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

№ 2 (лютий)

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. – №2 (лютий) . – 102с.

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

«Конфликт между новым руководством госпредприятия (ГП) "Информационный центр Министерства юстиции" и компанией-разработчиком программного обеспечения единых и государственных реестров вчера получил продолжение. Сотрудники компании призвали генерального прокурора Виктора Пшонку привлечь представителей ГП к уголовной ответственности за вмешательство в работу реестров. Руководство госпредприятия все обвинения отрицает.

Вчера компания "Арт-мастер" — разработчик программного обеспечения единых и государственных реестров — попросила привлечь к уголовной ответственности должностных лиц Министерства юстиции, а также и.о. гендиректора госпредприятия "Информационный центр Министерства юстиции" (ГП "Госинформюст") Леонида Богданова. Соответствующее заявление на имя генерального прокурора Виктора Пшонки подписали более 160 сотрудников компании.

Согласно заявлению, действия чиновников Минюста и главы Госинформюста "привели к остановке 1 октября работы реестров, что указывает на создание реальной угрозы информационной безопасности государства". "Богданов противоправно пошел на нарушение авторских прав "Арт-мастера", с использованием группы подконтрольных ему программистов-хакеров внес изменения в компьютерные программы, с помощью которых обеспечивается функционирование реестров",— говорится в заявлении компании…». ***(Галина Корба. Запрограммированы на ответ. Конфликт с госреестром получил продолжение // СТОПКОР ГО (https://stopcor.org/zaprogrammyrovan%d1%8b-na-otvet-konflykt-s-gosreestrom-poluchyl-prodolzhenye/). 05.02.2020).***

***

«На факультеті історії, політології та національної безпеки Східноєвропейського національного університету імені Лесі Українки розпочалося навчання у рамках проекту "Інформаційна безпека" від Луцького ІТ-кластеру.

Перша лекція відбулася 5 лютого.

LITaC започатковував новий навчальний проект - "Інформаційна безпека".

В рамках проекту фахівці компаній InternetDevels та ideil., які є засновниками кластеру, проведуть цикл навчальних заходів для студентів спеціальностей "Державна безпека" та "Кібербезпека" на факультеті історії, політології та національної безпеки Східноєвропейського національного університету імені Лесі Українки.

Першу лекцію для студентів прочитав керівник компанії InternetDevels Віктор Левандовський. Спілкувалися про шкідливе програмне забезпечення, можливі ризики та способи їх уникнення». ***(Луцькі айтішники вчать майбутніх спеців з кібербезпеки і держбезпеки // Вісник (https://visnyk.lutsk.ua/news/ukraine/regions/volyn/47451-lutski-aytishniki-vchat-maybutnikh-spyetsiv-z-kibyerbyezpyeki-i-dyerzhbyezpyeki/). 09.02.2020).***

***

«На Запорізькій АЕС відбулося чергове засідання ради з управління позитивними практиками, яка була створена з метою підвищення рівня культури безпеки на станції. Очолив захід генеральний директор ВП «Запорізька АЕС» Петро Котін.

На нараді розглянули питання кібербезпеки та інформаційної безпеки. Після обговорювань було прийняте рішення створити групи реагування з кібербезпеки — це команди фахівців, які будуть оперативно реагувати на кіберінциденти, проводити тренування і навчання персоналу з комп'ютерної безпеки. Також вирішили включити тренування з кібербезпеки в загальну систему тренувань на атомній станції, а при прийомі на роботу проводити спеціальний інструктаж з тематики інформаційної безпеки та зробити його регулярним…». ***(На Запорізькій АЕС відбулося засідання ради з управління позитивними практиками // МОЙ НИКОПОЛЬ.ОНЛАЙН (https://moi-nikopol.online/news/nikopol/32740-na-zaporizkij-aes-vidbulosja-zasidannja-radi-z-upravlinnja-pozitivnimi-praktikami/). 04.02.2020).***

***

«В рамках мероприятия состоялась пресс-конференция «Украина-Европа-Мир: кибербезопасность в 2019 и прогноз на 2020 от McAfee». Некоторые наиболее важные, по нашему мнению, тезисы ниже.

Вызовы

На современных вызовах в области информационной безопасности, которые поджидают компании в их работе остановился вице-президент McAfee в регионе EMEA Кевин О'Двайер.

В настоящее время все больше компаний переносят вычисления и обработку данных в облака. Но многие из них так и не задумываются над новыми видами угроз, которые возникают в результате этого.

Корпоративные пользователи и организации зачастую не осознают, что они уже работают в облаке и что часть их ресурсов также находится в облаке.

В этой связи одной из важнейших задач – возможность интеграции решений от различных производителей (в том числе конкурентов) и создание адаптивной архитектуры системы ИБ, которая должна позволить прогнозировать и бороться с новыми угрозами. В том числе, связанными с массовым переходом бизнес-процессов в облака.

Кевин О'Двайер, вице-президент McAfee в регионе EMEA: «В настоящее время все больше компаний переносят вычисления и обработку данных в облака. Но многие из них так и не задумываются над новыми видами угроз, которые возникают в результате этого»

Новые направления угроз

Одной из главных проблем для информбезопасности является то, что атаки постоянно меняются. Как технологически так и организационно. Например, стало обычным фактом. Когда обнаруженная уязвимость в информационной системе или ПО одной компанией злоумышленников используется другой для проникновения. Продажа уязвимостей стала товаром, который можно купить и продать.

Иван Яковлев, инженер McAfee: «Поскольку количество и разновидности угроз все время возрастают, то критически важным является анализ существующих и прогнозирование появления новых угроз, которые в данное время даже не актуальны». Здесь на первый план выходит использование технологий искусственного интеллекта.

Айзада Кидирбекова, территориальный менеджер по работе с партнерами McAfee «В 2021 году на 1 млн вакансий найдется 170 тысяч специалистов по ИБ. Решение – внедрение средств автоматизации в корпоративные системы ИБ»

Прогнозы экспертов

Территориальный менеджер по работе с партнерами McAfee Айзада Кидирбекова отметила тренды в области кибербезопасности, которые рассматривают аналитики компании как основные:

все решения ИБ должны интегрироваться друг с другом;

появились новые виды угроз, связанные с появлением облачных технологий;

дефицит кадров (в 2021 году на 1 млн вакансий найдется 170 тысяч специалистов по ИБ)

Иван Яковлев, инженер McAfee: «Поскольку количество и разновидности угроз все время возрастают, то критически важным является анализ существующих и прогнозирование появления новых угроз, которые в данное время даже не актуальны»

Защита критических инфраструктур

Евгений Бадах, генеральный директор группы компаний Бакотек: «На сегодня защитой промышленных систем автоматизации (SCADA) и ИТ-систем на предприятиях занимаются различные компании-разработчики. Ведь сегодня нет ни одного производителя, который выпускает полный спектр решений. Поэтому вопрос создания общей системы безопасности предприятия достаточно сложен и решается интеграцией усилий нескольких поставщиков». Кевин О'Двайер: «Не забывайте. Что в подобных проектах присутствуют всегда три важные составляющие – процессы, технологии, люди».

