы шифровальщика Maze случайно атаковали нью-йоркскую фирму, занимающуюся архитектурно-строительными работами, хотя собирались устроить атаку на Канадскую ассоциацию стандартизации.

Дело в том, что если поискать в Google «csa group», почти все результаты поиска будут связаны с Канадской ассоциацией стандартизации (Canadian Standards Association, CSA), но есть одно исключение: архитектурно-строительная фирма из Нью-Йорка — CSA Group.

Так сложилось, что эта фирма носит практически такое же имя, что и Канадская ассоциация стандартизации, и использует почти аналогичный домен: csagroup[.]com, тогда как ассоциации принадлежит домен csagroup[.]org.

Из-за этого совпадения фирма попала атаку вымогателей. Напомню, что малварь Maze не только шифрует файлы на зараженных машинах, но предварительно похищает из сетей жертв данные, которые хакеры затем используют в качестве рычага давления.

Бретт Кэллоу, аналитик компании Emsisoft, обнаружил ошибку хакеров, когда изучал опубликованный на сайте вымогателей дамп, который те обнародовали, пытаясь угрожать взломанной CSA Group и вынуждая компанию заплатить выкуп. Исследователь проверил файлы и нашел среди них документы, относящиеся к проектированию и строительству зданий в Пуэрто-Рико. Некоторые файлы, судя по всему, были отправлены с ящиков на csagroup[.]com, а это свидетельствует о том, что жертвами вымогателей стали архитекторы, а не Канадская ассоциация стандартизации.

Аналитик пишет, что это не первый подобный случай на его памяти. Ранее специалисты наблюдали, как операторы шифровальщика DoppelPaymer атаковали совсем не тот банк, который планировали, именно из-за того что названия двух финансовых учреждений оказались похожи. Кэллоу отмечает, что у создателей DoppelPaymer хотя бы хватило приличий опубликовать извинения и признать свою ошибку.

Эксперт Emsisoft полагает, что причиной ошибки операторов Maze стала работа в стрессовых условиях, ведь пандемия COVID-19 эффективно лишает компании наличных денег и возможности платить вымогателям выкупы. Он отмечает, что группировка намекала на это в одном из своих недавних сообщений, которое гласило: «Мы живем в той же экономической реальности, что и вы. Именно поэтому мы предпочитаем работать в рамках соглашений и всегда готовы к компромиссам».

На сайте Maze рядом с дампом данных по-прежнему значится название не той компании. Журналисты The Registe предприняли попытку связаться с представителями CSA Group (нью-йоркские архитекторы), но это оказалось затруднительно, так как фирма отключила свой сайт и практически неактивна в социальных сетях». ***(Мария Нефёдова. Операторы шифровальщика Maze по***

ошибке атаковали не ту компанию // Xakep (https://xakep.ru/2020/06/19/csa-group-is-not-csa/). 19.06.2020).

***

«Когда компания подвергается атаке с использованием вымогательского ПО, многие жертвы считают, что злоумышленники быстро устанавливают вредоносы и покидают сеть во избежание обнаружения. Но на самом деле преступники не так быстро отказываются от скомпрометированного ресурса, сообщило издание BleepingComputer.

Вместо этого кибератаки могут совершаться спустя несколько дней и недель после взлома уязвимой сети. Взлом может быть осуществлен с помощью уязвимой службы удаленного рабочего стола, уязвимостей в программном обеспечении VPN или путем удаленного доступа, предоставленного вредоносными программами, такими как TrickBot, Dridex и QakBot.

Преступники используют такие инструменты, как Mimikatz, PowerShell Empire и PSExec для хищения учетных данных и перемещения по сети. Получив доступ к компьютерам в сети, злоумышленники используют похищенные учетные данные для кражи конфиденциальных данных с устройств резервного копирования и серверов перед развертыванием вымогателей. Многие жертвы ошибочно предполагают, что на данном этапе преступники покидают скомпрометированную сеть, однако это убеждение далеко от истины.

Например, операторы вымогательского ПО Maze сообщили на своем сайте о взломе сети дочерней компании ST Engineering под названием VT San Antonio Aerospace (VT SAA). Преступники опубликовали документ, содержащий отчет IT-отдела жертвы об их атаке. Как показывает украденный документ, операторы Maze все еще скрывались в сети жертвы и продолжали похищать файлы, пока продолжалось расследование инцидента». ***(Операторы вымогательского ПО продолжают скрываться в сетях жертв после атак // SecurityLab.ru (https://www.securitylab.ru/news/509381.php). 22.06.2020).***

***

«Около четырех лет итальянская компания CloudEyE занималась легальным, на первый взгляд, бизнесом, предлагая защиту бинарников от реверс-инжиниринга для Windows-приложений, однако одновременно с этим фирма тайно рекламировала свои услуги на черном рынке и сотрудничала с операторами вымогательских программ.

Все это обнаружили эксперты компании Check Point, когда стали расследовать деятельность малвари GuLoader (1, 2, 3), чья активность заметно возросла с 2020 году.

Исследователи утверждают, что обнаружили в коде GuLoader упоминания CloudEyE Protector, защитного решения, созданного компанией CloudEyE. И если в целом подобные продукты для защиты исходного кода вполне легальны и широко используются разработчиками большинства коммерческий приложений, то в данном случае исследователи уверены, что CloudEyE и ее владельцы активны на хакерских форумах уже много лет.

Дело в том, что аналитикам Check Point удалось связать защитный продукт CloudEyE, продвигаемый на сайте securitycode.eu, с рекламой криптингового сервиса для малвари под названием DarkEyE, который широко рекламировался на хакерских форумах еще в 2014 году. Более того, эксперты также связали трех пользователей и три адреса электронной почты, замеченных в продвижении DarkEyE, с реальной личностью одного из основателей CloudEyE.

Исследователи пишут, что эти email-адреса и имена пользователей фигурируют в ряде сообщений на хакерских форумах. В этих публикациях рекламируются сервисы шифрования бинарников и малвари, причем сообщения датированы временами до DarkEyE, то есть они были написаны еще в 2011 году.

Основываясь на этом, эксперты делают вывод, что скрывающийся под этими псевдонимами человек давно и плотно связан с сообществом киберпреступников. Эксперты полагают, что именно эти старые связи помогли компании начать законный бизнес. Так, на официальном сайте разработчики CloudEyE хвастаются тем, что компания насчитывает более 5000 клиентов.

Аналитики Check Point подсчитали, что, исходя из минимальной ставки в 100 долларов в месяц, в общей сложности компания заработала не менее 500 000 долларов. Однако сумма может быть и намного больше, если принять во внимание, что стоимость некоторых ежемесячных подписок может доходить до 750 долларов, а многие клиенты явно использовали эту услугу несколько месяцев.

Исследователи говорят, что все «улики» указывают на то, что операторы CloudEyE попытались узаконить свою преступную деятельность, скрыв ее за подставной компанией, чтобы оправдать прибыли и избежать излишнего внимания со стороны местных налоговых органов при обналичивании огромных сумм.

«Операции CloudEyE могут выглядеть законными, но услуга, предоставляемая CloudEyE, была общим знаменателем в тысячах атак за последний год», — гласит отчет Check Point.

Хотя эксперты утверждают, что в последние годы DarkEyE и CloudEyE использовались весьма широко, похоже, основным клиентом разработчиков является лишь одна вредоносная кампания, это уже упомянутый выше шифровальщик GuLoader.

В своем отчете Check Point рассказывает о множестве связей между CloudEyE и GuLoader. Во-первых, наиболее очевидной их них является тот факт, что код приложений, прошедших через CloudEyE Protect, содержит паттерны, крайне похожие на образцы GuLoader, обнаруженные экспертами.

Дошло до того, что любое случайное приложение, прошедшее через CloudEyE Protect, практически наверняка будет обнаруживаться как вредоносное ПО GuLoader, хотя на самом деле это безобидное и легитимное приложение.

Во-вторых, аналитики Check Point заметили, что интерфейс CloudEyE содержал URL-заглушку, которую часто обнаруживали и в образцах GuLoader. В-третьих, многие функции CloudEyE, похоже, были специально разработаны для операций GuLoader.

«Учебные руководства, опубликованные на сайте CloudEyE, демонстрируют, как хранить полезные нагрузки в “облаках”, в том числе в Google Drive и OneDrive. Облачные хранилища обычно выполняют антивирусную проверку и технически не

позволяют загружать вредоносные программы. Однако шифрование полезной нагрузки, реализованное в CloudEyE, помогает обойти это ограничение», — отмечают эксперты.

Исследователи говорят, что подобная функциональность не имеет смысла для обычного приложения, а вот для малвари умение избегать облачных сканирований может оказаться весьма полезным. Особенно актуально подобное может быть для GuLoader, который представляет собой «сетевой загрузчик», то есть заражает компьютер жертвы, а затем скачивает полезную нагрузку второго уровня из Google Drive или Microsoft OneDrive.

После публикации отчета Check Point представители CloudEyE выступили с официальным заявлением и опровергли все выводы специалистов. Компания заявляет, что ее инструмент мог использоваться преступниками без ведома самих разработчиков. При этом работа компании была остановлена на неизвестный срок.

Некоторые ИБ-специалисты уже назвали заявление компании весьма плохой ложью и призвали итальянские власти провести расследование в отношении CloudEyE и двух ее основателей». ***(Мария Нефёдова. Итальянская компания заработала больше 500 000 долларов, работая с операторами шифровальщиков // Xakep (https://xakep.ru/2020/06/15/cloudeye-darkeye/). 15.06.2020).***

***

«Основатель WikiLeaks Джулиан Ассанж пытался завербовать хакеров на конференциях в Европе и Азии ради получения секретной информации для своего веб-сайта, а также вступил в сговор с членами хакерских организаций для получения правительственных секретов, говорится в новом обвинительном заключении Министерства юстиции США.

В документе утверждается о сговоре Ассанжа с хакерами из группировок LulzSec и Anonymous. В министерстве считают, что Ассанж и другие сотрудники организации завербовали хакеров и согласовали с ними взлом компьютеров в интересах WikiLeaks. В частности, основатель организации просил хакеров присылать данные ЦРУ, АНБ, The New York Times, а в 2010 году получил несанкционированный доступ к правительственной компьютерной системе одной из стран НАТО.

Минюст США уточняет, что второе обвинительное заключение не предусматривает новых обвинений в дополнение к 18 пунктам, выдвинутым в мае 2019 года. Но оно расширяет масштаб сговора с целью компьютерного взлома, который вменяют в вину Ассанжу.

Ассанж находится в тюрьме в Великобритании, его приговорили к 50 неделям заключения за нарушение условий освобождения под залог в 2012 году. Тогда его обвиняли в сексуальных домогательствах в Швеции, и Великобритания решала вопрос о его экстрадиции. Выйдя под залог, Ассанж не явился в суд и укрылся в посольстве Эквадора в Лондоне.

Он находился там до апреля 2019 года. Тогда его задержали в посольстве Эквадора после того, как страна отозвала его убежище и объявила о выселении. Президент Эквадора Ленин Морено обвинил Ассанжа в агрессивном поведении и нарушении международных соглашений. Власти США добиваются экстрадиции

Ассанжа, ему грозит по совокупности до 175 лет заключения». ***(Минюст США обвинил Джулиана Ассанжа в привлечении хакеров для получения госсекретов // РосКомСвобода (https://roskomsvoboda.org/60370/). 25.06.2020).***

***

«Специалисты Akamai рассказали, что в прошлое воскресение, 21 июня 2020 года, крупный европейский банк (название не раскрывается) стал мишенью для одной из мощнейших DDoS-атак в истории. Хотя мощность этой атаки составила лишь 418 Гбит/сек, при этом эксперты фиксировали до 809 миллионов пакетов в секунду.

Здесь стоит напомнить, что DDoS-атаки тоже бывают разными: их интенсивность измеряется в битах в секунду (BPS), пакетах в секунду (PPS) или запросах в секунду (RPS). Так, атаки на максимальный BPS обычно направлены на исчерпание интернет-канала, PPS чаще используются для атак на сетевые устройства и приложения в облаках и дата-центрах, а обычные мишени RPS-атак — это edge-серверы, где выполняются веб-приложения.

Исследователи пишут, что инцидент длился совсем недолго (около 10 минут), но атака «разогналась» до опасной мощности очень быстро. Потребовалось лишь несколько секунд, чтобы нормальный уровень трафика поднялся до 418 Гбит/сек, и около двух минут, чтобы атака достигла пика в 809 миллионов пакетов в секунду.

По мнению экспертов, за этим инцидентом стоит новый ботнет, таким образом впервые заявивший о себе. Этот вывод основан на большом количестве IP-адресов, участвовавших в атаке, многие из которых были замечены впервые: аналитикам компании оказались неизвестны 96,2% из них. Во время атаки количество IP-адресов, обычно наблюдаемых для этого клиента, подскочило в 600 раз.

Akamai заявляет, что это новый рекорд в области DDoS-атак типа PPS. Предыдущая мощнейшая атака в данной области произошла ранее в этом месяце и демонстрировала лишь 385 миллионов пакетов в секунду, то есть теперь предыдущий показатель был превзойден более чем вдвое.

Эксперты отмечают, что новая атака явно была оптимизирована для противодействия системам защиты от DDoS-атак и ориентировалась именно на максимальный показатель PPS. Так, отправленные злоумышленниками пакеты имели полезную нагрузку всего 1 байт при общем размере пакета 29 байт с заголовками IPv4, что скрывало их среди нескольких миллиардов пиров…». ***(Мария Нефёдова.Зафиксирован новый DDoS-рекорд: 809 миллионов пакетов в секунду // Xakep (https://xakep.ru/2020/06/26/809-mpps/). 26.06.2020).***

***

Діяльність хакерів та хакерські угруповування

«IT-компанію BellTroX InfoTech Services, розташовану в Делі, викрили в міжнародному шпигунстві. Протягом 7 років там на замовлення нібито зламали більше 10 тисяч облікових записів електронної пошти…

Хакери розробили десятки тисяч шкідливих повідомлень, і з 2013 року відправляли їх на пошту з метою виманити паролі. Як розповіли виданню три колишніх співробітники компанії, BellTroX атакувала європейських урядовців, власників казино на Багамах та відомих інвесторів у США.

У розмові з Reuters власник BellTroX Суміт Гупта відмовився називати імена замовників і не вважає, що займався чимось злочинним. Та дослідники організації Citizen Lab, які роками вивчали інфраструктуру кібершпигунства, випустили офіційний звіт, де запевняють, що індійські хакери виконували шпигунські дії.

«Це одна з найбільш розкритих замовних операцій з кібершпигунства», – запевнили експерти.

За фактом атак BellTroX на цілі в США нині ведеться розслідування…». ***(Індійську IT-компанію викрили у міжнародному шпигунстві // MEDIASAPIENS (https://ms.detector.media/it-kompanii/post/24854/2020-06-11-indiisku-it-kompaniyu-vikrili-u-mizhnarodnomu-shpigunstvi/). 11.06.2020).***

***

«Лаборатория Касперского» выявила, что APT-группировка Cycldek, которая ведёт свою деятельность по крайней мере с 2013 года, обладает гораздо более сложным набором инструментов, чем предполагалось ранее. Так, эксперты обнаружили вредоносное ПО USBCulprit, которое предназначено для кражи данных из корпоративной сети и даёт злоумышленникам возможность проникнуть в отключённые от сети физически изолированные устройства. Этот зловред активен с 2014 года, новые образцы появлялись в 2019 году.

Цели Cycldek (также известной как Goblin Panda, APT 27 и Conimes) – это преимущественно крупные организации и правительственные учреждения в Юго-Восточной Азии. Эксперты «Лаборатории Касперского» пристально следят за её деятельностью во Вьетнаме, Таиланде, Лаосе. Они обнаружили, что после 2018 года большинство атак начиналось с фишингового письма с RTF-вложением на политические темы, открытие которого приводило к использованию известных уязвимостей и загрузке зловреда NewCore RAT. Он, в свою очередь, устанавливал вредоносное ПО USBCulprit, которое изучает пути к исполняемым файлам и собирает документы с определёнными расширениями, а затем переносит их на подключаемые USB-устройства. Таким образом, можно предположить, что цель зловреда — не подключённые к интернету или физически изолированные устройства, на которые передавать данные можно только с помощью носителей.

При подключении промаркированных USBCulprit флешек зловред или загружает туда украденные данные, или, наоборот, забирает данные, которые были записаны копией USBCulprit на отключённом от сети компьютере в зависимости от конфигурации и полученных команд. Эта программа умеет находить специфические файлы, включая те, которые были недавно изменены, а также расширять свои возможности. Так, её последние версии могут также исполнять файлы с подключённых USB-носителей.

Таким образом, список собственных инструментов, используемых только Cycldek, достаточно широкий: в него, помимо USBCulprit, входят инструменты для кражи файлов cookie и паролей из баз данных веб-браузера.

«Мы видим, что эта группировка использует гораздо более сложные инструменты, а её присутствие в Юго-Восточной Азии гораздо шире, чем предполагалось раньше. Злоумышленники расширяют свой инструментарий и нацеливаются на новые страны. Мы продолжим наблюдение», — комментирует Юрий Наместников, руководитель российского исследовательского центра «Лаборатории Касперского». ***(Специальное ПО крадет данные с физически изолированных устройств // IKSMEDIA.RU (http://www.iksmedia.ru/news/5669979-Specialnoe-PO-kradet-dannye-s-fizic.html). 09.06.2020).***

***

«Хакери з угрупування DopplePaymer привітали SpaceX і NASA з першим запуском керованої людиною ракети, а потім відразу оголосили, що заразили пристрій одного з IT-підрядників NASA.

В опублікованому сьогодні повідомленні в блозі банда здирників DopplePaymer повідомила, що вона успішно проникла в мережу Digital Management Inc. (DMI), компанії з Меріленда, що надає керовані IT-послуги та послуги кібербезпеки за запитом.

Згідно з прес-релізом компанії, список клієнтів DMI включає кілька компаній зі списку Fortune 100 і багато урядові установи, у тому числі NASA.

Неясно, як глибоко проникли в мережі DMI хакери з DopplePaymer, час їх злому і скільки мереж клієнтів їм вдалося зламати. Три представника DMI не відповіли на телефонні дзвінки з ZDNet з проханням прокоментувати цю статтю.

Здається очевидним те, що вони взялися за файли, пов'язані з НАСА, що свідчить про те, що вони порушили інфраструктуру, пов'язану з НАСА, в DMI.

Для підтримки своїх тверджень оператори DeopplePaymer розмістили 20 архівних файлів у “темному інтернеті”.

Архіви включають в себе все, від кадрових документів до планів проектів, як видно з скріншоту, зробленого ZDNet для одного з файлів. Відомості про співробітників, включені в ці файли, що відповідають загальнодоступним записів LinkedIn.

Крім того, банда DopplePaymer також опублікувала список з 2583 серверів і робочих станцій, які, як стверджують хакери, є частиною внутрішньої мережі DMI і які вони зашифрували і тепер хочуть отримати за них викуп…» ***(Хакери зламали комп'ютер співробітника NASA, за секретні файли вимагають викуп // Знай.ua (https://techno.znaj.ua/315129-hakeri-zlamali-komp-yuter-spivrobitnika-nasa-za-sekretni-fayli-vimagayut-vikup). 03.06.2020).***

***

«Быть «крутым хакером», киберпреступником, взламывающим сети и компьютеры пользователей, на деле не так уж весело, считают эксперты Кембриджского университета. В своих выводах специалисты опираются на результаты исследования различных видов деятельности. Команда центра Кембриджского университета, изучающего киберпреступления, проанализировала работающий по модели «cybercrime-as-a-service» рынок. В частности, аналитики

уделили внимание ботнетам и организаторам DDoS-атак, размещающим свои предложения на чёрных онлайн-рынках. Исследователи пришли к выводу, что та романтика, которая приписывается деятельности «хакера», зачастую является просто вымыслом. Люди просто не учитывают, что чаще всего условный киберпреступник выполняет приблизительно то же самое, что и среднестатистический системный администратор в офисе. «Как правило, люди смотрят на киберпреступников как на рок-звёзд, а на их деятельность — как на что-то по-настоящему захватывающее», — заявил один из специалистов Ричард Клейтон в интервью Брайану Кребсу. «То есть основной посыл, который хотят навязать людям: быть хакером прибыльно и интересно. Однако в подавляющем большинстве случаев это вовсе не так». Также исследователи отметили, что современный киберпреступный мир тоже приспосабливается к реалиям. Теперь для «хакеров» больше важна не харизма, а чёткая и слаженная работа — как в офисе». ***(Екатерина Быстрова. Британские ученые опровергли романтизм жизни хакера // ООО «АМ-МЕДИА» (https://www.anti-malware.ru/news/2020-06-05-111332/32872). 05.06.2020).***

***

«…Фахівці міжнародного розробника антивірусного програмного забезпечення, експерта в галузі кіберзахисту – компанії ESET виявили нові атаки групи кіберзлочинців InvisiMole на військові і дипломатичні організації у Східній Європі, повідомляє прес-служба компанії ESET.

«У новій кампанії кіберзлочинці InvisiMole використовували оновлені інструменти, спрямовані на декілька організацій у військовому секторі та дипломатичні представництва в Східній Європі. Згідно з даними телеметрії ESET, спроби атак тривали з кінця 2019 і, щонайменше, до червня 2020 року», – йдеться в повідомленні.

За даними компанії ESET, група кіберзлочинців InvisiMole, яка активна щонайменше з 2013 року, була вперше виявлена в результаті цілеспрямованих операцій з використанням шпигунського програмного забезпечення в Україні та Росії. Зокрема, зловмисники використовували два багатофункціональних бекдори для шпигунства за жертвами. Однак, тоді фахівці з кібербезпеки не знали,як хакери доставляють, поширюють і встановлюють бекдори в систему. Тепер же, завдяки співпраці з постраждалими організаціями, дослідники отримали можливість дізнатися деталі подібних операцій.

У прес-службі повідомили, що одним з головних висновків, отриманих в ході дослідження стало співробітництво InvisiMole з іншою групою кіберзлочинців — Gamaredon. Дослідники виявили арсенал InvisiMole тільки після того, як Gamaredon вже проник в мережу, яка цікавила зловмисників і, можливо, отримав права адміністратора.

«Результати дослідження свідчать про те, що на цілях, які зловмисники вважають особливо важливими, спочатку використовують відносно просте шкідливе програмне забезпечення Gamaredon, а потім переходять до більш складної і сучасної загрози InvisiMole. Це дозволяє групі InvisiMole розробити нові

способи, щоб уникнути виявлення», — цитує прес-служба дослідницю ESET, яка аналізувала InvisiMole, Зузану Хромцову.

Дослідники ESET виявили, що аби уникнути виявлення група InvisiMole використовує чотири різні ланцюги виконання, створені шляхом об'єднання шкідливого shell-коду з легітимними інструментами і вразливими виконуваними файлами. Щоб приховати шкідливе програмне забезпечення від дослідників з безпеки, компоненти InvisiMole захищені шифруванням, яке є унікальним для кожної жертви і гарантує, що компонент можна розшифрувати і виконати тільки на інфікованому комп'ютері. Оновлений набір інструментів InvisiMole також містить новий компонент, який використовує тунелювання DNS для більш стійкою зв'язку з командним сервером (C&C).

Раніше фахівці ESET виявили нові цілеспрямовані атаки на користувачів соціальної мережі LinkedIn, для здійснення яких зловмисники використовували методи фішингу та видавали себе за інших людей.

За даними ESET, в Україні щодня фіксується близько 300 тис. нових кіберзагроз для інформаційної безпеки. При цьому, знайти хакерів-зловмисників вкрай складно, компаніям залишається лише проводити щохвилинні моніторинги на предмет виявлення кіберзагроз з метою їх подальшого блокування…» ***(IT-фахівці виявили нові кібератаки на військові і дипломатичні організації // UA.NEWS (https://ua.news/ua/it-spetsyalysty-obnaruzhyly-novye-kyberataky-na-voennye-y-dyplomatycheskye-organyzatsyy/). 18.06.2020).***

***

«Компания Eset обнаружила новую активность группы кибер-преступников Gamaredon, которая действует по меньшей мере с 2013 г. и отвечает за ряд атак, направленных в большинстве случаев на украинские учреждения.

Во время последней кампании злоумышленники воспользовались инновационными инструментами для распространения вредоносного ПО. Первый нацелен на Microsoft Outlook с использованием созданного Microsoft Outlook Visual Basic для приложений (VBA) проекта и позволяет злоумышленникам использовать учетную запись электронной почты жертвы для отправки фишинговых писем контактам из адресной книги. Использование макросов Outlook является достаточно нетипичным способом распространения вредоносов.

Второй инструмент используется указанной APT-группой для добавления макросов и ссылок на удаленные шаблоны в документах Office – Word и Excel. Оба инструмента предназначены для дальнейшего распространения вредоносного ПО Gamaredon в зараженных сетях.

«За последние несколько месяцев активность этой группы злоумышленников возросла, и киберпреступники целенаправленно отправляют вредоносные письма в почтовые ящики пользователей. К этим электронным письмам прикрепляют вложения – документы с вредоносными макросами, которые в случае запуска пытаются загрузить различные виды вредоносных программ», – комментирует Жан-Ян Боутин (Jean-Ian Boutin), руководитель исследовательской лаборатории Eset.

Новые инструменты используют вредоносные макросы или ссылки на удаленные шаблоны и добавляют их в существующие документы атакованной системы, что является очень эффективным способом распространения в корпоративной сети компании, поскольку документы, как правило, передаются коллегам. Кроме того, благодаря специальной функции, которая позволяет изменять настройки безопасности макросов Microsoft Office, зараженные пользователи не подозревают, что они подвергают риску свои рабочие станции каждый раз при открытии документов.

Группа киберпреступников использует бэкдоры и программы для похищения файлов с целью идентификации и сбора конфиденциальных документов в зараженной системе и загрузки их на командный сервер (C&C). Кроме того, эти вредоносные программы для похищения файлов имеют возможность выполнять команды с удаленного сервера.

Между Gamaredon и другими APT-группами есть одно существенное отличие – киберпреступники прилагают минимальные усилия, чтобы оставаться незамеченными в сети. Даже несмотря на то, что их инструменты способны использовать методы для маскировки, основная задача этой группы злоумышленников – как можно быстрее распространиться в сети своей жертвы, пытаясь похитить данные.

«Хотя использование скомпрометированного почтового ящика для отправки вредоносных писем без согласия пользователя не является новой техникой, мы считаем, что это первый зафиксированный случай атаки киберпреступников с использованием файла OTM и макроса Outlook, – объясняет Жан-Ян Боутин. – Мы смогли собрать множество различных образцов вредоносных скриптов, исполняемых файлов и документов, используемых группой Gamaredon во время всех вредоносных кампаний». ***(АТР-группа Gamaredon атакует пользователей Microsoft Outlook и Office // Компьютерное Обозрение (https://ko.com.ua/atp-gruppa_gamaredon_atakuet_polzovatelej_microsoft_outlook_i_office_133371). 12.06.2020).***

***

«Специалисты из компании Binary Defense исследовали ряд известных подпольных площадок в даркнете и сообщили, что услуга «хакеры по найму» (Hackers for Hire, HfH) вновь начинает набирать популярность

Наиболее известными HfH-группировками в настоящее время являются:

Hack Group;

Rent-A-Hacker;

Hacker Group;

Black Hat Journal;

Hacker for Hire;

Stroller;

Hackse;

Xhacker;

Digital Hackers.

Одной из самых популярных услуг, предлагаемых подобными сайтами, является взлом учетных записей в социальных сетях, таких как Facebook и Twitter. Когда злоумышленник перехватывает контроль над целевым аккаунтом, он публикует указанный покупателем контент от имени жертвы.

Также хакеры по найму предлагают изменить оценки в школах и университетах, похитить пароль электронной почты учителя и изменить определенные данные, например, количество пропущенных уроков. Многие группировки предлагают курсы по обучению хакерству.

Страницы злоумышленников не содержат сведений о том, как они взламывают учетные записи или как они получают пароли. Скорее всего, они делают это с помощью инфостиллеров, фишинга или узнают пароли из баз данных утекших ранее паролей.

Цены за подобные услуги варьируются. Например, осуществление DDoS-атак обойдется от $99, разрушительное вмешательство в чью-либо жизнь — от $699, а подрыв репутации компании — от $899. Последнее включает в себя плохие отзывы, негативные рекламные кампании, дефейс сайта или его удаление и пр». ***(Услуги хакеров по найму набирают популярность в даркнете // SecurityLab.ru (https://www.securitylab.ru/news/509312.php). 18.06.2020).***

***

«Специализирующаяся на вопросах кибербезопасности фирма ClearSky оценила в $200 млн ущерб, нанесенный хакерской группой CryptoCore, криптовалютным биржам США и Японии. Об этом говорится в блоге компании.

CryptoCore также известна под именами Crypto-gang, Dangerous Password и Leery Turtle.

Специалисты ClearSky нашли единый почерк в организации работы, используемой цифровой инфраструктуре и направлений атак, сделав вывод, что в ряде эпизодов стояла одна и та же группа хакеров.

«CryptoCore — группа, нацеленная почти исключительно на криптовалютные биржи и их партнеров посредством атак на цепочки поставок. На сегодняшний день известно, что этот альянс хакеров аккумулировал порядка $70 в результате успешных действий. По нашим расчетам, за два года группе удалось собрать более $200 млн», — говорится в отчете ClearSky.

Взяв за основу временную метку первого известного случая похожих атак, в компании установили, что хакеры начали свою деятельность в середине 2018 года и с тех пор «поддерживали устойчивую активность».

ClearSky не удалось обнаружить местонахождение команды, однако в компании считают, что она базируется в Украине, России или Румынии. В группу входит от трех до четырех человек, которые не обладают чрезвычайно высоким уровнем технической подготовки, что не мешает ей быть очень эффективной за счет настойчивости и быстроты.

«Ключевая цель CryptoCore — получить доступ к кошелькам криптовалютных бирж. Для такого рода операций группа начинает с обширной фазы разведки против компании, ее руководителей, специалистов высокого звена и

IT-персонала. Основной вектор проникновения группы на биржу обычно осуществляется через фишинг корпоративной сети и электронную почту руководителей», — отметили специалисты.

После получения доступа к электронной почте злоумышленники получают контроль над ключами от криптокошельков. Группа действует незаметно до тех пор пока ей не удается обойти всю защиту многофакторной аутентификации». ***(Хакерская группа CryptoCore украла у криптобирж $200 млн // LetKnow News (https://letknow.news/news/hakerskaya-gruppa-cryptocore-ukrala-u-kriptobirzh-200-mln-37869.html). 26.06.20200.***

***

«Специалисты Malwarebytes обнаружили, что MageCart-хакеры используют своеобразную стеганографию, прячут веб-скиммеры в метаданных изображений EXIF, а также используют картинки для извлечения украденных данных.

Напомню, что изначально название MageCart было присвоено одной хак-группе, которая первой начала использовать так называемые веб-скиммеры на сайтах для хищения данных банковских карт. Хакеры взламывают сайты, а затем внедряют на их страницы вредоносный код, который записывает и похищает данные платежных карт, когда пользователи вводят их во время оформления заказа.

Этот подход оказался настолько успешным, что у группировки вскоре появились многочисленные подражатели, а название MageCart стало нарицательным, и теперь им обозначают целый класс подобных атак. И если в 2018 году исследователи RiskIQ идентифицировали 12 таких группировок, то в конце 2019 года, по данным IBM, их насчитывалось уже около 40…

В открытом каталоге неназванного скомпрометированного сайта исследователям удалось обнаружить копию исходных кодов набора для скимминга, что позволило почерпнуть много новой информации и заметить, что обычный файл favicon.ico содержит внедренный скрипт внутри поля Copyright.

По словам экспертов, атака злоумышленников строится следующим образом: веб-скиммер был найден в метаданных EXIF-файла, который загружался взломанными интернет-магазинами с плагином WooCommerce для WordPress на борту. Посторонний код для загрузки опасного изображения добавлялся к легитимному скрипту, размещенному на сайтах самими владельцами магазинов.

Вредоносную активность удалось проследить до сайта cddn[.]site, с которого загружался вредоносный файл favicon. Как оказалось, злоумышленники использовали favicon, идентичные настоящим в скомпрометированных магазинах, а веб-скиммер подгружался из поля Copyright в метаданных изображения при помощи тега <img>.

Как не трудно догадаться, этот веб-скиммер, как и другая подобная малварь, похищал содержимое полей ввода, куда покупатели вписывали свое имя, биллинг-адрес, данные кредитной карты и так далее. Когда информация собрана, скиммер шифровал собранные данные, переворачивал строку и через POST-запрос передавал похищенную информацию на удаленный сервер своим операторам тоже

в виде файла изображения. Очевидно, злоумышленники решили быть последовательными и использовали картинки для сокрытия данных на всех этапах атаки.

Эксперты Malwarebytes также смогли обнаружить раннюю версию этого скиммера, в которой не было обфускации, присущей новейшей итерации. В целом эта версия имела те же функции, но изучение поведения обеих вариаций малвари позволило сделать вывод, что данная разработка может принадлежать MageCart-группировке номер 9». ***(Мария Нефёдова. Веб-скиммеры прячутся в метаданных изображений // Xakep (https://xakep.ru/2020/06/29/magecart9-technique/). 29.06.2020).***

***

«Киберпреступная группировка Cl0ud SecuritY взламывает устаревшие сетевые хранилища (NAS) LenovoEMC (в прошлом Iomega), стирает все файлы и требует $200-275 за их возвращение. После удаления данных злоумышленники оставляют текстовый файл RECOVER YOUR FILES !!!!.txt с указанием контактного электронного адреса (cloud@mail2pay.com).

По данным портала BitcoinAbuse, где пользователи могут сообщать о биткойн-кошельках, использующихся в вымогательских и других киберпреступных операциях, атаки продолжаются по крайней мере уже месяц. Атаки нацелены исключительно на сетевые хранилища LenovoEMC/Iomega с подключенным к интернету интерфейсом без парольной защиты.

Похоже, данная кампания является продолжением прошлогодней операции, в ходе которой злоумышленники также атаковали устаревшие сетевые хранилища LenovoEMC/Iomega, чья поддержка прекратилась в 2018 году. Хотя в первой кампании злоумышленники не называли себя и использовали другой контактный электронный адрес, записки с требованием выкупа в обоих случаях очень похожи, что может указывать на одну и ту же группировку.

Как сообщил изданию ZDNet исследователь безопасности из GDI Foundation Виктор Геверс (Victor Gevers), атаки являются делом рук малоопытных хакеров. Злоумышленники используют простой эксплоит, атакуют устройства, уже и так доступные через интернет, и не утруждают себя шифрованием файлов.

По словам киберпреступников, они копируют хранящие в сетевых хранилищах данные перед их удалением и намерены опубликовать их в открытом доступе, если выкуп не будет уплачен в течение пяти дней. Тем не менее, нет никаких доказательств того, что вымогатели действительно делают резервные копии удаляемых файлов, равно как и того, что данные публикуются в случае неуплаты». ***(Хакеры взламывают NAS LenovoEMC и стирают файлы // SecurityLab.ru (https://www.securitylab.ru/news/509571.php). 30.06.2020).***

***

«Эксперты Fox-IT рассказали о последней активности известной хакерской группы Evil Corp. По данным аналитиков, группа вернулась к жизни в январе текущего года и провела несколько вредоносных кампаний, а затем и вовсе возобновила активность с новыми инструментами.

Напомню, что группировку Evil Corp называют одной из наиболее активных и наглых среди киберпреступников. За сведения о ее членах американское правительство назначило награду в 5 миллионов долларов, а СМИ часто обсуждают слухи об их роскошном образе жизни и возможных связях с российскими спецслужбами. В начале текущего года мы постарались поподробнее разобраться в истории этой хакерской группы, образе действий и инструментах, с помощью которых она достигла своих сомнительных успехов и признания.

Ретроспектива

Evil Corp, также известная Dridex, активна примерно с 2007 года, когда несколько хакеров, ранее связанных с банковским трояном ZeuS, решили попытать счастья в распространении вредоносных программ. Сначала группа сосредоточила усилия на распространении банковского трояна Cridex, который впоследствии превратился в банкер Dridex, а еще позже в многоцелевой вредоносный набор инструментов Dridex.

Благодаря Dridex в распоряжении группировки оказался один из крупнейших ботнетов для распространения малвари и спама. Таким способом Evil Corp распространяла как собственную малварь, так и вредоносное ПО для других преступных групп, а также кастомные спамерские сообщения.

В 2016 году группирвока также начала заниматься распространением вымогателей, начиная с шифровальщика Locky. Но по мере того как фокус вымогателей начал смещаться с домашних потребителей на корпоративные цели, Evil Corp тоже адаптировалась к ситуации и создала новую вымогательскую малварь BitPaymer.

Evil Corp использовала свой гигантский ботнет из устройств, зараженных Dridex, для поиска корпоративных сетей, а затем разворачивала BitPaymer в сетях наиболее крупных предприятий, которые только удалось найти.

BitPaymer активно использовался в период между 2017 и 2019 годами, но потом атаки постепенно стали прекращаться. Причины этого спада до сих пор неясны, но он мог быть связан с тем фактом, что ботнет Dridex тоже «замедлился» в период между 2017 и 2019 годами.