Решение существующих проблем видится в создании средств автоматизации и построении в рамках корпораций и организаций единых центров управления безопасностью (Security Operation Center, SOC), которые смогут помочь управлять всеми операциями кибербезопасности: от конечных устройств до облаков. Это касается как корпораций так и предприятий критической инфраструктуры.

Евгений Бадах, генеральный директор группы компаний Бакотек: «На сегодня защитой промышленных систем автоматизации (SCADA) и ИТ-систем на предприятиях занимаются различные компании-разработчики. Ведь сегодня нет ни одного производителя, который выпускает полный спектр решений. Поэтому вопрос создания общей системы безопасности предприятия достаточно сложен и решается интеграцией усилий нескольких поставщиков» ***(McAfee Cybersecurity Forum. Интеграция и адаптивная архітектура // hi-Tech PRO (https://hi-tech.ua/mcafee-cybersecurity-forum-integracziya-i-adaptivnaya-arhitektura/). 10.02.2020).***

***

«6 февраля президент и премьер презентовали приложение государственных онлайн-услуг «Дія». Однако, как пишет на своей странице в Facebook вице-премьер и министр цифровой трансформации Украины Михаил Федоров, у пользователей приложения возникло множество вопросов относительно безопасности предложения и защиты персональных данных…

Создавать приложение «»Дія»» помогали 35 специалистов-волонтеров от крупнейшей в Украине аутсорсинговой ИТ-компании EPAM Systems. Они уделили особое внимание защите персональных данных.

«Авторизация осуществляется через BankID, само приложение построено в соответствии с лучшими практиками индустрии, все данные передаются и хранятся на смартфоне пользователя исключительно в зашифрованном виде, усиленная процедура аутентификации между приложением и сервером», — рассказывают в EPAM Systems.

«Следует отметить, что данные пользователей не сохраняются на сторонних хранилищах, а передаются транзитом через защищенный облачный сервер», — добавляют в компании.

Серверы EPAM для работы «Дія» не используются. Для выявленных потенциальных уязвимостей мобильное приложение и его серверная часть прошли несколько этапов проверок, в том числе тест на проникновение. Среди 35 волонтеров компании были архитекторы, инженеры, тестировщики, аналитики, специалисты по кибербезопасности. С каждым волонтером было подписано соглашение о неразглашении информации.

Вице-премьер и министр цифровой трансформации Украины Михаил Федоров на своей странице в Facebook сообщил:

«Почти 800 тысяч украинцев загрузили «Дію» за 2 суток, успешно авторизованных — 667 тысяч. Готовимся к первому миллиону». ***(О защите персональных данных в приложении «Дія» // ОБЩЕСТВЕННЫЙ ПРИБОЙ (https://www.priboi.news/obshchestvenno-vazhnoe/o-zashhite-personalnyx-dannyx-v-prilozhenii-diya/). 09.02.2020).***

***

«Україна посіла 12 місце в рейтингу країн, які найбільше вразливі до ботнетів — комп'ютерних мереж, які заражені шкідливим програмним забезпеченням.

Про це йдеться в дослідженні компанії IBM, яка є одним з найбільших у світі виробників і постачальників апаратного і програмного забезпечення, а також IT-серверів і консалтингових послуг.

Всього дослідники виділили 20 країн, які найбільше страждають від ботнетів. На першому місці опинилися США. Далі в списку йдуть Індія, Індонезія, Росія і Китай.

Відзначається, що країни з великою кількістю населення частіше стають жертвами ботнетів.

Також в досліджені зазначається, що у 2019 році в інтернеті викрали понад 8,5 млрд записів, що на 200% більше, ніж у 2018 році. 60% проникнень здійснювалось за допомогою раніше викрадених облікових даних та через відомі

вразливі місця в програмному забезпеченні, яких наразі є понад 150 тисяч…». ***(Борис Ткачук. Україна потрапила в топ-20 країн, які найбільше вразливі до ботнетів — дослідження // Громадське Телебачення (https://hromadske.ua/posts/ukrayina-potrapila-v-top-20-krayin-yaki-najbilshe-vrazlivi-do-botnetiv-doslidzhennya). 13.02.2020).***

***

«Міністерство освіти та науки України поступово впроваджуватиме єдиний державний кваліфікаційний іспит для здобуття ступеня бакалавра. Проєкт зараз доступний для громадського обговорення. У відомстві пропонують також розширити список спеціальностей, за якими проводиться державний іспит для здобуття ступеня бакалавра.

Якщо проєкт буде ухвалений, то єдиний державний іспит буде впроваджений для випускників освітнього рівня бакалавр за такими спеціальностями:

кібербезпека; атомна енергетика; медсестринство; технології медичної діагностики та лікування; державна безпека; безпека державного кордону; військове управління; забезпечення військ; озброєння та військова техніка; пожежна безпека; правоохоронна діяльність; цивільна безпека; річковий та морський транспорт; залізничний транспорт; автомобільний транспорт.

Для випускників з магістратури:

право; ветеринарна медицина; ветеринарна гігієна; санітарія і експертиза; стоматологія; медицина; медична психологія; фармація; промислова фармація; фізична терапія; ерготерапія; педіатрія; авіаційний транспорт; транспортні технології; публічне управління та адміністрування; міжнародне право.

Для вступників на магістратуру додатково необхідно скласти єдиний державний кваліфікаційний іспит за результатами здобуття ступеня бакалавра.

Додаткові іспити запроваджуються для того, щоб виміряти якість здобутих знань за результатами навчання в університеті.

Впровадження такої ініціативи робитиметься поступово. Спочатку іспити складатимуть випускники найбільш суспільно важливих та пов'язаних з ризиком спеціальностей». ***(Алла Широкова. Міносвіти планує запровадити додаткові іспити в університетах // 0532.ua - Сайт міста Полтави (https://www.0532.ua/news/2660619/minosviti-planue-zaprovaditi-dodatkovi-ispiti-v-universitetah). 13.02.2020).***

***

«Фахівець Запорізької АЕС Євген Калініченко виграв міжнародні змагання МАГАТЕ на написання найкращого есе на тему фізичної ядерної безпеки для студентів і молодих професіоналів.

Вручення сертифікатів про перемогу трьом фіналістам відбулося на конференції МАГАТЕ ICONS 2020, яка проходить у Відні, повідомляє Укрінформ.

Конкурс проводився у співпраці з Міжнародною освітньою мережею МАГАТЕ з фізичної ядерної безпеки.

Назва роботи Калініченка – "Поява технологічних загроз, а також можливостей у галузі фізичної ядерної безпеки в цифровий вік".