Наши дни

Fox-IT пишет, что это спад активности группы завершился после обвинений Министерства юстиции США, заочно предъявленных членам Evil Corp в декабре 2019 года. После этого хакеры замолчали почти на целый месяц, вплоть до января 2020 года, но затем возобновили активность и провели несколько вредоносных кампаний, в основном для других мошенников.

Весной 2020 года Evil Corp вновь «вернулась к жизни» и на этот раз с новыми инструментами. По данным исследователей, группировка разработала новый вымогатель WastedLocker, чтобы заменить им устаревший BitPaymer, использовавшийся с начала 2017 года.

По мнению исследователей, эта малварь была написана с нуля, и анализ нового вымогателя не выявил практически никаких признаков повторного использования кода и других сходств между BitPaymer и WastedLocker. Некоторые параллели можно заметить лишь в тексте записки с требованием выкупа.

Эксперты Fox-IT отслеживают использование WastedLocker с мая 2020 года. По их данным, пока вымогатель использовался исключительно против американских компаний, а суммы выкупов, которые требует у пострадавших Evil Corp, теперь исчисляются миллионами долларов. К примеру, исследователям известен случай, когда хакеры запросили у компании 10 000 000 долларов США. Опираясь на данные с VirusTotal, аналитики говорят, что WastedLocker применялся по назначению уже как минимум пять раз.

Операторы Evil Corp очень агрессивны при развертывании нового вымогателя WastedLocker: как правило, они атакуют файловые серверы, БД-сервисы, виртуальные машины и облачные среды. Также группировка стремится нарушить работу приложений для резервного копирования и связанной с ними инфраструктуры, то есть всячески затрудняет восстановление информации для пострадавших компаний. Ведь если у компаний нет оффлайновых резервных копий, удаление бэкапов почти наверняка подтолкнет ее к выплате выкупа (если они, конечно, компании по карману новые многомиллионные «тарифы» Evil Corp).

При этом Evil Corp пока не делает того, что сейчас в тренде среди других вымогательских группировок: WastedLocker не умеет похищать данные перед их шифрованием. Напомню, что в настоящее от 10 до 15 хакерских групп заражают сети компаний, крадут конфиденциальные данные, и лишь после этого шифруют файлы, а также угрожают опубликовать похищенные данные в открытом доступе (на своих собственных сайтах или файлообменниках). Подобную тактику используют группировки Maze, Sodinokibi, DopplePaymer, Clop, Sekhmet, Nephilim, Mespinoza, Ako, Netwalker и так далее.

Пока Evil Corp не делает ничего подобного, и специалисты Fox-IT полагают, что это вполне осознанное решение. Дело в том, что «слив» украденных данных обычно привлекает большое внимание СМИ, чего участники Evil Corp, скорее всего, хотели бы избежать, ведь некоторые члены группы и так входят в список самых разыскиваемых ФБР преступников». ***(Мария Нефёдова. Вымогатель WastedLocker, принадлежащий Evil Corp, требует миллионы долларов выкупа // Xakep (https://xakep.ru/2020/06/24/wastedlocker/). 24.06.2020).***

***

Вірусне та інше шкідливе програмне забезпечення

«Аналитики компании White Ops обнаружили в Google Play Store 38 вредоносных приложений (список можно увидеть здесь), которые показывали пользователям навязчивую рекламу и осуществляли нежелательные перенаправления в браузерах. Все эти приложения были созданы одной преступной группой.

Вредоносная функциональность в коде приложений была отключена: таким образом операторы малвари пытались обмануть защитные механизмы Google Play Store и проникнуть в каталог.

По данным специалистов, эта хак-группа активна с января 2019 года, именно тогда хакеры начали загружать приложения в официальный каталог Google.

Причем 21 из 38 вредоносных приложений группировки появились в Google Play Store именно на начальном этапе активности группировки.

Все приложения хакеров были так или иначе связаны с бьюти-фотографией (среди них были приложения для селфи или приложения, добавляющие различные фильтры к фотографиям). Но после установки они начинали бомбардировать пользователей рекламой, открывали рекламу в браузерах жертв, а также пытались максимально усложнить пострадавшим удаление, скрывая свои иконки.

При этом исследователи отмечают, что приложения и эту кампанию нельзя назвать сложными или успешными. Хотя adware проходила изначальные проверки Google, в конечном итоге приложения идентифицировались как вредоносные и удалялись. Так, большинство приложений группировки проработали перед удалением лишь 17 дней. Впрочем, даже за столь короткий срок большинство успевало в среднем набрать 565 833 установки, а в общей сложности рекламную малварь группы загрузили более 20 000 000 раз.

Так как приложения продолжали удалять, в сентябре 2019 года группировка изменила тактику и стала прилагать больше усилий для сокрытия вредоносной составляющей своих «продуктов».

Во-первых, хакеры начали использовать арабские символы, вставляя их в исходный код приложений. Идея заключалась в том, чтобы не дать инженерам Google заметить явно вредоносную функциональность приложений, используя для этого арабский текст вместо английского (в некоторых местах попадались даже цитаты из Корана).

Во-вторых, злоумышленники стали полностью удалять вредоносный код своих из приложений. Так, с сентября 2019 года хак-группа загрузила в Google Play 15 приложений, и во всех была отключена вредоносная функциональность. Технически эти продукты были «чистыми», однако через некоторое время они могли обновиться, и вредоносный код мог вернуться на место.

Нужно сказать, что в конечном итоге эти уловки не сработали. Дело в том, что приложения были загружены в официальный каталог уже известными Google мошенниками, почему компания все равно удалила их, не желая рисковать». ***(Мария Нефёдова. Из Google Play Store удалили 38 вредоносных приложений, загруженных более 20 млн раз // Xakep (https://xakep.ru/2020/06/10/38-adware-apps/). 10.06.2020).***

***

«Осенью прошлого года ИБ-специалисты обратили внимание на вымогателя STOP (Djvu), который по данным сервиса ID Ransomware, созданного известным ИБ-экспертом Майклом Гиллеспи, оказался одной из наиболее активных угроз года, наряду с Ryuk, GandCrab и Sodinkibi.

Тогда сообщалось, что ID Ransomware получает примерно 2500 сообщений об атаках вымогателей в день, но примерно 60-70% из них — это сообщения об атаках шифровальщика STOP, что оставляет другие вымогатели далеко позади. В настоящее время ID Ransomware по-прежнему получает порядка 600 сообщений о заражениях STOP в день.

В прошлом году специалисты компании Emsisoft и Майкл Гиллеспи выпустили бесплатную утилиту для дешифровки данных, пострадавших от атак шифровальщика STOP. Разработанный Emsisoft инструмент работал против 148 из 160 вариаций шифровальщика, то есть должен помочь примерно 70% жертв.

Теперь издание Bleeping Computer и MalwareHunterTeam предупреждают, что неизвестные злоумышленники создали вымогатель, который маскируется под ту самую бесплатную утилиту от Emsisoft. Малварь получила название Zorab: фальшивая утилита повторно шифрует все данные жертвы, уже пострадавшей от атаки STOP.

Когда пользователь вводит свои данные в фальшивый расшифровщик и нажимает «Начать сканирование», программа извлекает другой исполняемый файл crab.exe и сохраняет его в папке %Temp%. Этот файл и представляет собой основу Zorab, который тут же начинает снова шифровать данные на компьютере, добавляя к ним расширение .ZRB.

В итоге незашифрованной на пострадавшей машине остается лишь записка с требованием выкупа, содержащая инструкции о том, как связаться с операторами малвари для получения инструкций для оплаты.

Исследователи крайне не рекомендуют жертвам Zorab платить злоумышленникам и пишут, что уже занимаются анализом новой малвари». ***(Мария Нефёдова. Вредоносный дешифровщик Zorab не помогает жертвам вымогателя, а повторно шифрует файлы // Xakep (https://xakep.ru/2020/06/08/zorab/). 08.06.2020).***

***

«Операторы вымогательского ПО eCh0raix организовали вредоносную кампанию, нацеленную на сетевые хранилища (NAS) QNAP. Вредонос компрометирует устройства путем брутфорса и эксплуатации известных уязвимостей в сетевых хранилищах (CVE-2018-19943, CVE-2018-19949 и CVE-2018-19953), которые позволяют внедрить или удаленно выполнить код.

Как только злоумышленники получают доступ к устройству, они устанавливают вымогательское ПО, шифрующее файлы на системе жертвы и добавляющее расширение .encrypt к имени файлов. Затем жертва получает сообщение с требованием выкупа README_FOR_DECRYPT.txt, содержащее ссылку на сайт оплаты. За расшифровку данных злоумышленники требуют заплатить выкуп в размере 0,0547 BTC (примерно $500).

По словам пострадавших, после шифрования в AppCenter устройства появляются приложения QNAP со странными названиями. Неизвестно, являются ли они вредоносными пакетами, установленными преступниками, или загруженными пользователем пакетами, которые были зашифрованы.

В настоящее время нет способа восстановить файлы самостоятельно, если сервис моментальных снимков системы (Snapshot) на сетевых хранилищах QNAP был отключен. Данная функция позволяет использовать снимки для восстановления данных.

QNAP исправила уязвимости в версиях операционной системы QTS 4.4.1 (сборка 20190918 и младше) и QTS 4.3.6 (сборка 20190919 и младше).

Напомним, атаки с использованием вредоносного ПО eCh0raix были впервые обнаружены в июле прошлого года. Тогда компании QNAP и Synology предупредили пользователей об атаках с использованием вымогателя eCh0raix на сетевые накопители. В рамках атак злоумышленники похитили учетные данные администратора, с их помощью получили доступ к устройствам и зашифровали хранившуюся на них информацию». ***(Операторы вымогателя eCh0raix атаковали сетевые хранилища QNAP // SecurityLab.ru (https://www.securitylab.ru/news/508962.php). 08.06.2020).***

***

«Компанія Blackberry заявляє про новий вірус-шифрувальник Tycoon, якому вдається оминати антивіруси та тривалий час залишатися у мережі непомітним…

Для шифрування вірус використовує маловідомий формат файлів Java задля непомітного проникнення. Фахівці виявили Tycoon, коли працювали над відновленням інформації в одному з навчальних закладів Європи, постраждалому від кібератаки. У компанії зауважують, що атака вірусу починається стандартно: компрометація здійснюється через небезпечні RDP-сервери, "видимі" з інтернету.

Потім процес змінюється, зловмисники використовують ін'єкцію IFEO для забезпечення стійкої присутності в системі, запускають бекдор разом з OSK, а також відключають антивірусні програми, використовуючи ProcessHacker». ***(Фахівці знайшли новий небезпечний вірус-шифрувальник // Молодий буковинець (https://molbuk.ua/news/201684-fakhivci-znayshly-novyy-nebezpechnyy-virus-shyfruvalnyk.html). 06.06.2020).***

***

«Недавно специалисты по кибербезопасности выявили новый, опасный для операционных систем Windows и Linux, вирус-шифровальщик, который способен долго оставаться незамеченным на компьютере…

Неделю назад мир всколыхнула опасная хакерская атака – специалисты компании Blackberry обнаружили новый вирус-шифровальщик Tycoon, который может долго оставаться незаметным для антивирусов, и несет угрозу для операционных систем Windows и Linux, при том, что последняя – длительное время считалась одной из самых защищенных платформ. Основными жертвами вируса стали организации в сфере образования, разработчики программного обеспечения и компании среднего и малого бизнеса. И хотя вредоносная программа еще не добралась до Украины, ее обнаружение свидетельствует о том, что действия хакеров с каждым разом становятся более изощренными, и опасным угрозам могут быть подвержены любые операционные системы в любой точке мира…». ***(Надежда Бурбела. Эксперт по кибербезопасности ESET Ондрей Кубович: Мы советуем людям, пострадавшим от нового вируса-шифровальщика Tycoon, не платить выкуп хакерам - нет никаких гарантий того, что они будут расшифровывать файлы // УНИАН (https://www.unian.net/science/ekspert-po-kiberbezopasnosti-eset-ondrey-kubovich-my-sovetuem-lyudyam-postradavshim-ot-***

novogo-virusa-shifrovalshchika-tycoon-ne-platit-vykup-hakeram-net-nikakih-garantiy-togo-chto-oni-budut-rasshifrovyvat-fayly-novosti-11032400.html). 11.06.2020).

***

«Недавно пользователи сделали 32 млн загрузок мошеннических расширений для браузера Google Chrome, который является лидером рынка, пишет Reuters со ссылкой на исследование платформы по обнаружению кибератак на организации Awake Security. Исследователи подчеркнули неспособность технологической индустрии защитить браузеры, всё больше используемые для электронной почты, платежей и других чувствительных вещей.

В Alphabet Inc (GOOGL.O) Google заявили, что удалили более 70 вредоносных дополнений из официального интернет-магазина Chrome, после того как в прошлом месяце исследователи предупредили корпорацию. «Когда нас предупреждают о расширениях в веб-магазине, которые нарушают нашу политику, мы принимаем меры и тренируемся на этих инцидентах в целях улучшения нашего автоматизированного и ручного анализа», — сказал представитель Google Скотт Вестовер.

Большинство бесплатных расширений предупреждают пользователей о сомнительных веб-сайтах или преобразовывают файлы из одного формата в другой. Новые мошеннические расширения выкачивали историю браузера и данные, которые сливали учётные записи для доступа к внутренним бизнес-инструментам.

По словам соучредителя и главного научного сотрудника Awake Security Гэри Голомба, это была самая масштабная вредоносная кампания в Chrome store на сегодняшний день, судя по количеству загрузок.

Google отказался сравнивать последние шпионские программы с предыдущими кампаниями и обсуждать масштаб ущерба или причину, по которой он не обнаружил и не удалил плохие расширения самостоятельно, несмотря на прошлые обещания контролировать предложения в магазине более пристально.

Неясно, кто стоял за попыткой распространить вредоносное ПО. В Awake Security полагают, что разработчики дали поддельную контактную информацию, когда представляли расширения Google. «Все, что попадёт в чей-то браузер, электронную почту или другие чувствительные области, станет мишенью для национального шпионажа или организованной преступности», — прокомментировал ситуацию бывший инженер Агентства национальной безопасности Бен Джонсон, основавший компании по безопасности Carbon Black и Obsidian Security.

Эти расширения были разработаны таким образом, чтобы не быть обнаруженными антивирусами или ПО по безопасности, которое оценивает репутацию доменов, сказал Голомб. Если кто-то использовал браузер для интернет-серфинга на домашнем компьютере, он подключался к ряду веб-сайтов и передавал информацию, обнаружили исследователи. Любой человек, использующий корпоративную сеть, которая содержит службы безопасности, не будет передавать конфиденциальную информацию или даже заходить на вредоносные версии сайтов.

«Это показывает, как злоумышленники могут использовать чрезвычайно простые методы, чтобы скрыть, в данном случае, тысячи вредоносных доменов», — сделал вывод Голомб.

После публикации этой истории Awake Security обнародовала своё исследование, включающее список доменов и расширений. Все рассматриваемые и связанные между собой домены (в общей сложности более 15 тыс.) были приобретены у небольшого израильского регистратора Galcomm, официально известного как CommuniGal Communication Ltd.

В Awake Security считают, что в Galcomm должны были знать о происходящем. Владелец Galcomm Моше Фогель заявил Reuters, что его компания не сделала ничего плохого. «Galcomm не вовлечена и не участвует в какой-либо вредоносной деятельности. Можно сказать прямо противоположное: мы сотрудничаем с правоохранительными органами и органами безопасности, чтобы предотвратить подобное настолько, насколько мы можем», — написал Фогель.

Фогель также попросил список подозрительных доменов и сказал, что на электронной почте компании нет никаких сообщений о запросах Голомба насчёт злоупотреблений, которые тот отправил в апреле и продублировал в мае. После публикации Фогель заявил, что большинство этих доменных имен были неактивны и он продолжит изучение остальных.

Курирующая регистраторов компания Internet Corp for Assigned Names and Numbers заявила, что в течение нескольких лет получила некоторое количество жалоб на Galcomm, но ни одна из них не была о вредоносных программах.

В течение многих лет мошеннические расширения являются проблемой и становятся всё хуже. Поначалу они «выплёвывали» нежелательную рекламу, а теперь, более вероятно, устанавливают дополнительные вредоносные программы или отслеживают, где находятся пользователи и что они делают для правительственных или коммерческих шпионов…». ***(Joseph Menn. Exclusive: Massive spying on users of Google's Chrome shows new security weakness // Reuters (https://www.reuters.com/article/us-alphabet-google-chrome-exclusive/exclusive-massive-spying-on-users-of-googles-chrome-shows-new-security-weakness-idUSKBN23P0JO).18.06.2020).***

****

«Аналитики Microsoft обнаружили хакерскую кампанию, в ходе которой пользователей просят решить CAPTCHA перед тем, как они получат доступ к вредоносному контенту — документу Excel. Данный файл содержит макросы, которые устанавливают на машину жертвы троян GraceWire, ворующий конфиденциальную информацию (например, пароли).

Ответственность за эту кампанию исследователи возлагают на хак-группу Chimborazo, за которой специалисты наблюдают с января текущего года.

Данная кампания получила имя Chimborazo Dudear. Изначально хакеры действовали по классической схеме и прикладывали вредоносные документы Excel к фишинговым письмам. Затем перешли на встроенные в сообщения ссылки. А в последние недели группа начала рассылать фишинговые письма, содержащие ссылки на сайты-перенаправители (обычно это легитимные ресурсы, которые были

взломаны), а порой к письмам прикрепляется HTML-вложение, содержащее вредоносный iframe.

Кликнув по такой ссылке или открыв вложение, жертва в любом случае попадет на сайт с загрузкой вредоносного файла. Однако прежде чем получить доступ к самому файлу, пользователь будет вынужден решить CAPTCHA. Таким образом злоумышленники постарались затруднить работу автоматических защитных механизмов, которые должны обнаруживать и блокировать подобные атаки. Обычно такой анализ выполняется с помощью ботов, которые загружают образцы малвари, запускают их и анализируют на виртуальных машинах. CAPTCHA же гарантирует, что образчик малвари загрузит живой человек.

В январе текущего года специалисты Security Intelligence уже писали об атаках группировки Chimborazo. Тогда исследователи рассказывали, что хак-группа использует отслеживание IP-адресов для идентификации компьютеров, с которых загрузили вредоносный файл Excel. Предположительно, это тоже делалось для того, чтобы избежать автоматического обнаружения.

Эксперт Malwarebytes Жером Сегура (Jérôme Segura) пишет, что использование CAPTCHA хакерами – это редкий, но не беспрецедентный случай. К примеру, он ссылается на твит другого ИБ-специалиста, датированный концом декабря 2019 года. Тогда тоже была обнаружена фальшивая CAPTCHA, которую злоумышленники успешно использовали для усложнения работы автоматического анализа.