"У моїй роботі висвітлюються потенційні загрози для фізичної ядерної безпеки від кібератак і безпілотних літальних апаратів. В есе я розглянув варіанти протидії цим загрозам, а також можливості технологій штучного інтелекту і безпілотних систем для укріплення фізичної безпеки ядерних установок і матеріалів", - зазначив у коментарі Укрінформу Євген Калініченко.

За його словами, роботою зацікавилися в МАГАТЕ, і вона буде включена у протокол конференції ICONS 2020.

"Результати цієї конференції будуть використовуватись при розробці плану МАГАТЕ з ядерної безпеки на 2022-2025 роки", - додав Калініченко». ***(Українець виграв міжнародні змагання МАГАТЕ на написання найкращого есе // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/140220-ukrayinec-vygrav-mizhnarodni-zmagannya-magate-na-napysannya-naykrashchogo-ese). 14.02.2020).***

***

«Группа украинских хакеров «КиберХунта», известная своими операциями против российского руководства (именно они обнародовали переписку бывшего советника президента РФ В. Суркова с его помощником Карповым), завершила свою деятельность. Об этом на своей странице в Facebook написал спикер «Украинского киберальянса», известный в сети под ником Шон Таунсенд.

Волонтерское движение «Украинский киберальянс» было создано с целью противодействия российской пропаганде. В него вошли такие хакерские команды как «Falcons Fame», «Trinity», «ruh8» и «Киберхунта». Всех их объединила идея борьбы с Россией в киберпространстве (они взламывали аккаунты боевиков ЛДНР, сайты «Анна Ньюз» и «Первого канала», а также сайт Министерства обороны РФ). Они утверждают, что действуют в рамках украинского законодательства (17 статьи КУ) и потому обязаны обеспечивать информационную безопасность государства Украина. Полученную в ходе «взлома» информацию хакеры передают СБУ и Минобороны.

Шон Таунсенд не назвал причину закрытия сайта #CyberHunta, а лишь поблагодарил хакеров за их вклад в работу.

Сим официально всех уведомляю, что группа #CyberHunta завершила свою деятельность. Любые новые заявления от их имени - ложь и подделка. Хоть их сайт и выключен, тем не менее многие их разработки продолжают работать прямо сейчас. Хороший взлом никогда не заканчивается. Мы в Ukrainian Cyber Alliance благодарны нашим коллегам за все замечательные акции, и уверяем, что мы останавливаться не собираемся.

Подумайте сами, может ли здравомыслящий человек рассчитывать на то, что с бандитской федерацией можно договориться? Забордюрные раки никогда не были договороспособными. Их устраивает только "мир" на их условиях https://bit.ly/39LZqOM. "русский мир" в котором нет места свободе и достоинству, и сегодня они подтвердили сию нехитрую мысль в очередной раз.

Должны ли мы бояться россиян, испытывать так называемую "русофобию"? Ни в коем случае. Не нужно бояться врага, как бы отвратителен он ни был в своих

противоестественных устремлениях. И уж тем более стремиться к миру на их условиях? Никогда. У нас есть что противопоставить одичалым. Просто так случается, что секретная информация появляется в прессе, агентов с фальшивыми документами задерживают пограничники. Ломаются компьютеры и пропадает связь.

На России две беды, третьей будешь?

Если вы можете помочь в развале, разломе, гниении и разложении Российской Федерации и готовы к взаимодействию, пишите. У нас есть цель - победа в войне. Нам нужна победа, а не позорный мир. Сразу предупреждаю, что мы не говорим, что кому делать и не занимаемся обучением. Готов?, - написал он на своей странице Facebook». ***(Элина Сулима. Что на самом деле случилось с «КиберХунтой» // InternetUA (https://internetua.com/csto-na-samom-dele-slucsilos-s-kiberhuntoi-). 19.02.2020).***

***

«Колишній співробітник СБУ, а нині засновник компанії ProtectMaster звернув уваги на проблеми із захищеністю державних структур від кібератак та інших сторонніх втручань.

Днями у виданні Liga.Tech вийшло велике інтерв'ю із Микитою Книшем — фахівцем із кібербезпеки. Він працював в СБУ у «спекотний» час — 2014-2015 роках, коли Росія активно розгортала проти України збройну та інформаційну агресію. Спочатку ІТ-фахівець був задіяний у роботу контррозвідки з інформаційної безпеки в центральному апараті СБУ. Потім на інших посадах в Харкові і зоні АТО.

Про вірус Petya та захист держструктур

Фахівець поділися думками про те, наскільки захищеними від вірусів та кібератак зараз є державні установи в Україні.

На його думку, в держсекторі не зробили жодних висновків після кібератак та після поширення вірусу Petya. Водночас трохи покращилася безпека в комерційному секторі, каже він.

«Чи захищена Адміністрація президента, Кабмін або НБУ, якщо там Гончарука прослуховують? Ще питання є? Чи захищені нардепи, якщо Джокер їх листування зливає? Чи працює Держспецзв'язку, якщо все в Telegram або Signal спілкуються? Ви уявляєте собі, наприклад, при Кучмі ситуацію, коли хтось зливає інформацію з закритої наради прем'єра, а генерал СБУ або генерал МВС після цього не йде у відставку?», — зауважує Микита Книш.

ІТ-фахівець вважає, що людина, яка відповідає за забезпечення безпеки Офісу Президента, Кабміну, має бути звільнена наступного ж дня.

«Якби це був я, я б згорів від сорому», — додає він.

Про заборону російських соцмереж

Микита Книш є активним прихильником продовження блокування російських соцмереж в Україні. Також він вважає, що треба блокувати й російські та проросійські телеканали, доки Росія не віддасть Україні захоплених нею територій. У інтерв'ю він нагадав, що виступав за заборону російських соцмереж та сервісів ще з самого початку війни на Донбасі.

«Військові на "передку" орієнтувалися по Яндекс Навігатору. Зрозуміло, що до них "прилітало" тільки через те, що вони його використовували. Військові завантажували фотки з геоданих, кидали фотографії своїм близьким і так далі. Реально це був дуже потрібний і важливий крок», — пояснює Микита Книш необхідність заборони російських сервісів та соцмереж…». ***(ІТ-фахівець: «Чи захищений Кабмін, якщо там Гончарука прослуховують?» // MediaSapiens (https://ms.detector.media/kiberbezpeka/post/24227/2020-02-19-it-fakhivets-chi-zakhishchenii-kabmin-yakshcho-tam-goncharuka-proslukhovuyut/). 19.02.2020).***

***

«Украинский киберальянс», к членам которого в 25 февраля пришли сотрудники полиции и СБУ, отказывается сотрудничать с украинским властями. Помощь государственным органам в сфере кибербезопасности может быть возобновлена только после закрытия уголовных производств и принесения извинений. Такую позицию представители УКА озвучили на пресс-конференции в Киеве в среду, 26 февраля.