CAPTCHA, обнаруженная Microsoft, тоже может быть поддельной. Как видно на картинке выше, сайт злоумышленников утверждает, что использует reCAPTCHA, но ниже заявлено, что защиту от DDoS-атак обеспечивает Cloudflare. Это два отдельных сервиса, хотя вполне возможно, что хакеры использовали оба по отдельности». ***(Мария Нефёдова. Хакеры вынуждают пользователей решать CAPTCHA // Xakep (https://xakep.ru/2020/06/23/phishing-captcha/). 23.06.2020).***

****

«Специалисты Palo Alto Networks выявили таргетированные атаки на российские организации. Для этого вредонос AcidBox использовал эксплоит, который ранее связывали с русскоязычной хакерской группой Turla (она же Waterbug, Venomous Bear и KRYPTON).

В частности Turla известна тем, что была первой хак-группой, которая злоупотребляла драйвером стороннего устройства для отключения Driver Signature Enforcement (DSE) — защитной функции, появившейся в Windows Vista для предотвращения загрузки неподписанных драйверов.

Проблема CVE-2008-3431, которую эксплуатировала Turla, использовала подписанный драйвер VirtualBox (VBoxDrv.sys v1.6.2) для деактивации DSE и загрузки неподписанных драйверов-пейлоадов. Но эксплоит группировки, по сути, использовал две уязвимости, тогда как лишь одна из них была устранена. Существовала и вторая версия эксплоита, ориентированная на использование только этой неизвестной уязвимости.

Теперь аналитики Palo Alto Networks пишут, что с 2017 года неизвестные хакеры, явно несвязанные с Turla, используют ту же исправленную проблему, для эксплуатации новых версий драйвера VBoxDrv.sys.

Так, в 2017 году злоумышленники атаковали как минимум две российские организации, используя драйвер версии 2.2.0 (вероятно потому, что ранее эта версия не считалась уязвимой). Таким образом атакующие разворачивали ранее неизвестное экспертам семейство малвари, которое получило название AcidBox.

AcidBox использует некую форму стеганографии и прячет конфиденциальные данные в иконках, злоупотребляет интерфейсом SSP, чтобы надежно закрепиться в системе, хранит свою полезную нагрузку в реестре Windows и не демонстрирует каких-то явных параллелей с другой известной малварью (хоть и имеет небольшое сходство с Remsec).

«Поскольку других жертв обнаружено не было, мы полагаем, что это очень редкое вредоносное ПО, используемое только в целевых атаках», — пишут эксперты.

Аналитики подчеркивают, что AcidBox определенно входит в состав большого набора инструментов, вероятно, принадлежащих некой APT, и может использоваться до сих пор, при условии, что сама хак-группа по-прежнему активна. Вместе с другими ИБ-специалистами исследователи Palo Alto Networks смогли выявить три usermode-образца малвари (64-разрядные DLL, которые загружают main worker'a из реестра Windows) и kernelmode пейлоад-драйвер (который встроен в main worker'a).

Все образчики были скомпилированы 9 мая 2017 года и, скорее всего, использовались в рамках вредоносной кампании в том же году. Более новые образцы обнаружить не удалось, и пока неясно, активна ли эта хак-группа в настоящее время.

К сожалению, эксперты Palo Alto Networks не смогли идентифицировать инструментарий, частью которого является AcidBox, но все же поделились двумя правилами YARA для обнаружения данной угрозы, а также Python-скриптом, который поможет извлечь конфиденциальные данные из иконок». ***(Мария Нефёдова. Малварь AcidBox используется для атак на российские компании // Xakep (https://xakep.ru/2020/06/22/acidbox/). 22.06.2020).***

***

«Аналитики независимой лаборатории AV-Comparatives и Electronic Frontier Foundation (EFF) выяснили, что ситуация с обнаружением stalkerware-приложений на Android и Windows постепенно улучшается.

Напомню, что термином stalkerware обычно обозначают коммерческое шпионское ПО, которое позиционируется как легальное. С его помощью можно получить доступ к личным данным, хранящимся на смартфонах и планшетах других пользователей.

Stalkerware часто маскируется под приложения для родительского контроля, ПО для наблюдения за сотрудниками и даже под инструменты для организации удаленного доступа, предназначенные для корпоративного сектора. Такой софт, как правило, используется для тайного наблюдения за людьми, в том числе

инициаторами домашнего насилия, и поэтому нередко несет серьезные риски для тех, на чьих устройствах установлен.

Эксперты опубликовали доклад, согласно которому изучение данного вопроса было разделено на два этапа: первый прошел в ноябре 2019 года и второй в мае 2020 года. Для проведения тестов исследователи отобрали 20 образцов stalkerware для Android и 10 для Windows, исходя из популярности данных продуктов в США.

Как оказалось, 10 мобильных антивирусных приложений для Android и 10 антивирусных продуктов для Windows «научились» неплохо обнаруживать некоторые из наиболее распространенных на сегодня видов сталкерского ПО. Таким образом, многие антивирусные компании существенно улучшили свои показатели в период с ноября 2019 года до мая 2020 года.

Аналитики AV-Comparatives рассказывают, что в ноябре прошлого года уровень обнаружения шпионских приложений для Android варьировался от 30% до 95%, но при этом два продукта обнаруживали менее 50% тестовых случаев. В этот же период в Windows общий уровень обнаружения сталкерских приложений был низким даже по сравнению с Android: самый лучший результат составил всего 70%, и лишь два защитных продукта достигли такого уровня.

Шесть месяцев спустя, в мае текущего года, большинство продуктов (как для Android, так и для Windows) значительно повысили свои уровни обнаружения stalkerware. Так, 9 из 10 продуктов для Android теперь обнаружили от 75% до 95% вредоносных образчиков. Все продукты для Windows улучшили свои показатели как минимум до 70%, а четыре программы и вовсе достигли стопроцентного результата.

Эксперты говорят, что в целом результаты этого исследования обнадеживают, так как они показывают, что индустрия кибербезопасности наконец перестает игнорировать stalkerware. Напомню, что Electronic Frontier Foundation с 2018 года подталкивает индустрию к классифицированию подобных продуктов как вредоносных и старается информировать о данной угрозе пользователей…». ***(Мария Нефёдова. Антивирусы стали лучше обнаруживать сталкерское ПО // Xakep (https://xakep.ru/2020/06/15/stalkerware-detection/). 15.06.2020).***

***

«Лаборатория Касперского» обнаружила новые атаки с использованием буткита Rovnix, позволяющего загружать на устройство вредоносное ПО и скрывать его от защитных программ. В найденной экспертами кампании зловред распространялся через самораспаковывающийся архив на русском языке, в котором якобы содержится информация о новой инициативе «Всемирного банка» в связи с пандемией. Такие атаки были зафиксированы весной.

Буткит серьезно усовершенствован: в его составе появились средства обхода контроля учетных записей пользователя и необычный для него загрузчик. В результате работы Rovnix в систему закрепляется бэкдор с элементами Trojan-Spy, который может записать звук с микрофона, сделать скриншот экрана, а также в некоторых версиях украсть логин и пароль учетной записи пользователя системы.

Этот буткит был очень популярен у злоумышленников до того, как его исходный код попал в публичное пространство в 2013 г., и его начали анализировать эксперты по кибербезопасности». ***(Обнаружены новые атаки буткита Rovnix под прикрытием пандемии // Компьютерное Обозрение (https://ko.com.ua/obnaruzheny_novye_ataki_butkita_rovnix_pod_prikrytiem_pandemii_133544). 26.06.2020).***

***

«О новых атаках с использованием вируса-вымогателя сообщила компания Symantec

Российская хакерская группировка, лидерам которой в декабре были предъявлены обвинения в США, в отместку совершает атаки на американские госучреждения, крупные компании и СМИ…

…хакеры выявляют сотрудников, которые работают из дома во время пандемии, и пытаются проникнуть в их сети с помощью вируса-вымогателя, призванного парализовать их работу.

Новые атаки группировки, которая, по словам Министерства финансов, иногда работает на российскую разведку, были выявлены в последние дни корпорацией Symantec, специализирующейся на кибербезопасности.

В четверг вечером компания сообщила, что российские хакеры воспользовались внезапным изменением в режиме работы американских компаний, внедряя вредоносные коды в корпоративные сети с беспрецедентной скоростью и размахом, пишет газета.

Вирус-вымогатель требует от компаний денег за восстановление данных.

…Министерство внутренней безопасности США пытается в ускоренном порядке обезопасить системы для голосования, опасаясь, что и они подвергнутся атаке, нацеленной на срыв ноябрьских выборов». ***(NYT: Российские хакеры взламывают компьютеры работающих из дома американцев // Голос Америки (https://www.golos-ameriki.ru/a/russian-ransomware-group-reportedly-attacks-us-teleworkers/5478410.html). 26.06.2020).***

***

«Эксперты по кибербезопасности обнаружили новое ПО для скрытой добычи Monero и DDoS-атак, заражающее устройства на базе Windows.

На этой неделе эксперты по безопасности Unit 42 Palo Alto Networks предупредили о новом самораспространяющемся вредоносном ПО, проводящем атаки криптоджекинга и DDoS-атаки на системы Windows. Оно получило название Lucifer.

Согласно исследованию, Lucifer представляет собой гибридную вредоносную программу, которая может осуществлять захват мощностей компьютера для скрытого майнинга Monero и DDoS-атак. Программа использует старые уязвимости платформы Windows.

После взлома злоумышленники выполняют команды, устанавливающие XMRig Miner - приложение для майнинга Monero (XMR). Palo Alto Networks утверждает, что связанный с мошенниками кошелек Monero уже получил 0.493527

XMR. Исследователи предоставили некоторые рекомендации, как не стать жертвой Lucifer:

«Настоятельно рекомендуется своевременно устанавливать обновления и патчи для уязвимого программного обеспечения: Rejetto HTTP File Server, Jenkins, Oracle Weblogic, Drupal, Apache Struts, инфраструктуры Laravel и Microsoft Windows. Надежные пароли также помогут не стать жертвой атаки перебором по словарю».

Тем временем AT&T проанализировала работу скрытого майнинга Monero.

Помимо этого, Trend Micro помогает Интерполу бороться со скрытыми майнерами.

На фоне этого «Касперский» отмечает снижение числа вредоносного ПО для скрытого майнинга». ***(Обнаружено новое ПО для криптоджекинга // LetKnow News (https://letknow.news/news/obnaruzheno-novoe-po-dlya-kriptodzhekinga-37887.html).28.06.2020).***

***

«47 игр в магазине приложений Google Play являются троянами HiddenAds, заявляет компания Avast. Такие приложения могут скрывать свои значки на зараженном устройстве и навязчиво отображают рекламу, даже если пользователь удалит приложение.

Приложения имеют низкую пользовательскую привлекательность и низкий рейтинг, тем не менее, они были загружены более 15 млн раз. Компания уже сообщила в Google Play о найденных приложениях, но, по их словам, некоторые приложения все еще доступны для скачивания и установки.

Такие вирусы, как HiddenAds, могут попасть в официальный магазин Google Play, скрывая свое предназначение или раскрывая вредоносные функции, уже будучи загруженными на устройство, объясняют аналитик по компьютерной безопасности.

Рекламные кампании через трояны HiddenAds сложно предотвратить, поскольку злоумышленники используют одноразовые аккаунты разработчиков для каждого приложения.

При загрузке новых приложений рекомендуется обязательно посмотреть отзывы и особенно внимательно ознакомиться с отрицательными». ***(Ростислав Цуркан . В Google Play нашли 47 игр с троянами // ООО "Национальные информационные системы" (https://podrobnosti.ua/2357081-v-google-play-nashli-47-igr-s-trojanami.html). 26.06.2020).***

***

«Компания ESET, международный эксперт в области информационной безопасности, обнаружила вирус-вымогатель CryCryptor, нацеленный на пользователей Android. Он маскируется под инструмент мониторинга ситуации с COVID-19.

Злоумышленники призывали пользователей скачать программу через два сайта, посвященных коронавирусу. На данный момент оба ресурса заблокированы.

При запуске CryCryptor запрашивал разрешение на доступ к данным жертвы и шифровал файлы. Но вместо того, чтобы заблокировать девайс, малварь оставляла в каждом каталоге файл «readme» с почтой преступника. Это необходимо для оповещения пользователя и требования выкупа.

CryCryptor разработан на основе открытого исходного кода, размещенного на GitHub. Благодаря ошибке разработчиков вредоноса, экспертам ESET удалось оперативно создать дешифровщик. С его помощью жертвы могут вернуть доступ к файлам. Однако, дешифровщик актуален только для этой версии малвари, в других случаях он может оказаться бессилен, и пользователь навсегда потеряет доступ к файлам…». ***(ESET: новый вирус-вымогатель распространяется под видом приложения для мониторинга COVID-19 // ESET (https://www.esetnod32.ru/company/press/center/eset-novyy-virus-vymogatel-rasprostranyaetsya-pod-vidom-prilozheniya-dlya-monitoringa-covid-19/). 25.06.2020).***

***

«Компании, ведущие бизнес в Китае, предупреждены о том, что программное обеспечение, предназначенное для загрузки местными банками, оказалось заражено. Специалисты из компании Trustwave обнаружили бэкдор GoldenSpy в приложении Intelligent Tax. Причем он не удаляется даже после удаления приложения.

Бэкдор позволяет злоумышленнику удаленно выполнять команды Windows или загружать и выполнять любые файлы (включая вирусы-вымогатели, трояны и другие вредоносные программы). По сути, этот бэкдор является широко открытой дверью в сеть с привилегиями системного уровня.

Пока неясно, как бэкдор попал в официальное банковское приложение. Также неясно, какие еще приложения могут быть скомпрометированы и какое число организаций затрагивает данная проблема.

Несмотря на то, что текущая кампания началась в апреле этого года, первые варианты GoldenSpy были обнаружены еще в декабре 2016 года, через несколько месяцев после того, как Aisino (производитель пострадавшего ПО) объявила о новом партнерстве в области «больших данных» с компанией Chenkuo Network Technology.

Комментариев от китайских компаний пока не поступило». ***(Китайское банковское приложение оказалось заражено бэкдором // SecureNews (https://securenews.ru/chinese-banking-application-has-been-infected-by-a-backdoor/). 29.06.2020).***

***

«Эксперты Symantec Threat Intelligence обнаружили, что операторы вымогателя REvil (Sodinokibi) сканировали сеть одной из своих жертв в поисках серверов Point of Sale (PoS).

Исследователи напоминают, что REvil (он же Sodinokibi) это малварь, работающая по схеме шифровальщик-как-усулуга (ransomware-as-a-service, RaaS). REvil специализируется на компрометации корпоративных сетей с помощью

эксплоитов, уязвимых служб удаленного доступа, спама, а также взлома поставщиков управляемых услуг (Managed services providers).

Проникнув в сеть, REvil развивает свою атаку в боковом направлении, похищает информацию со всех доступных серверов и рабочих станций, и лишь после этого шифрует файлы.

Теперь специалисты Symantec заметили, что группировка стала использовать инструментарий для пентестов Cobalt Strike для развертывания пейлоадов REvil в сетях жертв. Так, Cobalt Strike был найден в сетях восьми пострадавших компаний, и злоумышленники зашифровали данные трех крупных компаний, работающих в сферах услуг, пищевой промышленности и здравоохранения.

Аналитики считают, что выбирая крупные и многонациональные компаниями, злоумышленники надеются, что те смогут заплатить большой выкуп за восстановление доступа к своим системам. Так, у каждой пострадавшей компании хакеры потребовали 50 000 долларов в криптовалюте Monero или 100 000, если выкуп не будет вылечен в течение трех дней.

Компании, работающие в сферах услуг и пищевой промышленности, были идеальными целями для злоумышленников, так как это крупные организации, способные заплатить большой выкуп за расшифровку своих данных. Однако организация из сферы здравоохранения была куда меньше и вряд ли могла бы позволить себе такие расходы.

Судя по всему, хакеры тоже это понимали и опасались, что жертва не сможет заплатить за расшифровку файлов. Поэтому операторы REvil сканировали сеть организации в поисках PoS-систем, стремясь на всякий случай найти и похитить еще и информацию о банковских картах.

Исследователи пишут, что это совсем не похоже на обычную тактику операторов REvil в частности и на целевые вымогательские атаки в целом. В скором времени станет ясно, была это незапланированная попытка подстраховаться от невыплаты выкупа, или же среди вымогательских хак-групп наметился новой тренд, который вскоре подхватят и другие хакеры». ***(Мария Нефёдова. Шифровальщик REvil ищет PoS-системы в сетях своих жертв // Хакер (https://xakep.ru/2020/06/24/revil-pos-scan/). 24.06.2020).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Компания Facebook заплатила фирме по кибербезопасности за разработку хакерского инструмента. Таким образом социальная сеть решила помочь ФБР разоблачить преступника из Калифорнии, который неоднократно преследовал девушек в социальной сети Facebook, сообщило издание Motherboard.

Facebook годами отслеживала Бастера Эрнандеса (Buster Hernandez). Преступник использовал защищенную операционную систему Tails, скрывал свой настоящий IP-адрес и продолжал преследовать своих жертв, используя чаты,

электронную почту и Facebook. Компания приняла решение помочь ФБР взломать учетную запись Эрнандеса с целью собрать доказательства, которые позволили бы его арестовать.

Команда безопасности Facebook сотрудничала со сторонней ИБ-фирмой над разработкой хакерского инструмента для эксплуатации уязвимости в видеоплеере Tails. Эксплуатация уязвимости позволяла узнать реальный IP-адрес человека, просматривающего видео. ФБР использовало данный инструмент для отправки Эрнандесу видеоролика, который позволил ведомству собрать доказательства для ареста. В феврале Эрнандес признал себя виновным по 41 пункту обвинения.

По словам сотрудников Facebook, это был первый и единственный раз, когда компания помогла правоохранительным органам преследовать преступника с помощью подобных методов. Как отметило издание, Facebook не сообщила подробности о взломе команде разработчиков Tails». ***(Facebook прибегла к хакерству для помощи в поимке преступника // SecurityLab.ru (https://www.securitylab.ru/news/509157.php). 11.06.2020).***

***

«Двое совладельцев ныне отключенного сервиса DDoS-как-услуга vDOS, который в течение четырех лет помогал своим клиентам осуществить более двух миллионов DDoS-атак, были приговорены к шести месяцам исправительных работ израильским судом. Подсудимые были признаны виновными в нарушении работы компьютерных систем и порче компьютерной информации.

Израильский суд вынес приговоры, а также назначил штрафы и испытательный срок в отношении Ярдена Бидани и Итая Хури, арестованных в 2016 году в возрасте 18 лет в связи с расследованием ФБР в отношении сервиса vDOS.

До закрытия в 2016 году vDOS был самым крупным сервисом DDoS-как-услуга, позволяющим даже совершенно неопытным интернет-пользователям запускать разрушительные атаки и отключать большинство сайтов.