В организации считают необоснованными обыски, которые у киберэкспертов провели в рамках расследования дела о взломе табло в Одесском аэропорту.

"Нас обвиняют как группу людей. То есть, мы сидели все за клавиатурой и писали сообщение", - заявил эксперт УКА Андрей Перевезий.

На пресс-конференции напомнили, что эксперт по кибербезопасности Александр Галущенко, к которому приходили с обыском во вторник, еще год назад передал Службе безопасности Украины информацию об уязвимости ресурсов Одесского аэропорта. Он также общался на эту тему с руководством аэропорта. В УКА пояснили, что СБУ не может в приказном порядке заставить руководство предприятия "залатать дыры" в системе безопасности, так как этот объект не является государственным.

"Вчера было очень острое желание передать все найденные уязвимости в международную систему безопасности полетов. Результат у этого был один единственный – одесскому аэропорту бы запретили принимать международные рейсы... Но тогда бы пострадали простые одесситы. Потому что те, кто заказали обыски – умеют сами летать. На чартерах", - отметил Перевезий.

Он также заявил, что если бы хакеры сообщали обо всех уязвимостях сразу в международные институты, а не украинским властям, то Евросоюз мог бы лишить Украину безвизового режима.

Киберэксперты также выразили возмущение в связи с тем, что правоохранители в ходе обысков изымали у них технику, включая Wi-Fi роутеры. Хотя закон обязывает их не изымать носители информации, а копировать. Следователь пояснил отказ от копирования отсутствием носителя необходимой емкости.

Представители УКА также рассказали, что перед обыском у них отключился беспроводной интернет и перестали работать мобильные телефоны. В то время, как телефон следователя работал. Это может свидетельствовать об использовании правоохранителями средств радиоэлектронной борьбы.

Киберэксперты также заверили своих информаторов, что киберполиция и СБУ не смогут взломать зашифрованную информацию. А также допустили, что именно эти данные, а не расследование инцидента в Одесском аэропорту, стали истинной причиной обысков у активистов «Украинского киберальянса». ***(Хакеры из Украинского киберальянса отказались сотрудничать с властями из-за обысков // Зеркало недели. Украина (https://zn.ua/UKRAINE/hakery-iz-ukrainskogo-kiberalyansa-okazalis-sotrudnichat-s-vlastyami-iz-za-obyskov-346316_.html). 26.02.2020).***

***

«За останні роки кібербезпека стала однією з ключових міжнародних тем для обговорення та полем для спільних дій. Від хакерів потерпають окремі компанії та цілі країни, а збитки від кібератак у 2021 році можуть досягти $6 трлн. Цю тему не можуть самостійно вирішити ані найрозвиненіші країни, ані транснаціональні корпорації…

Факти ICTV поговорили із співініціатором та CEO Глобального центру взаємодії в кіберпросторі (GC3) Володимиром Павелком, який розповів:

чому усім гравцям у сфері кібербезпеки необхідно об'єднуватись;

в якому стані перебуває система кібербезпеки в Україні;

навіщо потрібно створювати незалежний кіберцентр.

– Як Ви оцінюєте поточний рівень системи кібербезпеки в Україні?

– Питання кібербезпеки – не нове. У розвинених країнах про неї заговорили наприкінці 90-х минулого століття, тоді як в Україні за її впровадження активно взялись лише шість-сім років тому. За останні п'ять років в Україні ухвалено низку важливих стратегічних документів, визначені відповідальні інституції з боку держави, які мають дбати про безпеку кіберпростору країни.

Зокрема, це СБУ, Нацбанк, Національна поліція, Держслужба спеціального зв'язку, Міноборони, розвідувальні органи України, Мінцифри. Формально створений Національний координаційний центр кібербезпеки у складі РНБО.

Сфера кібербезпеки в Україні перебуває на етапі організаційного дитинства, з усіма відповідними внутрішніми і зовнішніми проблемами та викликами.

Хоча в Україні хороша IT-інфраструктура та програмісти, які розробляють конкурентоздатні IT-рішення, але не вистачає кваліфікованих управлінських рішень щодо стратегії кіберзахисту.

На жаль, Україну розглядають сьогодні як кіберполігон, де випробовуються нові зразки кіберзброї, яку далі розповсюджують на інші країни. Це проблема, але водночас і перевага – у нас хороші спеціалісти, і ми першими стикаємось з кіберзагрозами, тому маємо найновішу інформацію.

У питанні кіберзахисту нам не вистачає системного мислення та дієвої співпраці. У нас недостатня інтеграція між державними інституціями, на початковому етапі співпраця між державою і бізнесом, ще гірша ситуація в освітній сфері.

– Чи може Україна самостійно вирішити власні проблеми в сфері кіберзахисту?

– Кіберзлочини сьогодні не мають національних кордонів, а захист від них потрібен на всіх рівнях. Ще кілька років тому кількість підключених до інтернету пристроїв у світі оцінювалась на рівні 8,4 млрд. Сьогодні ця цифра може сягати 20 млрд.

На жаль, всі ми поки досить несвідомо пов'язуємо свої електронні пристрої з глобальною мережею і віддаємо велику кількість персональної інформації. А це іміджеві, операційні та фінансові ризики.

Після масштабних кібератак, на кшталт WannaCry та Petya, які нанесли мільярдні збитки, важливість кібербезпеки в України та світі набула виняткового значення. Але проблему кіберзлочинів не в змозі вирішити самостійно жодна країна чи велика компанія.

Найскладніше малому та середньому бізнесу, адже для надійного захисту потрібні великі кошти – створення ефективних систем кіберзахисту можуть собі дозволити лише великі корпорації. Та навіть це не допоможе їм бути повністю захищеними, адже вони убезпечують тільки свій периметр.

Провідні країни вже давно зрозуміли, незважаючи на те, що у них потужні економіки, великі інтелектуальні та організаційні ресурси, вони не можуть діяти у питаннях кібербезпеки самостійно. Світ стає більш глобальним. Кіберсередовище та кіберзлочини не мають національних кордонів. Ми перебуваємо в Україні, а наші дані знаходяться на серверах на інших континентах.

Україна може ефективно стежити за IT-інфраструктурою, дата-центрами, хостингами в межах власної території, але це не дозволить нам почувати себе у безпеці.

– На Вашу думку, якою має бути модель впровадження системи кібербезпеки в Україні? Які приклади є у світовому досвіді?

– Для ефективної протидії кіберзагрозам дуже важливо створювати незалежні платформи для взаємодії – кіберцентри.

Це інтеграційні платформи для світових та національних кібергравців, де вони можуть обмінюватись своїми напрацюваннями у сфері кібербезпеки. Таким чином Україна зможе швидко реагувати на кіберзагрози.

Наприклад, кіберцентр у Пітсбурзі, США працює вже 18 років, об'єднуючи представників правоохоронних органів, державних інституцій, IT-компаній, навчальних закладів задля цілей кіберзахисту. Такі центри діють у багатьох розвинених країнах. В Україні ж поки немає жодного. Створення першого кіберцентру буде обговорюватись під час конференції 19 березня.

Найцікавішим для України є досвід Естонії, яка єдиною на пострадянському просторі досягла значних успіхів у формуванні системи кіберзахисту.

У 2007 році Естонія стала першою країною НАТО, кіберсередовище якої цілеспрямовано атакували хакери за підтримки іншої держави. Тоді до захисту своєї країни в кіберпросторі долучилися громадяни – кваліфіковані IT-інженери зібрались та почали спільно думати і впроваджувати систему захисту.

Естонці створили такі стандарти кібербезпеки, які потім в секторі безпеки та оборони впровадило НАТО. Сьогодні у світі діє 32 центри, які взяли на озброєння саме естонські стандарти. Зараз в країні з населенням у 1,2 млн осіб діє п'ять кіберцентрів.

Нам цікавий досвід Естонії у багатьох аспектах – ми маємо спільне минуле, вони територіально недалеко від нас, у нас є ті самі зовнішні чинники впливу, які спонукали естонців швидко створювати систему кіберзахисту.

Кіберцентр, який ми зараз створюємо, буде працювати за моделлю, яка показала себе ефективною у розвинених країнах. Коли ми зможемо об'єднати ключових гравців, то отримаємо унікальний досвід, що дозволить Україні стати одним з найвпливовіших кібергравців світу». ***(Лілія Ященко. Як убезпечити світ від кіберзлочинів та навіщо будувати кіберцентр – Павелко // ФАКТИ. ICTV (https://fakty.com.ua/ua/lifestyle/tehnika/20200228-yak-ubezpechyty-svit-vid-kiberzlochyniv-ta-navishho-buduvaty-kibertsentr-pavelkom/). 28.02.2020).***

***

Правове забезпечення кібербезпеки в Україні

«Парламентарі ухвалили низку проектів постанов щодо проведення парламентських слухань…

…підтримали проект постанови № 2777 про проведення парламентських слухань 15 квітня 2020 року на тему "Кібербезпека, критична інфраструктура, електронні комунікації в Україні: стан, проблеми, шляхи їх вирішення". Відповідне рішення підтримали 342 народних депутатів України…» ***(Антоніна Карташева. Нардепи схвалили проведення низки парламентських слухань // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1850384-nardepi-skhvalili-provedennya-nizki-parlamentskikh-slukhan). 04.02.2020).***

***

Кібервійна проти України

«Спецслужби РФ використовують Україну, як випробувальний майданчик для здійснення кібератак, зокрема це робить російська група кібернетичних операцій Gameredon.

Принаймні так вважають у безпековій компанії SentinelLabs…

"Ми з високою впевненістю припускаємо, що російські атаки та підхід до України — це підготовка, яку застосують для реалізації інших цілей, в інтересах уряду РФ", - заявив голова компанії SentinelLabs Віталій Кремез.

Кремез підготував звіт, щоб висвітлити ескалацію кібершпигунських атак на стратегічні об'єкти в Україні — у галузі безпеки та інших. У звіті SentinelLabs вказується, що група Gameredon вже атакувала 5 тисяч "унікальних об'єктів" в Україні.

Хакери використовують модифіковану шкідливу програму для операційної системи Windows. Програма має на меті збір заволодіння даними, пошук інструкцій для сервера дистанційного керування та контролю…» ***(Росія використовує Україну як випробувальний майданчик для кібератак // iPress (https://ipress.ua/news/rosiya_vykorystovuie_ukrainu_yak_vyprobuvalnyy_maydanchyk_dlya_kiberatak_305930.html). 06.02.2020).***

***

«За последние две недели рост политической напряженности в стране спровоцировал и серьезную активизацию хакерского криминала. С кибератаками столкнулись не только веб-сайты критически настроенных к власти СМИ (в том числе и ZN.UA), но и интернет-ресурсы органов власти. Процесс стал приобретать неадекватные формы. Вопрос информационной безопасности становится все более актуальным для Украины. Под ударом разворачивающейся кибервойны оказывается и банковская система, в которой концентрируются интересы всей экономики.

Масштабы проблемы

Ограбление с помощью компьютера — уже не просто популярный сюжет голливудского фильма, а вполне реальная угроза, с которой сталкиваются финучреждения и их клиенты по всему миру.Согласно оценкам комиссии по внутренним делам британского парламента, потери мировой экономики от преступлений, совершенных с помощью Интернета, достигли 388 млрд долл. в год. Тем самым киберпреступность обошла по своему размаху мировой наркорынок, годовой оборот которого оценивается в 288 млрд долл. Руководитель отдела финансовой стабильности Банка Англии Эндрю Хелдейн заявлял, что пять крупнейших банков Великобритании боятся киберпреступлений даже больше, чем долгового кризиса. По его словам, система защиты от хакерских атак в банковском секторе находится фактически в зачаточном состоянии: раньше финансисты больше заботились о ликвидности, чем о безопасности.

Какова ситуация в Украине? До последнего времени киберпреступность у нас ассоциировалась преимущественно с различными видами махинаций с банковскими картами клиентов-физлиц. Так, преступники с помощью специальных устройств (например, так называемых скиммеров, которые устанавливаются на банкоматах) получали данные клиентов и изготавливали дубликаты карт для дальнейшего снятия денег со счетов. По оценкам НБУ, в прошлом году удельный вес подобных мошенничеств составил 0,002% от общего объема операций с карточками. С этим явлением банки и правоохранители, как они заверяют, в целом уже научились бороться. Об этом свидетельствует в том числе увеличение количества выявленных скиммеров (в текущем году — около 160, в прошлом — 73, в 2011-м — 45).

Но за последние год-два киберпреступники начали менять "профиль" и переходить в "высшую лигу". Они переориентировались в том числе на клиентов-юрлиц (где цена вопроса, понятно, более высокая), что предусматривает вмешательство в системы дистанционного банковского обслуживания (ДБО, например, "клиент—банк" и т.п.). К слову, если в 2010–2011 гг. преступники использовали украинские банки преимущественно как "кассы" для снятия и обналичивания средств, украденных со счетов в иностранных банках, то в 2012-м тенденция изменилась, и начались атаки на клиентские счета именно отечественных финучреждений на территории Украины.

По словам начальника управления по борьбе с киберпреступностью МВД Украины Максима Литвинова, в текущем году уже зафиксировано более 270 попыток несанкционированного списания средств со счетов клиентов банков на общую сумму более 108 млн грн. Статистика примерно такая же, как и в прошлом

году. "Наши механизмы, которые мы наработали совместно с банками и Госфинмониторингом, позволяют предотвратить завладение средствами со стороны преступников в 70% случаев", — подчеркивает страж правопорядка.