Как сообщается в судебном документе, молодые люди заработали более $600 тыс. с помощью vDOS. В приговоре также упоминается вспомогательная роль 23-летнего Джесси Ву (Jesse Wu), который зарегистрировал компанию-оболочку U.K., используемую сервисом vDOS, и управлял регистратором доменных имен NameCentral. Ву также создал платежную инфраструктуру и получал 15% от общего дохода vDOS за свои услуги.

Владельцы vDOS также продали API-доступ к своей бэкэнд-инфраструктуре атак другим DDoS-сервисам, включая Vstress, Ustress, PoodleStresser и LizardStresser.

Обвиняемые получили самый мягкий приговор из возможных — шесть месяцев общественных работ под надзором израильской тюремной службы. Это связано с тем, что обвиняемые были несовершеннолетними на момент совершения большинства своих преступлений. Судья также наложил небольшие штрафы на каждого из обвиняемых, отметив, что более чем $175 тыс. уже были конфискованы из их прибыли.

vDOS — сервис для организации DDoS-атак, позволявший создавать трафик порядка 50 Гбит/с. Он работал в период с 2012 по 2016 год, и только за четыре месяца в 2016 году суммарное время всех атак на web-сайты с помощью сервиса превысило 3,2 тыс. Суток». ***(Владельцы DDoS-сервиса vDOS отделались 6 месяцами исправительных работ // SecurityLab.ru (https://www.securitylab.ru/news/509009.php). 09.06.2020).***

***

«64-летний Кененти Ким (Kenenty Kim), также известный под псевдонимом Мен Ким (Myung Kim), признался в федеральном суде Южного округа Техаса в осуществлении BEC-атак (business email compromise – компрометация деловой почты), в рамках которых он отправлял поддельные электронные письма сотрудникам компаний якобы от имени руководителей.

В судебных документах указаны две жертвы — строительная компания Solid Bridge и компания Electrolux, являющаяся материнской компанией нескольких крупных брендов бытовой техники.

В первом случае Ким использовал поддельную учетную запись электронной почты, имя которой было похоже на адрес электронной почты настоящей компании, с целью убедить Solid Bridge перевести ему более $200 тыс. Затем преступник переместил похищенные денежные средства на несколько разных банковских счетов, прежде чем поместить их на оффшорный счет.

Ким выдавал себя за владельца легитимной субподрядной компании Chance Contracting в Пайнхерсте, штат Техас. В 2018 году Solid Bridge получила поддельные электронные письма якобы от владельца компании Бретта Чанса (Brett Chance). Как сообщалось в письме, у Чанса возникли проблемы с получением чековых платежей от Solid Bridge, и он попросил Solid Bridge отправить чек на другой почтовый адрес.

Во втором инциденте Ким использовал похожую тактику с целью убедить североамериканское подразделение Electrolux перевести более $300 тыс.

В дополнение к осуществлению BEC-атак Ким также занимался мошенничеством с кредитными картами, заработав около $200 тыс. незаконными методами. Ким создал систему для обработки платежей по кредитным картам, похищал персональную идентификационную информацию жертвы и снимал с ее кредитной карты более $10 тыс. У преступника было 36 разных кредитных карт, зарегистрированных на разные имена, четыре разных номера социального страхования, 11 разных почтовых адресов и ранее приостановленная лицензия на недвижимость.

В рамках соглашения о признании вины Ким сообщил, что с помощью мошеннических схем получил более $700 тыс. Преступнику может грозить до 20 лет тюремного заключения и штраф в размере $500 тыс». ***(Преступник обманул компании Electrlux и Solid Bridge на сумму более $500 тыс. // SecurityLab.ru (https://www.securitylab.ru/news/508972.php). 08.06.2020).***

***

«В 2017 году мы уже рассказывали о деле иранца Камьяра Джаханракхшана (Kamyar Jahanrakhshan, также известен под именами Kamyar Jahan Rakhshan, Andy или Andrew Rakhshan, Andy или Andrew Kamyar, Kamiar или Kamier Rakhshan).

Напомню, что тогда правоохранительные органы США арестовали его в Сиэтле и обвинили в том, что Джаханракхшан пытался шантажировать ряд компаний и их сотрудников, а также устраивал вполне реальные DDoS-атаки для подкрепления своих угроз, покупая мощности у хакерских сервисов ItsFluffy и RageBooter.

Среди пострадавших от его действий числятся юридический ресурс Leagle.com, а также медиакомпании Sydney Morning Herald, Canadian Broadcasting Corporation (CBC), Metro News Canada, официальный сайт правительства Канады и многие другие.

Различными угрозами Джаханракхшан пытался добиться от этих компаний и сайтов удаления ряда ссылок и статей, которые рассказывали о его криминальном прошлом. В ход пошло все, от DDoS-атак, до личных сообщений в адрес сотрудников компаний и посланий, с обещаниями устроить взрыв.

Дело в том, еще в 1991 году злоумышленник получил гражданство США, но проживал в Канаде с 1995 года. Между 2005 и 2011 годами он совершил ряд преступлений, включая кражу и мошенничество, в результате чего в 2014 году его депортировали из Канады в США, после чего Джаханракхшан решил избавиться от записей о своих криминальных деяниях.

Хотя некоторые случаи шантажа (подкрепленные DDoS-атаками) даже увенчались успехом, многие компании не спешили выполнять требования Джаханракхшан. Тогда преступник пошел на крайние меры и начал присылать в офисы компаний сообщения с угрозами устроить взрыв, а также стал угрожать расправой конкретным сотрудникам целевых компаний и их близким.

Как теперь сообщило Министерство Юстиции США, еще в феврале текущего года Камьяр Джаханракхшан признал себя виновным в сговоре с целью совершения компьютерного мошенничества. В результате на прошлой неделе он был приговорен к пяти годам тюремного заключения, а также суд постановил, что он обязуется выплатить более 520 000 долларов в качестве компенсации.

Нужно отметить, что пять лет лишения свободы – это максимальный срок, который хакер мог получить в итоге, так как суд был ограничен досудебным соглашением и признанием вины.

Изначально, в 2018 году, федеральное жюри вообще проголосовало за осуждение Джаханракхшана по статье за умышленную передачу команд защищенному компьютеру, а это правонарушение предусматривает максимальный срок тюремного заключения до 10 лет. Однако позже в том же году суд удовлетворил ходатайство защиты о новом судебном разбирательстве, так как адвокаты защиты сообщили, что они были неэффективны в вопросах представления своего клиента на суде.

Таким образом, в апреле 2019 года первоначальное обвинительное заключение было отменено, но к обвинениям добавился сговор. После этого, перед самым началом повторного процесса, Джаханракхшан решил признать себя

виновным, и срок заключения в итоге не мог превышать 5 лет. Судья отмечает, что если бы не этот нюанс, приговор был бы куда более суровым.

В заявлении Минюста отмечается, что во время слушаний для вынесения приговора обвиняемый всячески препятствовал правосудию, а во время процесса в 2017 году давал ложные показания под присягой. Так, он солгал о наличии 10 адресов электронной почты, которые использовал для совершения преступлений, и солгал о незаконном возвращении в Канаду после депортации.

Забавно, но статьи, удаления которых так отчаянно добивался тогда Джаханракхшан, даже столько лет спустя свободно находятся любым поисковиком…». ***(Мария Нефёдова. DDoS-шантажист получил 5 лет тюрьмы // Xakep (https://xakep.ru/2020/06/16/kamyar-jahanrakhshan-sentence/). 16.06.2020).***

***

«Российского хакера Алексея Буркова, задержанного в Израиле и переданного в США, приговорили к 9 годам тюрьмы.

Отмечается, что Бурков признал свою вину и заявил в суде, что сожалеет о содеянном…

«В детстве я познакомился с хакерами и это увлекло меня на неправильный путь. И лишь в тюрьме я осознал, насколько неправильно веду себя в жизни», – заявил Бурков.

С учетом уже проведенного времени в тюрьме, Бурков сможет выйти на свободу через 4,5 года.

Согласно судебным документам, Бурков управлял веб-сайтом Cardplanet, который продавал номера платежных карт, многие из которых принадлежали гражданам США.

Кроме того, согласно обвинениям, Бурков руководил интернет-форумом по киберпреступности, где хакеры могли общаться, планировать киберпреступления, совершать покупки и продажи краденых товаров и услуг, а также предлагать свои услуги.

Подозреваемого задержали в аэропорту Тель-Авива в 2015 году, когда он приехал в Израиль в отпуск.

Позднее ему предъявили обвинения в преступлениях в сфере кибербезопасности. Сам себя он называл специалистом по информационной безопасности и долго отрицал свою вину…» ***(В США посадили российского кибер-мошенника Алексея Буркова // cursorinfo.co.il (https://cursorinfo.co.il/all-news/v-ssha-posadili-rossijskogo-kiber-moshennika-alekseya-burkova/). 26.06.2020).***

***

«Специалисты по кибербезопасности рассекретили личность русскоязычного хакера под ником Fxmsp, известного в даркнете как одного из самых активных продавцов доступа в корпоративные сети компаний. За три года он нанес ущерб 135 компаниям в 44 странах мира, следует из отчета международной компании Group-IB…

По минимальным оценкам, за это время Fxmsp мог заработать 1,5 миллиона долларов (около 100 миллионов рублей). Среди его жертв были государственные

организации, провайдеры IT-сервисов, ретейлеры, а также банки и организации энергетического сектора.

Вместе с сообщником под ником Lampeduza, осуществлявшего сопровождение всех сделок и отвечавшего за рекламу, с октября 2017 по сентябрь 2019 года они выставили на продажу данные для доступа к десяткам компаний. Пострадавшие предприятия находились в том числе в России, США, Англии, Франции, Италии, Нидерландах, Сингапуре, Японии и Австралии.

По информации Group-IB, с начала 2020 года более 40 киберпреступников стали применять приемы и техники Fxmsp для дальнейшей продажи доступа в корпоративные сети компаний различных отраслей. Как считают в Group-IB, сам хакер продолжает находиться на свободе.

Технический директор Group-IB Дмитрий Волков подчеркнул, что исследование компании позволит ускорить задержание хакера и снизить число желающих следовать его примеру. «Именно поэтому мы приняли решение передать расширенную версию отчета международным правоохранительным органам», — добавил он.

Fxmsp — русскоязычный хакер, который с 2017 года был активен в даркнете. Вскоре он стал абсолютным лидером по числу лотов с доступом в корпоративные сети компаний. Основная активность Fxmsp пришлась на 2018 год, а с начала 2019 года у киберпреступника появились многочисленные последователи». ***(Русскоязычный хакер заработал миллионы в даркнете и был рассекречен // ООО «Лента.Ру» (https://lenta.ru/news/2020/06/23/fxmsp/). 23.06.2020).***

***

«Сергей Медведев, гражданин России, управляющий сервисом обмена и условного депонирования цифровой валюты, который он основал в 2010 году, признал себя виновным по обвинениям в вымогательстве и мошенничестве с платежными картами на сумму 568 миллионов долларов. Правительство США назвало это крупнейшим в истории случаем кибер-мошенничества.

33 -летний Медведев признал в своем заявлении от 26 июня в Окружном суде США штата Невада, что он основал и управлял организацией Infraud, международным предприятием по киберпреступности, которое способствовало продаже краденых кредитных карт и оборудования, вредоносных программ и украденных данных учетных записей в течение восьми лет.

Он также подтвердил наличие службы обмена и условного депонирования «цифровой валюты» для 10 901 члена Infraud. В обвинительном заключении 2018 года говорится, что члены Infraud использовали ныне несуществующий Liberty Reserve и биткойн, среди прочих «цифровых валют», для отмывания своих средств.

В июньском заявлении не упоминается, в какой степени обменный сервис Медведева осуществлялся в биткойнах или других криптовалютах. В нем говорится, что до мая 2013 года Медведев накопил 1,04 миллиона долларов в цифровой валюте Liberty Reserve.

В целом, Infraud способствовал продаже 4 миллионов краденых номеров платежных карт, чем причинил фактический ущерб в размере 568 миллионов

долларов своим жертвам, American Express, Visa, MasterCard и другим, что признал Медведев.

Министерство юстиции закрыло Infraud в феврале 2018 года и впоследствии предъявило обвинение 36 членам организации в рамках операции «Теневая паутина».

По данным Bangkok Post, на момент ареста в Таиланде в 2018 году у Медведева было более 100 000 биткойнов .

Слушание приговора по Медведеву назначено на 9 декабря». ***(Романов Роман. Россиянин признан виновным в кибер-мошенничестве на сумму $568 миллионов // Internetua (https://internetua.com/rossiyanin-priznan-vinovnym-v-kiber-moshennicsestve-na-summu-568-millionov-). 30.06.2020).***

***

Технічні аспекти кібербезпеки

«Ученые из Кембриджского университета и ИБ-компании Industrial Defenica провели интересный эксперимент с целью изучить угрозы, к которым потенциально уязвимы промышленные системы управления, используемые для управления оборудованием в различных сферах - от химических процессов до выработки энергии и систем автоматизации зданий.

Для связи многие промышленные системы управления используют как старые коммуникационные протоколы, так и IP-сети, включая интернет, что создает риски безопасности. Кроме того, уязвимости в таких системах часто остаются неисправленными, к тому же, только некоторые промышленные протоколы используют авторизацию или шифрование.

В рамках исследования специалисты развернули сеть из 120 так называемых ханипотов - ловушек, замаскированных под программируемые логические контроллеры и удаленные терминалы, в 22 странах мира. За 13 месяцев эксперимента исследователи зафиксировали 80 тыс. атак на ханипоты (в основном случаи сканирования через системы Censys или Shodan) и 9 попыток эксплуатации промышленных протоколов (атаки исходили из США, России, Украины, Вьетнама, Китая и с Сейшельских островов), включая 4 попытки использования ранее неизвестных уязвимостей. В одной из этих атак применялся ранее опубликованный PoC-эксплоит. Всю информацию об эксплуатируемых уязвимостях исследователи передали производителям устройств.

Чаще всего специалисты фиксировали DoS-атаки и command-replay атаки. Как пояснил один из авторов эксперимента Майкл Додсон (Michael Dodson), в реальной ситуации DoS-атака могла бы полностью вывести из строя целевое устройство либо нарушить возможность коммуникации по сети.

«Если вы сможете повторно воспроизвести команды, позволяющие изменить состояние или осуществлять запись в регистры, то получите полный контроль над поведением устройства и, соответственно, частью процесса, которым он управляет», - добавил Додсон». ***(Атаки на «ханипоты» раскрыли 4 0Day-***

уязвимости в промышленных системах // SecurityLab.ru (https://www.securitylab.ru/news/509360.php). 21.06.2020).

***

«Эксперты международного проекта "Топ-500" признали японский суперкомпьютер "Фугаку" самым быстрым в мире. Электронная машина находится в Институте естественных наук страны, сообщает информационное агентство Киодо.

"Японский суперкомпьютер показал также лучшие параметры при использовании в промышленности, в сфере искусственного интеллекта и при анализе больших цифр. Машина совершает более 415 квадриллионов вычислений в секунду. Это примерно в 2,8 раза превышает скорость суперкомпьютера "Саммит" из Национальной лаборатории США в Ок-Ридже, который занимал первое место рейтинга с ноября 2019 года"…

В мае "Фугаку" доставили в Центр компьютерных исследований института в городе Кобе. Ожидается, что на полную мощность компьютер заработает с апреля 2021 года. А пока эту машину используют в том числе и для разработок различных препаратов против нового коронавируса». ***(Эксперты назвали самый быстрый в мире комп'ютер // ФГБУ «Редакция «Российской газеты» (https://rg.ru/2020/06/23/eksperty-nazvali-samyj-bystryj-v-mire-kompiuter.html). 23.06.2020).***

***

«Эксперты из некоммерческой организации Shadowserver Foundation опубликовали предупреждение, где в очередной раз рекомендовали компаниям не оставлять принтеры доступными через интернет для всех желающих.

Для своего исследования специалисты просканировали четыре миллиарда адресов IPv4 в поисках принтеров с открытым портом IPP (Internet Printing Protocol). Как нетрудно понять по названию, этот протокол позволяет пользователям управлять подключенными к интернету принтерами и удаленно отправлять им задания на печать.

Разница между IPP и множеством других протоколов для управления принтерами заключается в том, что IPP — безопасный протокол, который поддерживает списки управления доступом, аутентификацию и зашифрованные соединения. Но, к сожалению, это не гарантирует, что владельцы устройств действительно будут использовать какие-то из этих функций.

По данным Shadowserver Foundation, они специально искали в интернете принтеры с поддержкой IPP, но без защиты брандмауэром, которые позволяли бы злоумышленникам запрашивать локальные данные с помощью функции Get-Printer-Attributes.

По словам экспертов, как правило, ежедневно они обнаруживают около 80 000 принтеров, доступных в онлайне через порт IPP. Это число составляет примерно восьмую часть от общего количество принтеров с поддержкой IPP, подключенных к интернету. При обычном сканировании с помощью поисковика

BinaryEdge ежедневно в сети обнаруживается от 650 000 до 700 000 устройств с доступным портом IPP (TCP/631).

С открытыми портами IPP (без брандмауэра и аутентификации) сопряжено сразу несколько проблем. Так, этот порт можно использовать для сбора информации. Многие принтеры с поддержкой IPP охотно сообщают дополнительную информацию о себе, в том числе имя устройства, данные о местоположении, модели, версии прошивки, названии организации и даже Wi-Fi SSID. Исследователи предупреждают, что злоумышленники могут собирать такую информацию, а затем использовать ее для поиска корпоративных сетей для будущих атак.

Кроме того, около четверти от общего числа принтеров с поддержкой IPP (около 21 000) также предоставляют информацию о своей марке и модели. Раскрытие такой информации способно значительно облегчить злоумышленникам процесс обнаружения групп конкретных устройств, уязвимых для определенных проблем.

Инструменты для взлома принтеров посредством IPP совсем не трудно найти в сети. Такие решения как опенсорсный PRET (Printer Exploitation Toolkit) в прошлом уже использовались для массового взлома принтеров, после чего им приказывали печатать произвольные сообщения. При этом в теории инструментарий может быть применен и для более серьезных атак, например, чтобы полностью перехватить контроль над уязвимыми устройствами.

Специалисты Shadowserver Foundation планируют публиковать ежедневные отчеты о доступных через IPP устройствах на своем сайте. Они надеются, что это поможет привлечь внимание к проблеме и, в конечном итоге, приведет к сокращению количества общедоступных принтеров с поддержкой IPP». ***(Мария Нефёдова. В интернете через порт IPP доступны более 80 000 принтеров // Xakep (https://xakep.ru/2020/06/24/ipp-stats/). 24.06.2020).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«В рамках июньского «вторника обновлений» компания Intel исправила более 20 различных уязвимостей в своих продуктах… производитель выпустил обновленные микрокоды для процессоров, уязвимых перед новой MDS-проблемой CrossTalk.