Правда, следует иметь в виду, что официальные данные, безусловно, не охватывают все случаи преступлений, поскольку зачастую банки пытаются "урегулировать" проблемы на своем уровне, не предавая их огласке, чтобы избежать репутационных рисков. "Но нельзя сказать, что данные катастрофические. Если бы мы все вместе — НБУ, МВД, НАБУ не уделяли этой проблеме должного внимания, преступности было бы намного больше. Мы все-таки минимизируем это явление", — утверждает руководитель комитета НАБУ по вопросам банковской инфраструктуры и платежных систем, председатель правления банка "Старокиевский" Юрий Яременко.

Как рассказывает руководитель по безопасности технологий розничного бизнеса "Альфа-банка" (Украина) Сергей Досенко, в апреле и октябре текущего года около 30 финучреждений в Украине столкнулись с одновременными мощными DDoS-атаками, целью которых было в том числе прикрытие попыток вывода средств со счетов клиентов. "С точки зрения методов работы и масштаба их можно характеризовать не просто как киберпреступность, но и как кибертерроризм", — говорит специалист.

При этом он уточняет, что в октябре клиенты почувствовали только сложности с доступом к сервисам дистанционного обслуживания, однако финансовых потерь они не понесли (была попытка похищения средств со счета одного клиента). Такой результат удалось получить в том числе благодаря большим инвестициям (на миллионы гривен) в систему информационной безопасности финансового учреждения.

По словам специалистов, устроить DDoS-атаку на десятки банков — не такое уж дешевое "удовольствие". На это может понадобиться даже не одна сотня тысяч гривен. Понятно, что злоумышленники свои "капиталовложения" рассчитывают окупить сторицей.

Хотя иногда имеют место факты, когда продвинутые компьютерщики "просто" решают испытать на прочность IT-системы банков, не ставя себе четкую цель украсть средства с чужих счетов (такой вот профессионально-квалификационный интерес). Кроме того, рассказывают эксперты, иногда IT-шники не до конца осознают ответственность за свои действия, когда к ним обращаются люди с "деликатными" просьбами, полностью не раскрывая своих мотивов.

Кстати, по данным немецкого оператора связи Deutsche Telekom, Украина находится на четвертом месте в мире после России, Тайваня и Германии среди стран, из которых в основном идут кибератаки. Ежемесячно с украинских серверов запускается более полумиллиона вредоносных программ.

Последний яркий пример хакерского криминала — попытка вывесить на сайт НБУ нашумевшее в соцсетях "постановление" регулятора от 2 декабря 2013 г. №6565, в котором говорится в частности об ограничении валютно-обменных операций, движения денег по банковским счетам и т.д. Слово "постановление"

берется в кавычки исходя из того, что в Нацбанке категорически опровергли его существование.

"Хакеры даже поставили номер на сайте НБУ, но само "постановление" разместить не смогли — сработала система защиты. Его писал человек, который явно имеет опыт работы с официальными документами. И если бы это "постановление" попало на сайт НБУ, оно произвело бы эффект разорвавшейся бомбы. Мы должны понимать, что если такие попытки делаются, то они могут быть и успешными", — подчеркивает председатель совета НАБУ Борис Тимонькин.

Слабые звенья

Чьи действия или бездействие в наибольшей степени повышают успешность хакерских атак? Банков, которые экономят на системах защиты, противодействия преступности, или клиентов, которые либо небрежно пользуются финансовыми услугами, либо применяют уязвимое нелицензионное программное обеспечение? "Не могу и не хочу давать оценок, кто виноват. Считаю, что виноваты те, кто хочет завладеть чужими деньгами. Но если говорить о банках, то не знаю примеров, чтобы они пользовались нелицензионными программами", — дипломатично убеждает Ю.Яременко.

Очевидно, что проблемы с обеспечением надлежащего уровня защиты имеют место с обеих сторон. Хотя, по словам представителей госрегулятора и участников рынка, клиентская составляющая все-таки более весомая. "Клиенты не совсем понимают те риски, которые они могут понести, и поэтому не уделяют большего внимания защите своих персональных данных", — говорит специалист департамента платежных систем НБУ Дмитрий Макаренко. "Клиент часто недооценивает, насколько важно соблюдать правила безопасности. Абсолютное большинство взломов там, где нет этой защиты вообще, где пренебрегают условиями по безопасности", — добавляет эксперт проекта НАБУ "Противодействие киберпреступности" Алена Кузьмина.

По словам же первого заместителя руководителя службы безопасности Приватбанка Михаила Фролова, финучреждениям не совсем корректно спрашивать у клиента, у которого украли деньги, — было ли лицензионным программное обеспечение, которое он применял. "Это будет проявлением предвзятого отношения банка к клиенту. Но банк должен научить клиента, как правильно действовать", — отмечает М.Фролов.

Свидетельством того, что и в банках не все так гладко с безопасностью в сфере дистанционного банковского обслуживания, может быть, в частности, недавний случай, когда сотрудники одного из финучреждений скопировали электронные ключи доступа к счетам клиентов и похитили с них несколько миллионов гривен. Правда, представители группы злоумышленников были задержаны, когда пытались с наличными средствами пересечь госграницу Украины.

Вместе с тем директор Украинской межбанковской ассоциации членов платежных систем "ЕМА" Александр Карпов обращает внимание, что сегодня на рынке достаточно лояльные условия с точки зрения возврата средств клиентов, счета которых пострадали от хакеров-грабителей. А также отмечает необходимость

усиления уголовной ответственности киберпреступников за их действия. "Является ли Украина удобным местом для осуществления киберпреступлений? Да. Банальный пример. Вы в банкомате вынули 200 тыс. грн за три минуты, вас, возможно, поймали. Вы отдали 80 тыс. грн штрафа и пошли жульничать дальше. Вот так сейчас выглядит с точки зрения законодательства противодействие кибермошенничеству", — сетует эксперт.

Такое положение дел сформировалось в том числе из-за "гуманизации" статьи 200 Уголовного кодекса. В ее текущей редакции предусмотрено, что подделка документов на перевод, платежных карточек или других средств доступа к банковским счетам, неправомерный выпуск или использование электронных денег и т.д. наказывается штрафом от трех до пяти тысяч необлагаемых минимумов доходов граждан. То есть тюремные нары преступникам именно по этой статье не угрожают.

Отдельное внимание специалисты уделяют качеству работы МВД. С одной стороны, особых претензий непосредственно к профильному управлению по борьбе с киберпреступностью вроде бы и нет. С другой — существуют вопросы к другим структурным подразделениям правоохранительного министерства, которые тем или иным образом также участвуют в противодействии преступлениям (прежде всего, речь идет об органах следствия). Кроме того, в более высоком качественном уровне нуждается и работа судебных органов — их компетенция часто хромает.

Но даже при всех многочисленных нюансах система противодействия киберпреступности работает, утверждают представители правоохранительных органов. "Прошлогодние дела — на завершающей стадии в судах. Преступники получают свои заслуженные сроки лишения свободы", — констатирует М.Литвинов.

Воспитательные моменты

Для предупреждения мошенничеств в системах дистанционного банковского обслуживания специалисты советуют соблюдать, по крайней мере, несколько элементарных правил безопасности. В частности, использовать лицензионное программное обеспечение; не передавать коды доступа другим лицам (в т.ч. сотрудникам банка); не использовать компьютер системы "клиент—банк" для других целей, кроме проведения операций со счетами; не применять системы дистанционного управления компьютером; подписывать платежные документы двумя ключами электронно-цифровой подписи (например, директора и бухгалтера) и т.д.

Но без грамма преувеличения можно утверждать, что киберпреступники используют не только технические огрехи своих потенциальных жертв, но и пробелы в морали и правовой культуре всего общества. Ведь для того, например, чтобы перевести украденные с банковских счетов деньги в наличную форму, они часто обращаются к совершенно посторонним лицам за помощью. Предлагая "комиссию"/откат за их "услуги". И здесь преимущественно вопрос в цене, которая достигает обычно 20–30% суммы махинаций.

"С конца 2012 г. уже зафиксировано 500 контрагентов (из них третья часть — юрлица), которые способствовали отмыванию средств, полученных преступным путем с использованием инструментов кибермошенничества. Это довольно

значимая цифра. Это и предприятия, которые ведут полноценную хозяйственную деятельность, налоговый учет. Более того, когда мы заблокировали средства, полученные преступным путем, предприниматель вступает с нами в конфликт, и на его стороне копии каких-то договоров об оказании услуг, какие-то юристы, которые должны нас вынудить разблокировать эту сумму", — рассказывает С.Досенко.

Добавить здесь, как говорится, нечего.» ***(Киберспреступность как политическое оружие // СТОПКОР ГО (https://stopcor.org/kybersprestupnost-kak-polytycheskoe-oruzhye/). 08.02.2020).***

***

Боротьба з кіберзлочинністю в Україні

«…Працівники кіберполіції в Миколаївській області спільно зі слідчими поліції Миколаєва, за процесуального керівництва місцевої прокуратури, викрили у протиправних діях місцевого мешканця.

Фігурант був учасником тематичних хакерських форумів, на яких купував персональну банківську інформацію користувачів мережі Інтернет. Після отримання цих даних він здійснював покупки на закордонних інтернет-магазинах, а згодом реалізовував товар на території України. Від його злочинної діяльності постраждали іноземні громадяни.

Для конспірування своєї злочинної діяльності зловмисник використовував VPN та proxy-сервери для приховування реального місцезнаходження та підміни інформації щодо особи платника.

Кіберполіція провела обшуки за місцями мешкання та реєстрації фігуранта. За результатами було вилучено мобільний телефон та комп’ютерну техніку. Вилучене направлено на експертизу.

Також під час попереднього огляду техніки спеціалісти кіберполіції встановили наявність облікових записів, що підтверджують факти злочинної діяльності.

За даним фактом розпочато кримінальне провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Наразі вирішується питання щодо оголошення чоловіку підозри». ***(Кіберполіція викрила мешканця Миколаєва у заволодінні грошима іноземців // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-meshkanczya-mykolayeva-u-zavolodinni-groshyma-inozemcziv-5393/). 12.02.2020).***

***

«Фейковий Telegram-бот Ощадбанку виманював кошти. Заблокувати його допомогли користувачі.

На прохання творців чат-бота «СтопНаркотик» українські користувачі Telegram зупинили роботу бота, який з точністю копіював «Ощадбанк»…

Фейкового бота створили кібершахраї для незаконного отримання даних платіжних карт.

Представники державного банку «Ощадбанк» звернулися до розробника бота для месенджера Telegram «СтопНаркотик» з проханням про допомогу в боротьбі з фейковим ботом банку. Бот @OschadBankkBot імітував ознаки офіційного ресурсу, щоб вводити клієнтів в оману і незаконно отримувати у них фінансову інформацію, що дозволяє зняти гроші з рахунків.

«Завдяки користувачам чат-боту «СтопНаркотик» (@StopDrugBot) адміністрація месенджеру Telegram встановила позначку «Шахрайство» (Scam) та відповідне попередження Telegram-боту @OschadBankkBot, що був створений кібершахраями для незаконного отримання даних платіжних карток та подальшого заволодіння коштами клієнтів банку», — йдеться у повідомленні.

Там зазначили, що нещодавно до факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ звернулися представники державного банку «Ощадбанк» з проханням допомогти припинити роботу боту для месенджера Telegram @OschadBankkBot, який працював вже тривалий час.

Автори чат-боту «СтопНаркотик» вивчили можливість надання такої допомоги. Там вирішили провести День протидії кібешахраям у чат-боті «СтопНаркотик».

Масові скарги на @OschadBankkBot дали адміністрації месенджера Telegram можливість встановити позначку Шахрайство (Scam) і виводити відповідне попередження на сторінці бота…». ***(Ощадбанк поскаржився на фейковий Telegram-бот, що виглядав як справжній. Його заблокували // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/24170/2020-02-05-oshchadbank-poskarzhivsya-na-feikovii-telegram-bot-shcho-viglyadav-yak-spravzhnii-iogo-zablokuvali/). 05.02.2020).***

***

«…Працівники кіберполіції спільно зі слідчими Харківської поліції під процесуальним керівництвом місцевої прокуратури встановили, що до протиправної діяльності причетні двоє 31-річних мешканців Харківщини.

За допомогою активного сканування сайту на вразливість із використанням спеціалізованого программного забезпечення та засобів анонімізації фігуранти здійснювали несанкціоновані втручання в роботу сайтів конкурентів та отримували доступ баз даних.

Правоохоронці провели обшуки у фігурантів, у результаті яких вилучили мобільні телефони та комп’ютерну техніку.

За даним фактом розпочато кримінальне провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Наразі вирішується питання щодо оголошення чоловікам підозр. Фігурантам загрожує до шести років ув’язнення». ***(Кіберполіція встановила двох мешканців Харківщини у викраденні баз даних конкурентів // Національна поліція (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vstanovila-dvox-meshkancziv-xarkivshhini-u-vikradenni-baz-danix-konkurentiv/). 20.02.2020).***

***

«…Працівники Департаменту кіберполіції спільно зі слідчими поліції Харківщини під процесуальним керівництвом Київської прокуратури припинили злочинну діяльність чоловіка.