Но одной только CrossTalk дело не ограничилось, и на этой неделе стало известно еще об одной проблеме, так же угрожающей процессорам Intel. Эта ничуть не менее серьезная уязвимость получила название SGAxe, и она представляет собой вариацию спекулятивной атаки CacheOut, обнаруженной в начале 2020 года.

…CacheOut относится к классу уязвимостей Microarchitectural Data Sampling (MDS), в который входят RIDL, Fallout и ZombieLoad, и рна может привести к

утечке данных из процессоров Intel, виртуальных машин и анклавов SGX. Также стоит отметить, что CacheOut является своего рода наследницей другой процессорной проблемы, Foreshadow, которая впервые использовала кэш L1 для извлечения ключей SGX.

По словам исследовательской группы, обнаружившей проблему CacheOut, а теперь еще и SGAxe, меры, которые Intel предприняла для устранения side-channel атак на SGX (обновления микрокодов и новые архитектуры) оказалось недостаточно. Благодаря этому эксплуатация проблемы SGAxe позволяет осуществить атаку типа transient execution, а та приводит к восстановлению криптографических ключей SGX, которым доверяет сервер аттестации Intel.

Механизм аттестации является важной частью SGX. По сути, с его помощью анклавы могут доказать третьим сторонам, что они правильно инициализированы и работают на подлинном процессоре Intel. В частности, это позволяет убедиться, что ПО, работающее внутри ЦП, не было подменено. Таким образом, извлечение ключей аттестации SGX позволяет злоумышленникам выдавать себя за легитимную машину SGX Intel с криптографической точки зрения.

Исследователи отмечают, что атака сработает даже в том случае, если анклав SGX находится в режиме ожидания, то есть она обходит все аппаратные средства защиты.

«Если ключи аттестации машины скомпрометированы, любые секреты, предоставляемые сервером, могут быть тут же прочитаны недоверенным клиентским хост-приложением, тогда как все выходные данные, предположительно созданные анклавами, работающими на стороне клиента, не могут считаться достоверными. Фактически делает все DRM-приложения на основе SGX бесполезными, так как любой секрет может быть легко восстановлен», — объясняют специалисты.

Полный список процессоров, для которых SGAxe представляет опасность, был опубликован специалистами Intel Product Security Incident Response Team (PSIRT) и его можно увидеть здесь.

Хотя в январе Intel уже выпускала исправления для проблемы CacheOut, теперь планируется, что Intel вновь обновит микрокоды для защиты от CacheOut и SGAxe и устранения основной причины этих уязвимостей. Также компания выполнит восстановление Trusted Compute Base (TCB), что приведет к аннулированию всех ранее подписанных и скомпилированных ключей аттестации.

«Этот процесс гарантирует, что ваша система находится в безопасном состоянии и может снова использовать удаленную аттестацию», — пишут исследователи». ***(Мария Нефёдова. Процессоры Intel уязвимы перед атакой SGAxe // Xakep (https://xakep.ru/2020/06/11/sgaxe/). 11.06.2020).***

***

«Ученые из Амстердамского свободного университета и Швейцарской высшей технической школы Цюриха обнаружили новую уязвимость, влияющую на процессоры компании Intel. Баг получил название CrossTalk, и он позволяет вредоносному коду, выполняющемуся в одном ядре процессора,

«сливать» данные другого софта, работающего на другом ядре (в том числе в анклавах Intel SGX).

Исследователи объясняют, что CrossTalk представляет собой еще одну вариацию MDS-бага. Напомню, что проблемы Microarchitectural Data Sampling (MDS) были обнаружены в процессорах Intel весной 2019 года.

Тогда эксперты выявили сразу четыре новые уязвимости и разделили их на три группы: RIDL, Fallout и ZombieLoad (CVE-2018-12130, CVE-2018-12126, CVE-2018-12127 и CVE-2018-11091). Равно как и нашумевшие уязвимости Spectre и Meltdown, новые баги оказались связаны с упреждающим (или спекулятивным — speculative) механизмом исполнения команд. Они позволяли атакующему считывать данные из тех мест, к которым у него не должно быть доступа (ядро ОС, процессы, анклавы Software Guard eXtensions), а затем похищать пароли, криптографические ключи и прочие данные.

CrossTalk атакует данные, пока те обрабатываются Line Fill Buffer (LBF), одной из систем кэш-памяти ЦП. По словам экспертов, проблема заключается в том, что кэш LBF, по сути, работает с ранее недокументированным «промежуточным буфером» (staging buffer), который используется всеми ядрами процессора.

«С помощью CrossTalk мы обнаружили, что различные инструкции выполняют offcore-запросы на чтение данных из промежуточного буфера, совместно используемого всеми ядрами ЦП. Мы заметили, что этот промежуточный буфер содержит конфиденциальную информацию, включая выходные данные аппаратного генератора случайных чисел Digital Random Number Generator (DRNG), и что такие данные могут передаваться между ядрам с помощью атак RIDL (они же MDS)», — пишут эксперты.

Видеоролик ниже демонстрирует, как CrossTalk используется для атаки на упомянутый промежуточный буфер через кэш LBF, а затем это приводит к утечке данных из других ядер (в видео рассматривается утечка ключа Intel SGX)…

Стоит отметить, что исследователи не только создали для проблемы CrossTalk собственный сайт, но также подготовили подробный технический доклад об уязвимости и опубликовали PoC-эксплоит на GitHub.

Исследовательская группа пишет, что работала со специалистами Intel над исправлением проблемы CrossTalk более 20 месяцев (с сентября 2018 года). Специалисты объясняют, что из-за сложности проблемы на исправление уязвимости ушло куда больше стандартных 90 дней, кроме того, изначально возможность «межъядерной» утечки вообще не рассматривалась.

Инженеры Intel, в свою очередь, опубликовали собственный отчет, где сообщают, что уже внесли значительные изменения в свои ЦП, и для большинства свежих продуктов компании CrossTalk не представляет угрозы.

Что касается более старых процессоров, для них на этой неделе были выпущены обновленные микрокоды для исправления CrossTalk: обновление Special Register Buffer Data Sampling (SRBDS, CVE-2020-0543, Intel-SA-00320).

Полный список из пятидесяти с лишним уязвимых процессоров (мобильных, десктопных и серверных) можно найти здесь. В частности, атака опасна для процессоров Core от 3 до 10 поколения, Core X-Series, Pentium, Celeron и Xeon E3.

При этом представители Intel подчеркивают, что на сегодняшний день вряд ли можно говорить о каких-то реальных атаках с использованием CrossTalk вне контролируемой тестовой среды». ***(Мария Нефёдова. Атака CrossTalk представляет угрозу для мобильных, десктопных и серверных процессоров Intel // Xakep (https://xakep.ru/2020/06/10/crosstalk/). 10.06.2020).***

***

«…Разработчики Adobe тоже исправили ряд серьезных проблем в составе Flash Player, Framemaker и Experience Manager.

Во Flash Player, обновления безопасности для которого продолжат выходить лишь до конца текущего года, была устранена критическая use-after-free уязвимость. Проблема позволяла злоумышленнику выполнить произвольный код в контексте текущего пользователя. Патч для этой уязвимости включен в состав Flash Player 32.0.0.387 (в том числе для Chrome, Edge и Internet Explorer).

В процессоре документов Adobe FrameMaker были исправлены сразу три критических уязвимости, включая две проблемы out-of-bounds записи, которые допускают выполнение произвольного кода, а также ошибку нарушения целостности информации в памяти, которая тоже может быть использована для выполнения кода.

В решении для управления контентом Adobe Experience Manager было устранено шесть XSS-багов, а также уязвимость, связанная с подделкой запросов на стороне сервера (server-side request forgery, SSRF). Все эти уязвимости оцениваются как важные. Так, XSS-проблемы можно использовать для выполнения произвольного кода JavaScript в браузере пользователя, а SSRF для получения конфиденциальной информации.

Adobe сообщает, что эти уязвимости не находились под атаками и не использовались злоумышленниками…» ***(Мария Нефёдова. Adobe устранила критические уязвимости во Flash и Framemaker // Xakep (https://xakep.ru/2020/06/10/adobe-june-patches/). 10.06.2020).***

***

«Специалисты команды Cisco Talos сообщили о критической уязвимости (CVE-2020-12405) в браузере Mozilla Firefox, эксплуатация которой позволяет злоумышленнику удаленно выполнить код. Уязвимость была обнаружена исследователем Марцином Нога (Marcin Noga).

Проблема получила оценку в 8,8 балла по шкале CVSS и может быть проэксплуатирована только тогда, когда пользователь переходит на вредоносную страницу. Уязвимость затрагивает версию Firefox 76.0a1 x64 и содержится в компоненте SharedWorker и внутренних объектах, связанных с ним.

Как пояснили эксперты, для объекта SharedWorkerService выделение выполняется внутри потока, а освобождение происходит в результате обработки следующего события внутри другого потока. Однако выполнение потока продолжается, что приводит к использованию после освобождения объекта SharedWorkerService.

Уязвимость связана с отсутствием объекта Mutex в методе GetOrCreateWorkerManager. Таким образом, один и тот же объект SharedWorkerService передается в качестве аргумента методу GetOrCreateWorkerManagerRunnable и удаляется с помощью деструктора ~SharedWorkerManagerHolder ().

«Корректная очистка кучи может дать злоумышленнику полный контроль над уязвимостью типа использование после освобождения (use-after-free) и, как следствие, может превратить ее в выполнение произвольного кода», — объяснили специалисты.

Для того чтобы проэксплуатировать уязвимость, злоумышленнику необходимо создать web-страницу HTML и настроить ее таким образом, чтобы она вызывала состояние гонки и приводила к уязвимости типа использование после освобождения, а затем к удаленному выполнению кода». ***(В браузере Mozilla Firefox обнаружена RCE-уязвимость // SecurityLab.ru (https://www.securitylab.ru/news/509151.php). 11.06.2020).***

***

«Компания Arm, являющаяся одним из крупнейших производителей RISC-процессоров (с архитектурой ARM), выпустила руководство для разработчиков программного обеспечения с подробным описанием мер предотвращения эксплуатации новой уязвимости (CVE-2020-13844), обнаруженной в архитектуре процессора Armv8-A (Cortex-A).

Проблема, получившая название SLS (Straight-Line Speculation), представляет собой атаку по сторонним каналам со спекулятивным выполнением команд (Speculative Execution).

Спекулятивное выполнение позволяет повысить производительность, оптимизируя загрузку операционных блоков CPU. Для того чтобы точки ветвления программного кода не останавливали его опережающее выполнение, используется логика предсказания ветвлений. Собирая статистику о ранее выполненных ветвлениях, процессор определяет наиболее вероятные целевые адреса, отдавая им приоритет при опережающем исполнении инструкций, в расчете на то, что после условного или косвенного перехода, выполнение программы продолжится по предсказанному адресу. В этом случае результаты заблаговременно выполненных действий будут востребованы. Атаки по сторонним каналам со спекулятивным выполнением команд позволяют злоумышленникам читать конфиденциальные данные.

SLS представляет собой еще одну форму уязвимостей Spectre, однако затрагивает только процессоры Arm Armv-A.

Хотя вычислительные операции являются частью процесса спекулятивного выполнения, когда происходит изменение в потоке управления командами процессора Arm, ЦП реагирует, выполняя команды, найденные в своей памяти, после изменения потока управления.

По словам экспертов, на практике будет сложно использовать уязвимость, и пока еще никто не представил рабочий эксплоит для данной уязвимости.

Компания еще с прошлого года активно работает над решением проблемы. Инженеры разработали исправления для различных программных проектов и операционных систем, включая FreeBSD, OpenBSD, Trusted Firmware-A и OP-TEE. Выпущенные патчи должны блокировать попытки эксплуатации на уровне прошивки и ОС. Компания также предоставила исправления для GCC и LLVM — двух самых популярных на сегодняшний день компиляторов кода.

В отличие от ситуации с Spectre и Meltdown, данные исправления вряд ли будут оказывать негативное влияние на производительность.

Уязвимость SLS была обнаружена исследователями безопасности в рамках проекта Google SafeSide, изучающего атаки по сторонним каналам». ***(Процессоры Arm уязвимы к атакам по сторонним каналам // SecurityLab.ru (https://www.securitylab.ru/news/509122.php). 10.06.2020).***

***

«ИБ-специалист опубликовал эксплоит и информацию о новой уязвимости в UPnP, получившей название CallStranger (CVE-2020-12695). Проблема позволяет злоумышленникам захватывать контроль над различными «умными» устройствами, использовать их для DDoS-атак, а также для обхода защитных решений, сканирования внутренней сети жертвы и хищения данных.

Уязвимость связана с набором сетевых протоколов UPnP, которые в наши дни можно найти на большинстве «умных» устройств. Напомню, что UPnP позволяет устройствам видеть друг друга в локальных сетях, а затем устанавливать соединение, обмениваться данными, настройками и так далее. С 2016 года разработкой и стандартизацией набора протоколов занимается Open Connectivity Foundation.

Проблема CallStranger была обнаружена в декабре 2019 года ИБ-исследователем Юнусом Чадырджи (Yunus Çadirci). Он объясняет, что проблема похожа на SSRF: злоумышленник может отправлять на удаленное устройство TCP-пакеты, содержащие искаженное значение параметра callback в заголовке для функции SUBSCRIBE.

Используя CallStranger, хакер нацеливается на «смотрящий» в интернет интерфейс устройства, однако выполнение кода задействует UPnP-функциональность устройства, которая обычно работает лишь на внутренних портах, то есть внутри локальной сети.

Искаженный заголовок может использоваться для атак на любые устройства, подключенные к интернету и поддерживающие UPnP, включая камеры наблюдения, видеорегистраторы, принтеры, маршрутизаторы и многое другое. В частности, Чадырджи пишет, что проблема распространяется на ПК под управлением Windows, игровые приставки, телевизоры и маршрутизаторы производства Asus, Belkin, Broadcom, Cisco, Dell, D-Link, Huawei, Netgear, Samsung, TP-Link, ZTE и так далее.

У CallStranger есть несколько применений. Так, атакующие могут использовать CallStranger, чтобы обойти защитные решения и межсетевые экраны, а также сканировать внутренние сети компаний. Более того, проблема может

использоваться и для организации DDoS-атак (злоумышленник может усилить TCP-трафик, используя для этого поддерживающие UPnP-устройства с доступом к интернету) и хищения данных.

Чадырджи еще в прошлом году уведомил о проблеме представителей Open Connectivity Foundation, и с тех пор организация уже обновила спецификации для протоколов UPnP. Обновления были выпущены 17 апреля 2020 года, но эксперты CERT/CC предупреждают, что далеко не все поставщики успели применить эти исправления на практике.

Специалисты CERT/CC и Чадырджи сходятся во мнении, что для окончательного устранения проблемы может потребоваться очень много времени, так как речь все же идет о проблеме в протоколе. В настоящее время, по данным поисковика Shodan, в интернете можно обнаружить 5,4 млн устройств с поддержкой UPnP, которые могут пострадать от атак хакерских групп и стать участниками ботнета. При этом исследователь и вовсе предупреждает о том, что уязвимых девайсов могут насчитываться миллиарды». ***(Мария Нефёдова. Уязвимость CallStranger позволяет устраивать DDoS-атаки и сканировать локальные сети // Xakep (https://xakep.ru/2020/06/09/callstranger/). 09.06.2020).***

***

«Специалисты из компании RiskSense проанализировали 54 проекта с открытым исходным кодом и сообщили, что количество уязвимостей в данных инструментах удвоились в 2019 году — с 421 проблемы в 2018 году до 968 в прошлом году.

Как сообщается в отчете «The Dark Reality of Open Source», эксперты обнаружили в общей сложности 2694 уязвимости в популярных проектах с открытым исходным кодом в период с 2015 года по март 2020 года. В отчет не вошли такие популярные платформы, как Linux, WordPress, Drupal, поскольку они постоянно проверяются, а исправления для уязвимостей выпускаются достаточно быстро.

Эксперты из RiskSense рассмотрели другие популярные проекты с открытым исходным кодом, которые не так хорошо известны, но используются сообществом разработчиков программного обеспечения. Это включало такие продукты, как Jenkins, MongoDB, Elasticsearch, Chef, GitLab, Spark, Puppet и пр.

Одна из основных проблем заключалась в том, что большое количество уязвимостей были переданы в Национальную базу данных уязвимостей США (National Vulnerability Database, NVD) спустя много недель после их обнародования. В среднем уходит около 54 дней на уведомление об обнаруженной уязвимости в проанализированных проектах. Например, сообщения об уязвимостях в PostgreSQL передаются в NVD спустя восемь месяцев.

По словам специалистов, среди всех 54 проанализированных проектов сервер автоматизации Jenkins и сервер баз данных MySQL содержали самые опасные уязвимости с 2015 года.

Напомним, ранее специалисты из компании Veracode проанализировали 351 тыс. внешних библиотек в 85 тыс. приложений и отметили высокую распространенность библиотек с открытым исходным кодом. Например,

большинство JavaScript-приложений содержат сотни библиотек с открытым исходным кодом, а некоторые — более 1 тыс. 70% настольных и мобильных приложений содержат как минимум одну уязвимость, связанную с использованием библиотеки с открытым исходным кодом». ***(Число уязвимостей в проектах с открытым исходным кодом удвоилось в 2019 году // SecurityLab.ru (https://www.securitylab.ru/news/509102.php). 10.06.2020).***

***

«Агентство по кибербезопасности и безопасности инфраструктуры (CISA) США предупредило пользователей Windows о том, что недавно опубликованный PoC-эксплоит для «червеобразной» уязвимости в Windows 10 (CVE-2020-0796) используется для осуществления атак.

SMBGhost, также известный как CoronaBlue, представляет собой уязвимость, затрагивающую версию сетевого протокола передачи данных Microsoft Server Message Block 3.1.1 (SMBv3). Уязвимость затрагивает ОС Windows 10 и Windows Server и может использоваться для DoS-атак, повышения локальных привилегий и выполнения произвольного кода на системе.

Для осуществления атак на SMB-серверы злоумышленнику необходимо отправить вредоносные пакеты на целевую систему. Преступник также должен обманом убедить жертву подключиться к вредоносному SMB-серверу.

Компания Microsoft сообщила об опасности уязвимости, а затем выпустила исправления и меры предотвращения эксплуатации уязвимости в марте нынешнего года. Исследователи начали публиковать PoC-эксплоиты для уязвимости вскоре после ее раскрытия, но они касались только DoS-атак или повышения привилегий. Несколько компаний и исследователей утверждали, что разработали PoC-коды для эксплуатации уязвимости, обеспечивающие удаленное выполнение кода, но ни один из них не был обнародован.

Однако на прошлой неделе исследователь, использующая псевдоним Chompie, опубликовала PoC-эксплоит для SMBGhost, позволяющий удаленно выполнить код. По словам Chompie, не является на 100% надежным и может привести к сбою в работе системы, однако несколько экспертов, протестировавших эксплоит, подтвердили, что удаленное выполнение кода можно осуществить.

CISA порекомендовало пользователям и администраторам установить исправления для SMBGhost и блокировать порты SMB с помощью межсетевого экрана и предупредило, что уязвимость в настоящее время эксплуатируется преступниками». ***(CISA предупредило об атаках с использованием уязвимости SMBGhost // SecurityLab.ru (https://www.securitylab.ru/news/509004.php). 08.06.2020).***

***

«Специалисты из компании Cisco Talos обнаружили две критические уязвимости в программном обеспечении для видеоконференций Zoom. Эксплуатации уязвимостей позволяет злоумышленнику взломать компьютерные системы через чат.

Проблемы представляют собой уязвимости обхода пути, которые могут быть использованы злоумышленниками для записи или установки произвольных файлов на системах с установленными уязвимыми версиями Zoom. Преступник может использовать уязвимости путем отправки специально сформированного сообщения в чате.

Первая уязвимость (CVE-2020-6109) связана с тем, как Zoom использует сервис GIPHY, позволяющий пользователям искать и обмениваться анимированными GIF-файлами через чат. Zoom не проверяет источник GIF-файлов и сохраняет изображение на системе получателей в определенной папке, позволяя злоумышленникам отправлять GIF-файлы с вредоносного сервера.

Вторая проблема — уязвимость удаленного выполнения кода (CVE-2020-6110), связанная с процессом обработки фрагментов кода, передаваемых через чат. Отправка специально сформированного сообщения пользователям чата может вызвать произвольную установку двоичного кода, который может быть использован для выполнения произвольного кода на системе.

Функциональность чата Zoom построена на основе XMPP-протокола с дополнительными расширениями, одно из которых поддерживает функцию включения фрагментов исходного кода с полной поддержкой подсветки синтаксиса. Функция отправки фрагментов кода реализована как расширение поддержки обмена файлами и требует установки дополнительного плагина, но для их получения установка не требуется.

Программное обеспечение создает zip-архив, содержащий фрагмент общего кода перед отправкой, который распаковывается на системе получателя. Функция извлечения zip-файлов в Zoom не проверяет содержимое zip-файла перед его извлечением, что позволяет злоумышленнику устанавливать произвольные двоичные файлы на целевых системах без взаимодействия с пользователем.

Уязвимости затрагивают версию Zoom 4.6.10, компания исправила их в версии 4.6.12». ***(Уязвимости в Zoom позволяют взламывать системы через чат // SecurityLab.ru (https://www.securitylab.ru/news/508920.php). 05.06.2020).***

***

«Исследователи безопасности из компании NCC Group обнаружили 26 уязвимостей в операционной системе реального времени Zephyr, специально разработанной для IoT-приложений, и аппаратно-независимом загрузчике с открытым исходным кодом MCUboot. Эксплуатация уязвимостей позволяет злоумышленнику вызвать отказ в обслуживании (DoS) и повысить привилегии.

Данные компоненты содержатся в ряде датчиков и IoT-устройств, включая детские мониторы, светодиоды и беспроводные шлюзы.

NCC Group обнаружила 25 уязвимостей в Zephyr, и одну в MCUboot. Эксперты обнаружили проблемы, связанные с повреждением памяти, множественные пути, позволяющие скомпрометированному пользовательскому приложению повысить привилегии до уровня ядра, и многочисленные уязвимости в дизайне некоторых систем защиты в ядре. Проблемы могут быть проэксплуатированы как локально, так и удаленно.

Уязвимость удаленного повреждения памяти в стеке Zephyr IPv4 может быть проэксплуатирована путем отправки одного специально сформированного ICMP-пакета. Синтаксический анализатор MQTT также содержал уязвимость (CVE-2020-10062) удаленного повреждения памяти, которая была связана с некорректной проверкой полей длины, извлеченных из заголовка MQTT-пакета.

Стек IPv6 содержит DoS-уязвимость — удаленный злоумышленник может нарушить работоспособность ядра путем отправки серии вредоносных пакетов. Другая DoS-уязвимость (CVE-2020-10063) была обнаружена в драйвере протокола CoAP.

В подсистеме USB было обнаружено несколько проблем, которые могут быть проэксплуатированы вредоносным хостом с подключенным к нему устройством Zephyr. Например, драйвер USB DFU содержал опасную уязвимость (CVE-2020-10019) повреждения памяти, а драйвер USB-накопителя содержал множественные уязвимости (CVE-2020-10021) повреждения памяти и проблемы, позволяющие извлечь данные из памяти. Недочет в дизайне USB DFU позволяет атакующему раскрыть образ прошивки в открытом тексте во внутренней памяти микроконтроллера и таким образом обойти функцию шифрования в MCUboot.

В настоящее время были исправлены 15 из 26 обнаруженных проблем». ***(В компонентах IoT-устройств обнаружено 26 уязвимостей // SecurityLab.ru (https://www.securitylab.ru/news/508787.php). 02.06.2020).***

***

«Фахівець з кібербезпеки з Делі Бхавук Джайн виявив помилку в системі авторизації “Вхід з Apple”. З її допомогою зловмисники отримували доступ до акаунтів користувачів, якщо ті переходили на сторонні сайти, використовуючи обліковий запис в Apple…

Тепер же компанія оцінила старання програміста, і вручила йому 100 тисяч доларів за виявлений баг, який ставив під загрозу роботу всієї системи Apple iPhone. Швидше за все, цей баг працював ще з 2019 року, коли його презентувала яблучна корпорація.

В Apple запевнили спеціаліста, провели внутрішнє розслідування і з'ясували, що до того, як вразливість прибрали, жодного випадку злому аккаунта не було виявлено. Нагадаємо, що ще в січні компанія Google Виявила в браузері Safari подібну помилку…» ***(Apple озолотило програміста на 100 тисяч доларів за знайдений в iPhone баг // Знай.ua (https://techno.znaj.ua/314876-apple-ozolotilo-programista-na-100-tisyach-dolariv-za-znaydeniy-v-iphone-bag). 02.06.2020).***

***

«В WhatsApp, одному з найпопулярніших месенджерів, знову виявили проблему безпеки. Повідомляється, що тепер користувачі можуть бачити свої особисті телефонні номери в загальнодоступних результатах пошуку Google. А це дає нові можливості для всіх видів шахрайства і кібератак. Дивно, але у популярного месенджера WhatsApp захист даних користувачів побудована не кращим чином. Тепер користувачі можуть піддатися атаки хакерів.

Дослідник безпеки (Athul Jayaram) виявив 300000 номерів, оприлюднених за допомогою цієї “дірки”. При натисканні на веб-сторінку не розкривається повне ім'я користувача, але з'являється його зображення в профілі месенджера. Таким чином, навіть приховування номера не допоможе залишатися інкогніто. Враховуючи, що в WhatsApp більше мільярда користувачів щодня, збиток від такої витоку може бути колосальний.

Він з'ясував про цей недолік безпеки ще 23 травня і повідомив про цю проблему Facebook через програму винагороди за помилки. Проте заявка була відхилена на тій підставі, що користувачі WhatsApp повністю контролюють інформацію, прикріплену до їх профілю, яка є загальнодоступною. Можливо, компанія змінить своє рішення, якщо користувачі будуть скаржитися на форумах, що точно негативно вплине на популярність месенджера». ***(Дані мільйонів користувачів WhatsApp виявилися в пошуковику Google // Знай.ua (https://techno.znaj.ua/316877-dani-milyoniv-koristuvachiv-whatsapp-viyavilisya-v-poshukoviku-google). 11.06.2020).***

***

«Персональные данные пользователей мессенджера WhatsApp могут стать добычей злоумышленников из-за функции Click to Chat, присваивающей номеру телефона QR-код, написал в своём блоге на портале Medium специалист в области безопасности Атул Джаярам.

«Эта функция не шифрует телефонный номер, поэтому, если эта ссылка используется где-либо, ваш телефонный номер также отображается в виде открытого текста. Например, вы делитесь этой ссылкой с другом в твиттере, чтобы связаться с вами в WhatsApp. Номер вашего мобильного телефона отображается в текстовом виде в этом URL-адресе, и любой, кто получит этот URL-адрес, может узнать номер вашего мобильного телефона», - отметил Джаярам.

Как пояснил эксперт, уязвимость уже затронула свыше 30 тыс. пользователей мессенджера. Получив доступ к телефонному номеру жертвы, мошенники могут осуществлять спам-рассылки, спам-звонки и использовать эти данные для создания баз данных, предназначенных для последующей перепродажи.

Обнаружив уязвимость, Джаярам сообщил в Facebook о найденной уязвимости, однако в компании сообщили, что индексируют только ту информацию, которую сами пользователи согласились сделать открытой». ***(Пользователей WhatsApp предупредили об уязвимости их персональных даннях // Rambler News Service (RNS) (https://rns.online/internet/Polzovatelei-WhatsApp-predupredili-ob-uyazvimosti-ih-personalnih-dannih-2020-06-09/). 09.06.2020).***

***

«Специалисты из JSOF, небольшой компании-консультанта по кибербезопасности, расположенной в Иерусалиме (Израиль), обнаружили 19 уязвимостей — в совокупности именуемых Ripple20 — в небольшой библиотеке, выпущенной в 1997 году софтверной фирмой Treck из Цинциннати (штат Огайо).

За прошедшие с тех пор более двух десятков лет эта библиотека, содержащая облегченный стек TCP/IP для подключения маломощной техники к Интернету, была интегрирована в «сотни миллионов» промышленных и потребительских продуктов. Список уязвимого оборудования включает устройства умного дома, медицинские системы жизнеобеспечения, производственную технику, принтеры, маршрутизаторы, авионику, различные решения уровня предприятия и многое другое.

JSOF с группами реагирования на компьютерные инциденты (CERT) в разных странах проделали большую работу по координации процесса выявления и исправления уязвимостей. В понедельник Treck сообщила о готовности патчей для всех уязвимостей Ripple20.

Тем не менее, эксперты опасаются, что продукты, использующие эту библиотеку, в большинстве своём останутся уязвимыми из-за сложных или неотслеживаемых цепочек поставок компонентов их программного обеспечения. Они указали, что многие компании вообще не знают о том, что у них применяется этот код, и название уязвимой библиотеки не фигурирует в их кодовых манифестах.

Не все 19 уязвимостей Ripple20 опасны, однако в вышедшем вчера бюллетене Министерство внутренней безопасности США присвоило четырём из них рейтинги 10 и 9,8 по 10-балльной шкале серьезности уязвимостей CVSSv3.

Эти четыре уязвимости позволяют преступникам легко брать под контроль интеллектуальные устройства, любое промышленное или медицинское оборудование. Атаки возможны через Интернет или из локальных сетей, например, через взломанный маршрутизатор. Установка патчей от этих четырёх проблем, таким образом, является приоритетной задачей для любой компании». ***(Уязвимая библиотека TCP/IP за 20 лет обрела прописку в миллионах устройств IoT // Компьютерное Обозрение (https://ko.com.ua/uyazvimaya_biblioteka_tcp_ip_za_20_let_obrela_propisku_v_millionah_ustrojstv_iot_133425). 17.06.2020).***

****

«ИБ-эксперты Адам Николс (Adam Nichols) и d4rkn3ss независимо друг от друга обнаружили, что 79 моделей маршрутизаторов Netgear уязвимы для серьезного бага, который может позволить хакерам удаленно захватить контроль над устройством.

Уязвимость затрагивает 758 различных версий прошивки, которые использовались в 79 роутерах Netgear на протяжении многих лет, причем некоторые версии прошивки можно найти на устройствах, выпущенных еще в далеком 2007 году.

Специалисты пишут, что уязвимость связана с компонентом веб-сервера, который входит в состав прошивок Netgear. Данный веб-сервер используется для обеспечения работы встроенной панели администрирования. Николс рассказывает, то сервер некорректно проверяет вводимые пользователем данные, не использует canary's куки для защиты памяти, а бинарник сервера скомпилирован не как Position-independent Executable (PIE), то есть защита ASLR не применяется.

Все это позволяет злоумышленнику направлять уязвимому устройству вредоносные HTTP-запросы, которые можно использовать для перехвата контроля над маршрутизатором.

PoC-эксплоит уже опубликован на GitHub, и Николс отмечает, что в итоге ему «удалось запустить telnet-демон [маршрутизатора] с правами root на TCP-порту 8888 и ввод пароля не требовался».

Еще в начале текущего года оба исследователя сообщили об уязвимости представителям Netgear. Но из-за высокой опасности проблемы и большого объема работы, требующейся для создания и тестирования патчей, производитель попросил экспертов временно придержать информацию о баге и запросил больше времени. В итоге отсрочка истекла на этой неделе, исправления так и не были выпущены, и эксперты решили все же обнародовать данные о проблеме.

Работа над патчами по-прежнему ведется, но точные сроки их выхода пока не называются. К тому же ожидается, что не все маршрутизаторы вообще получат исправления, так как некоторые из них уже давно не поддерживаются.

Список уязвимых версий прошивок для всех уязвимых моделей маршрутизаторов можно найти здесь». ***(Мария Нефёдова. 79 моделей роутеров Netgear в опасности из-за неисправленного бага // Хакер (https://xakep.ru/2020/06/19/netgear-routers-bug/). 19.06.2020).***

***

«Специалисты из компании NanoLock Security сообщили о критической уязвимости во встроенном программном обеспечении некоторых домашних маршрутизаторов Buffalo, эксплуатация которой позволяет злоумышленникам перехватить контроль над устройством.

Проводные и беспроводные маршрутизаторы, используемые миллионами пользователей, уязвимы к атакам с использованием уязвимости в прошивке, позволяющей откатить версию ПО до менее безопасной (с исправленной версии 2.46 до уязвимой 2.34) и затем использовать сетевой протокол telnet для компрометации устройства.

Как утверждают специалисты, проблема затрагивает миллионы устройств, продаваемых японским производителем Buffalo и его дочерней компанией в США — Buffalo Americas. Эксперты уведомили Buffalo о своих находках в 2019 году, однако производитель маршрутизаторов еще не выпустил исправление для уязвимости». ***(В прошивке маршрутизаторов Buffalo обнаружена критическая уязвимость // SecurityLab.ru (https://www.securitylab.ru/news/509410.php). 23.06.2020).***

***

«В феврале текущего года специалисты Palo Alto Networks выявили ряд серьезных уязвимостей в маршрутизаторах D-Link DIR-865L, о чем поспешили сообщить производителю. К сожалению, данная модель роутера, выпущенная еще в 2012 году, уже вообще не поддерживается в США, хотя для европейских пользователей статус этого продукта обозначен как «End of Sale». Это

означает, что модель уже снята с продажи, однако еще должна поддерживаться производителем.

Увы, как стало известно теперь, из-за «почтенного возраста» этой модели, роутеры все же получили исправления не для всех обнаруженных уязвимостей. Так, исследователи выявили следующие баги в D-Link DIR-865L:

CVE-2020-13782: инъекция команд, критическая уязвимость (9,8 баллов по шкале CVSS); не исправлена;

CVE-2020-13786: CSRF-уязвимость, высокий уровень серьезности (8,8 баллов по шкале CVSS); исправлена;

CVE-2020-13785: некорректная криптографическиая стойкость, высокий уровень серьезности (7,5 баллов по шкале CVSS); исправлена;

CVE-2020-13784: предсказуемое seed в генераторе псевдослучайных чисел, высокий уровень серьезности (7,5 баллов по шкале CVSS); не исправлена;

CVE-2020-13783: хранение конфиденциальной информации открытым текстом, высокий уровень серьезности (7,5 баллов по шкале CVSS); исправлена;

CVE-2020-13787: передача конфиденциальной информации открытым текстом, высокий уровень серьезности (7,5 баллов по шкале CVSS); не исправлена.

Стоит отметить, что хотя уязвимость CVE-2020-13782 получила статус критической, в своем отчете исследователи пишут, что ее использование все же требует аутентификации. И хотя этого можно добиться с помощью вышеупомянутого CSRF-бага, это все же снижает уровень опасности проблемы. Тем не менее, эксперты говорят и о том, что объединение некоторых из этих уязвимостей может позволить злоумышленникам перехватывать сетевой трафик жертвы и похищать cookie сессий, что, разумеется, очень опасно.

Специалисты D-Link отреагировала на сообщение экспертов релизом бета-версии прошивки, однако, как уже можно было понять по вышеприведенному списку, в ней были исправлены лишь три уязвимости из шести перечисленных: CSRF, слабое шифрование и хранение конфиденциальной информации открытым текстом.

Более того, пользователям из США представители D-Link вообще рекомендуют отказаться от использования проблемных роутеров, так как это может представлять опасность для подключенных к ним устройств и конечных пользователей.

Издание Bleeping Computer обратилось за комментарием к представителям компании, желая узнать судьбу трех оставшихся уязвимостей, но производитель так и не ответил. Журналисты отмечают, что большинство пользователей крайне редко меняют свои маршрутизаторы и не следят за истечением периода их поддержки. Данный тип оборудования скорее относится к разряду «установи и забудь», а меняют роутеры лишь тогда, когда они перестают функционировать. Из-за этого вряд ли стоит рассчитывать на то, что многие владельцы D-Link DIR-865L когда-либо прочтут предупреждение производителя или установят патчи хотя бы для трех из шести уязвимостей». ***(Мария Нефёдова. Роутеры D-Link не получили исправлений для критических багов // Xakep (https://xakep.ru/2020/06/16/d-link-dir-865l/). 16.06.2020).***

***

«Во вторник, 30 июня, Кибернетическое командование США предупредило о том, что иностранные хакеры, скорее всего, попытаются эксплуатировать раскрытую в этот же день уязвимость в PAN-OS.

PAN-OS представляет собой операционную систему для межсетевых экранов и корпоративных VPN-установок от компании Palo Alto Networks.

«Пожалуйста, немедленно установите исправления на все устройства, затронутые CVE-2020-2021, в особенности, если используется SAML», - сообщило Киберкомандование в своем Twitter. Как считают в Киберкомандовании, уже скоро АТР-группы начнут атаки с использованием данной уязвимости.

Опасения американских властей небеспочвенны. CVE-2020-2021 – тот редкий случай, когда опасность уязвимости была оценена в 10 баллов из 10 по шкале CVSSv3. Другими словами, ее может легко проэксплуатировать даже малоопытный хакер, причем удаленно через интернет, без необходимости сначала проникать в атакуемое устройство.

Проблема представляет собой уязвимость обхода аутентификации, позволяющую злоумышленнику получить доступ к устройству без ввода действительных учетных данных. Проэксплуатировав ее, атакующий может менять настройки и функции PAN-OS. Хотя изменение функций ОС кажется безобидным и незначительным, на самом деле уязвимость является серьезной угрозой, поскольку ее можно использовать для отключения межсетевых экранов и политик контроля доступа VPN.

По словам специалистов Palo Alto Networks, уязвимость можно проэксплуатировать, только если отключена опция Validate Identity Provider Certificate и используется язык разметки SAML.

По умолчанию опция Validate Identity Provider Certificate включена, а SAML отключен, поэтому, если настройки не были изменены вручную, злоумышленники не смогут воспользоваться уязвимостью. Тем не менее, в некоторых инструкциях производитель сам рекомендует отключить опцию и включить SAML, если на устройстве используются сторонние провайдеры идентификации.

Проблема затрагивает следующие устройства Palo Alto Networks:

GlobalProtect Gateway;

GlobalProtect Portal;

GlobalProtect Clientless VPN;

Authentication and Captive Portal;

Межсетевые экраны следующего поколения PA-Series и VM-Series, web-интерфейсы Panorama;

Системы Prisma Access».

(В PAN-OS исправлена чрезвычайно опасная уязвимость // SecurityLab.ru (https://www.securitylab.ru/news/509569.php). 30.06.2020).

****

«В конце мая 2020 года ИБ-эксперты и журналисты Bleeping Computer обнаружили, что сайт ebay.com сканирует локальные порты посетителей в поисках приложений для удаленной поддержки и удаленного доступа. Многие из этих портов были связаны с такими инструментами, как Windows Remote Desktop, VNC, TeamViewer, Ammy Admin и так далее.

Как оказалось, аукцион использовал для этого скрипт ThreatMetrix, созданный компанией LexisNexis и применяемый для обнаружения мошенников. Хотя eBay, по сути, ищет известные и легитимные программы для удаленного доступа и администрирования, в прошлом некоторые из них действительно использовались в качестве RAT в фишинговых кампаниях.

Сканирование выполняется с использованием WebSockets для подключения к 127.0.0.1. Все 14 сканируемых портов и связанные с ними программы перечислены в таблице ниже. Журналисты Bleeping Computer так и не смогли определить программу на порту 63333. Основываясь на идентификаторе «REF» они предполагают, что это контрольный порт для тестов.

Чтобы узнать, какие еще сайты могут использовать этот скрипт, Bleeping Computer обратился за помощью к специалистам ИБ-компании DomainTools. Компания помогла изданию составить список из 387 аналогичных уникальных хостов на online-metrix.net. В частности, оказалось, что компьютеры пользователей сканируют скрипты на сайтах Citibank, TD Bank, Ameriprise, Chick-fil-A, Lendup, BeachBody, Equifax IQ connect, TIAA-CREF, Sky, GumTree и WePay.

Тогда журналисты протестировали несколько способов избавиться от такого наблюдения. Оказалось, что блокировщик рекламы uBlock Origin в браузере Firefox оказался способен заблокировать работу скрипта ThreatMetrix. Увы, но во время прочих тестов uBlock Origin не смог блокировать сканирование ни в новом Microsoft Edge, ни в Google Chrome.

Однако позже многие читатели сообщили, что uBlock Origin для Chrome все же смог заблокировать сканирование портов на eBay, и тогда журналисты связались с разработчиком блокировщика Раймондом Хиллом и спросили, не вносил ли тот какие-то изменения в код своего продукта. Теперь издание пишет, что создатель uBlock Origin ответил, что ничего не менялось, и предположил, что сайты могли сами отказаться от использования ThreatMetrix.

Хилл предложил журналистам использовать логи uBlock Origin, чтобы обнаружить правила, блокирующие скрип для сканирования портов. Таким образом удалось понять, что изначально eBay сканировал порты посетителей при посещении домашней страницы и прочих страниц сайта. Но теперь аукцион принес функцию сканирования портов на страницы оформления заказа.

Посмотрев логи после посещения страницы оформления заказа, исследователи увидели, что список фильтров EasyPrivacy блокирует скрипт-сканер, расположенный по адресу src.ebay-us.com/fp/check.js.

Изучение различных коммитов для списка EasyPrivacy, помогло понять, что скрипт для сканирования портов на eBay блокирует недавно добавленное правило.

Как показало изучение других сайтов, скрипт для сканирования портов блокировался фильтром, предназначенным для скрипта /fp/tags.js?, который использовался для запуска скрипта-сканера.

В итоге, благодаря новому фильтру, теперь EasyPrivacy блокирует сканирование портов на eBay, Ameriprise, Citi, TD Bank, Lendup, BeachBody, Equifax IQ Connect и Sky. К сожалению, правил для TIAA.org, Chick-Fil-A, Gumtree и WePay пока нет, и эти сайты по-прежнему изучают порты посетителей, даже если те используют расширение uBlock Origin.

Журналисты Bleeping Computer предприняли попытку связаться с операторами EasyList, однако пока не получили ответа». ***(Мария Нефёдова. Теперь uBlock Origin блокирует сканирование портов для большинства сайтов // Xakep (https://xakep.ru/2020/06/09/ublock-origin-vs-threatmetrix/). 09.06.2020).***

***

«Компания Google добавила в опцию Safety check своего браузера Chrome новый инструмент Chrome Cleanup, позволяющий выявлять и удалить потенциально нежелательное ПО.

Изначально Google представила инструмент Software Removal (нынешнее название Chrome Cleanup) как отдельную программу, которую пользователи могли загружать для сканирования ПК, обнаружения потенциально нежелательного ПО и исправления вызванных им проблем с браузером.

Позднее Chrome Cleanup был добавлен в настройки браузера, и теперь его можно найти здесь: Настройки > Дополнительные > Сброс настроек и удаление вредоносного ПО > Удалить вредоносное ПО с компьютера. Далее следует нажать на «Поиск», и инструмент начнет сканировать компьютер на предмет ПО, которое может причинить ему вред.

Перед началом сканирования рекомендуется снять галочку возле опции, позволяющей инструменту отправлять Google данные как об обнаруженных в ходе сканирования программах, так и сведения о системе.

Недавно Google добавила Safety check в обновленные настройки конфиденциальности и безопасности Chrome. Этот инструмент сканирует пароли, расширения, технологию безопасного просмотра и статус обновления браузера. Теперь Google добавила в него Chrome Cleanup». ***(Chrome теперь позволяет находить потенциально нежелательное ПО // SecurityLab.ru (https://www.securitylab.ru/news/509006.php). 08.06.2020).***

***

«Стартап з Нової Зеландії PRAAS створив новий сервіс, який буде стежити за тим, що друкують будинку співробітники на віддаленій роботі. Це допоможе запобігти витоку конфіденційної корпоративної інформації.

За словами творців, сервіс буде сумісний з принтерами будь-якого виробника і моделі. Якщо співробітник на віддаленій роботі почне щось роздруковувати, відділ безпеки компанії отримає копію документа.

У PRAAS пояснили, що через пандемію COVID-19 питання кібербезпеки стало гострішим. Працівники розумової праці, швидше за все, не повернуться в офіси найближчим часом, а відстежувати друк вдома у керівників можливості не було. За даними аналітиків, 84% IT-директорів вже поскаржилися на те, що через віддалену роботи їм стало складніше відстежувати витоки даних». ***(Лужна Софія. Новий сервіс буде стежити за тим, що друкують вдома співробітники на віддаленій роботі // TechnoPortal.com.ua (https://technoportal.com.ua/technology/51602). 20.06.2020).***

***

«Компания Check Point Software Technologies представила полностью автоматизированную облачную платформу – Cloudguard Cloud Native Security. Данная платформа обеспечивает безопасность развертываний в облаке и защиту рабочих нагрузок, а также позволяет заказчикам управлять системой безопасности с помощью единой панели. Cloudguard упрощает облачную безопасность и позволяет предотвратить ведущие кибератаки шестого поколения.

Согласно исследованию SANS 2020 Cybersecurity Spending Survey, быстрая миграция в облако является основным источником сбоев в архитектуре корпоративной безопасности. Больше половины респондентов отмечают в качестве основной причины нарушения безопасности использование публичных облаков. Из-за пандемии и массового перехода на удаленную работу проблема лишь усложнилась. Текущие средства управления безопасностью компаний не справляются со скоростью, масштабом и сложностью развертываний в облаке, что делает компании уязвимыми для атак.

«По данным IDC, более 80% организаций имеют несколько поставщиков облачных услуг, что делает обеспечение безопасности мультиоблачных системах сложной задачей. Поэтому основная цель – это установление единой политики управления для всех поставщиков, – отметил Фрэнк Диксон (Frank Dickson), вице-президент по безопасности и доверию в IDC. – Платформа безопасности Check Point направлена на объединение политик безопасности между частными и публичными облаками».

Check Point Cloudguard решает вопрос защиты мультиоблачных систем, предоставляя наиболее полную и простую в управлении платформу облачной безопасности. Решение обеспечивает беспрепятственное развертывание и управление средствами защиты в любой облачной среды и рабочих нагрузок, а также позволяет автоматизировать процессы безопасности для удовлетворения требований DevOps.

«Проблема безопасности часто становится преградой для развертывания корпоративных облачных систем, поскольку традиционные средства защиты недостаточно гибки, чтобы справиться со скоростью и масштабом облака, – отметил Итай Гринберг (Itai Greenberg), вице-президент по управлению продуктами Check Point. – Cloudguard – это ведущее решение, которое обеспечивает безопасность облачных систем заказчиков, а автоматизированное управление, комплексный мониторинг и политики безопасности делают его удобным в использовании».

Особенности Cloudguard Cloud Native Security: интегрированная система безопасности и предотвращения угроз. Платформа защищает облако и рабочие нагрузки от APT и атак нулевого дня благодаря унифицированной безопасности, включающей брандмауэр, IPS, управление приложениями, IPSec VPN, антивирус и анти-бот, работающий на основе ведущей в отрасли системы обнаружения угроз в реальном времени; управление безопасностью облачной среды. Cloudguard обеспечивает представление данных о сразу нескольких облачных средах компании в едином месте, обеспечивая непрерывный анализ и контроль их безопасности от CI/CD до производственных сред; автоматизация защиты для любой рабочей нагрузки в любом облаке. Cloudguard обеспечивает безопасность независимо от облачной среды развертывания, позволяя организациям защищать любую рабочую нагрузку в любом месте с помощью автоматической подготовки, масштабирования и обновления политик безопасности. Технология обеспечивает комплексное управление безопасностью из единой точки, а также защиту бессерверных и контейнерных приложений в мультиоблачных средах». **(Check Point представила платформу для защиты мультиоблачных сред и рабочих загрузок // Компьютерное Обозрение (https://ko.com.ua/check_point_predstavila_platformu_dlya_zashhity_multioblachnyh_sred_i_rabochih_nagruzok_133404). 16.06.2020).**

***

«Разработчики Instagram работают над внедрением новых функций по борьбе с фейковыми учетными записями и «троллями» в приложении. По словам исследователя Алессандро Палуцци (Alessandro Paluzzi), обнаружившего новые функции в программе, для подтверждения своей личности пользователям социальной сети с большим количеством подписчиков необходимо будет предоставить официальный документ, удостоверяющий личность.

Пользователи должны будут загрузить изображение своего удостоверения личности, выданного правительством, указать свои настоящее имя в приложении, а также загрузить свои данные о местоположении и предоставить селфи-видео. Предоставленные пользователями данные будут затем проверены реальными людьми.

Как отметил исследователь, проверка личности поможет защитить сообщество и поможет убедиться в том, что контент, который пользователи видят в приложении Instagram, является подлинным и создан с настоящих учетных записей. Для данной процедуры можно будет использовать паспорт, водительские права или любой другой документ, подтверждающий личность пользователя.

Таким образом Instagram сможет идентифицировать и удалять учетные записи злоумышленников со своей платформы. Некоторые пользователи могут быть обеспокоены своей безопасностью и конфиденциальностью, однако представители компании Facebook, владеющей Instagram, пообещали, что предоставленный идентификатор никогда не будет опубликован на платформе. Кроме того, загруженные пользователями документы будут удаляться в течение тридцати дней». ***(Instagram введет новые методы борьбы с фейковыми учетным***

записями // SecurityLab.ru (https://www.securitylab.ru/news/509425.php). 23.06.2020).

***

«После того, как компания Apple объявила об увеличении защиты пользовательской конфиденциальности как в браузере Safari, так и в программном обеспечении в целом, интернет-издание Wired сделано небольшой обзор этих изменений, а также рассказало об улучшениях в браузерах Chrome и Firefox — возможно, IT-гигант вдохновился именно их опытом, когда задумался о нововведениях в своём браузере.

Apple раскрыла, какие изменения придут вместе с новой операционной системой macOS Big Sur в этом году. Наряду с визуальным редизайном, внедрением Центра управления и обновлением сообщений, встроенный в систему браузер Safari получает новые и улучшенные функции конфиденциальности для сохранности ваших данных.

Однако не обязательно ждать macOS Big Sur, чтобы получить эти функции в Safari: Mozilla Firefox и Google Chrome имеют аналогичные функции или могут получить их при помощи стороннего расширения..

Изменения в Safari

Приватность и защита данных уже являются большими приоритетами для Safari, но версия в macOS Big Sur пошла ещё дальше, чтобы защитить вас от слежки в интернете. Некоторые из существующих функций становятся всё более заметными, Safari также включает в себя всё больше расширений, заботясь о безопасности пользователей настолько, насколько может.

Браузер уже предупреждает вас об использовании паролей, которые легко угадываются или которые вы использовали раньше (предполагая, что они сохранены в менеджере паролей Safari). Следующая же версия скажет вам, были ли ваши адрес электронной почты, имя пользователя или пароль скомпрометированы, а, следовательно, имеет смысл срочно принять меры и изменить пароль.

Новая кнопка отчета о конфиденциальности добавляется на панель инструментов — вы можете нажать на нее, чтобы увидеть, какие именно трекеры Safari блокирует, постоянно пытаясь помешать рекламодателям и компаниям следить за вами в интернете. Safari особенно хорошо противодействует созданию «отпечатков пальцев», когда различные характеристики вашего устройства, такие как разрешение экрана и операционная система, используются для определения вашей личности.

Этот же отчет о конфиденциальности будет отображаться на начальной странице вашего браузера, что должно лучше показывать вам, какие сайты наиболее агрессивно пытаются отслеживать вас, и демонстрировать работу, которой Safari занят в фоновом режиме. Safari в macOS Big Sur также сильно увеличивает поддержку расширений (Safari уже имеет расширения, но таковых пока очень мало).

Новые инструменты разработчика облегчат перенос дополнений из Chrome и Firefox, а Safari предоставит пользователям набор элементов управления для

ограничения данных браузера и другой информации, к которой расширения могут получить доступ..

Добавленные функции в Chrome

Google уже проверяет пароли, которые он сохраняет для вас, по базе данных утечек учётных данных (помимо предупреждения о дубликатах и паролях, которые можно легко угадать) – в действительности это функция учетной записи Google и Chrome. На панели настроек Chrome нажмите кнопку «Пароли», а затем «Проверка паролей» для запуска проверки.

Вы уже можете получить некоторые данные слежения о сайте, щёлкнув значок слева от URL-адреса в адресной строке Chrome (значок будет в виде либо висячего замка, либо информационного пузыря).

Чтобы получить еще больше данных слежения и выборочно блокировать их в стиле Safari, вы можете использовать расширение типа uBlock Origin: один клик показывает вам — сколько трекеров активны на странице и какие были остановлены uBlock Origin.

Кроме остановки отслеживания на нескольких сайтах, uBlock Origin подавляет агрессивную рекламу и защищает от сайтов со встроенным вредоносным ПО. Аналогичный инструмент для Chrome, который вы можете попробовать, — это Disconnect. Снова один клик блокирует технологии отслеживания, нежелательную рекламу и социальные плагины, подобные используемым Facebook, чтобы увидеть, что вы делаете, когда находитесь вне сети или около неё.

Отдельным трекерам и сайтам в целом может быть предоставлено разрешение на работу без ограничений, введённых uBlock Origin и Disconnect, которое может быть использовано для сайтов с ответственной рекламой, что вы хотите поддержать. В качестве дополнительного бонуса отслеживание и блокировка также должны означать более быстрый опыт просмотра в браузере.

Управление расширениями в Chrome не такое простое, но там есть опции: выбрать «Дополнительные инструменты», затем «Расширения» в меню Chrome, далее — «Детали» рядом с любым расширением. Следующая страница показывает вам разрешения, которые имеет надстройка, и позволяет установить, когда и как утилита может читать ваши данные о просмотре: на всех сайтах (везде, куда вы заходите, без вопросов), на определённых сайтах (только на сайтах, которые вы специально перечисляете) или по клику (разрешение спрашивают всегда, когда требуется доступ)..

Добавленные функции в Firefox

Firefox уже включает в свой интерфейс множество технологий защиты приватности пользователей и защиты от отслеживания, так что вам не нужно прилагать слишком много усилий, чтоб настроить его наравне с улучшениями, которые Apple анонсировала для Safari. Например, он блокирует более двух тысяч веб-трекеров по умолчанию и сигнализирует вам с помощью Firefox Monitor и Firefox Lockwise, когда защита ваших данных нарушена.

Нажмите на маленький фиолетовый значок-щит слева от адресной строки на любом сайте, чтобы увидеть, что Firefox заблокировал, включая рекламные трекеры, плагины социальных сетей, попытки снять отпечатки пальцев с вашего устройства и т.п. Firefox позволит некоторым плагинам работать, если их

блокировка серьёзно нарушит функциональность сайта. Тогда вы сможете выбрать, продолжать использовать сайт или найти ему альтернативу. Чтобы открыть отчет о том, как эти меры работают с течением времени, откройте главное меню Firefox и выберите пункт «Защита конфиденциальности».

Если вы откроете «Персональные настройки», а затем «Конфиденциальность и безопасность» в меню Firefox, вы можете выбрать, как применить меры расширенной защиты от отслеживания.

В доступе три разных режима работы — стандартный, строгий и пользовательский. Также можно настроить уровень блокировки для конкретных сайтов. Расширенная защита от отслеживания может быть отключена и для сайтов, которым вы особенно доверяете. Все эти функции встроены прямо в Firefox, и, возможно, именно там Apple частично получила вдохновение для Safari. Множество сторонних расширений также доступны, если вы хотите пойти ещё дальше.

uBlock Origin и Disconnect доступны как для Firefox, так и для Chrome и работают одинаково: после одного клика на панели инструментов браузера вы можете увидеть, какие объявления и трекеры блокируются.

Для того чтобы следить за тем, какие расширения в Firefox разрешены и для чего, выберите в меню программы «Дополнения», а затем «Расширения». Нажмите на три точки рядом с любым расширением, чтобы увидеть данные и функции браузера, к которым он имеет доступ. Сейчас вы не можете изменить это, хотя способны заблокировать запуск в частных окнах браузера. Если расширение использует разрешение, которое вас не устраивает, вам придётся его удалить». ***(How to Get Safari's New Privacy Features in Chrome and Firefox // Condé Nast. (https://www.wired.com/story/get-safari-new-privacy-features-chrome-firefox/). 28.06.2020).***

***