Встановлено, що до вчинення правопорушення причетний 31-річний мешканець Харкова. Чоловік працював провідним спеціалістом одного з науково-дослідних інститутів і мав відповіді технічні навички.

Нібито для потреб інституту фігурант орендував віртуальний сервер, через який проходили міжнародні виклики, минаючи Міжнародний цент комутації, що призвело до порушення встановленого порядку маршрутизації. В результаті міжнародні дзвінки тарифікувались як національні.

Також несанкціоноване втручання в роботу телекомунікаційної мережі оператора підтверджено комісією Українського державного центру радіочастот.

Правоохоронці провели обшуки за місцями мешкання та роботи чоловіка, в результаті яких вилучили комп'ютерну техніку, мобільні телефони та документацію - усе це направили на експертизу.

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

Наразі вирішується питання про оголошення чоловіку підозри. Йому загрожує до шести років ув'язнення». ***(Кіберполіція викрила чоловіка у несанкціонованому втручанні в роботу оператора телефонного зв'язку // Національна поліція (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-cholovika-u-nesankczionovanomu-vtruchanni-v-robotu-najbilshogo-operatora-telefonnogo-zv-yazku/). 17.02.2020).***

***

«Припинення протиправної діяльності відбувалось в рамках міжнародної спецоперації з правоохоронними органами США. Хакерське угруповання спеціалізувалося на викраденні фінансової інформації громадян та комерційних структур із подальшим заволодінням їх грошовими активами.

Працівники кіберполіції та правоохоронні органи США, у межах реалізації міжнародної спецоперації, викрили протиправну діяльність транснаціональної групи хакерів. Фігуранти спеціалізувалися на викраденні фінансової інформації громадян та комерційних структур із подальшим заволодінням їх грошовими активами.

Зокрема у лютому нинішнього року, у ході розслідування кримінального провадження, розпочатого Головним слідчим управлінням Національної поліції України, під процесуальним керівництвом Офісу Генерального прокурора, було задокументовано протиправну діяльність громадянина України, який є учасником цього хакерського угрупування. Його роль полягала у створенні шкідливого програмного забезпечення, яке в подальшому використовувалося для спустошення банківських рахунків по всьому світу.

На підставі зібраних доказів працівники кіберполіції Київщини із залученням бійців підрозділу спецпризначення ГУНП в Київській області провели обшук за місцем мешкання фігуранта. За результатами вилучено комп'ютерну техніку та

телекомунікаційне обладнання. Попередній огляд підтвердив відношення особи до вчинення вказаних вище злочинів.

Дії зловмисника кваліфікуються за ознаками ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Наразі тривають слідчі дії». ***(Кіберполіція викрила учасника міжнародного хакерського угруповання // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-uchasnyka-mizhnarodnogo-xakerskogo-ugrupovannya-6102/). 24.02.2020).***

***

«У кіберполіції розповіли про суми збитку і компенсації від кібершахраїв та про основні схеми, які застосовували зловмисники. Зазначається, що вдалося повернути майже половину коштів, вкрадених шахраями українців.

У 2019 сума завданих збитків від кібершахраїв в Україні склала 25,5 млн грн, повідомляє Retailers.ua. Про це йдеться у відповіді, яке отримало видання на запит до Департаменту кіберполіції.

Протягом минулого року до відомства надійшло 20 567 звернень громадян. З них в сфері платіжних систем 701, йдеться у звіті. Серед них:

— Крадіжка (ст.185 КК України) — 159 звернень;

— Незаконні дії з інформацією, яка обробляється в комп'ютерах, автоматизованих системах, вчинені особою, яка має доступ до неї (ст.362 КК) – 362;

— Незаконні дії з переказами, платіжними картками та іншими засобами доступу до банківських рахунків (ст. 200 КК) - 180.

Зазначається, що сума матеріальних збитків від шахраїв, що застосовували інформаційні технології, становить 25,5 млн грн (ті, що стосуються кіберполіції — 13,8 млн грн). При цьому сума відшкодованих збитків, з урахуванням накладеного арешту або вилученого майна, становить 12,5 млн грн (кіберполіції - 5,1 млн грн).

Представники кіберполіції також перерахували виданню найбільш часті схеми, які використовують шахраї за допомогою інтернету:

Фішинг — розсилка фейкових електронних листів зі шкідливим програмним забезпеченням;

Вішин — використання мобільного зв'язку з метою вкрасти персональні і платіжні дані;

Використання банківських карт і платіжних систем, в тому числі позика грошей у фінансових організацій;

Фейкові інтернет-магазини, які продають неіснуючий товар і просять передоплату.

Імітація реалізації товарів або послуг через інтернет-аукціон, віртуальні дошки оголошень;

Імітація виграшу в лотерею або так звані миттєві призи;

Фейкові сервіси для переказу грошей або поповнення мобільних телефонів». ***(Стало відомо, скільки збитків завдали українцям кібершахраї // MediaSapiens (https://ms.detector.media/kiberbezpeka/post/24253/2020-02-25-stalo-vidomo-skilki-zbitkiv-zavdali-ukraintsyam-kibershakhrai/). 25.02.2020).***

***

«Служба безпеки України (СБУ) розкрила мережу ботоферм, обладнання яких підтримувалося через російські онлайн-сервіси. Як зазначається на сайті української спецслужби у понеділок, 17 лютого, "телекомунікаційні платформи використовували для створення і просування фейкових акаунтів та спільнот для проведення незаконних операцій в інтернеті".

Загалом угруповання зареєструвало понад вісім тисяч активних акаунтів. Через ці акаунти проводилося "поширення у популярних соцмережах недостовірної інформації про ситуацію в Україні, підбурювання протестних настроїв, залякування населення, розсилання повідомлень про мінування об'єктів критичної інфраструктури та здійснення інформаційних атак на акаунти українських чиновників", повідомляє пресцентр СБУ.

Через ці акаунти також поширювали вогнепальну зброю, вибухові пристрої та наркотичні засоби. Реєстрацію акаунтів провадили через російські онлайн-сервіси, що надавали послуги віртуальних мобільних номерів.

"Частину обладнання зловмисники використовували для нелегального переправлення телефонного трафіку незаконно створених "операторів" "Фенікс" і "Лугаком", які функціонують на тимчасово непідконтрольних територіях, на мережі вітчизняних операторів", - повідомили в СБУ.

У рамках операції проведено обшуки в Києві, Харкові, Дніпрі, Дубно Рівненської області та Ірпені Київської області. Під час обшуків виявлено та вилучено комп'ютерну техніку, спеціальне обладнання, зокрема GSM-модеми та шлюзи, понад 22 тисячі SIM-карт операторів стільникового мобільного зв'язку України.

Було також вилучено чорнові записи про реєстрацію користувачів соціальних мереж, які розміщували провокативні коментарі під публікаціями українських політиків. Наразі перевіряється версія про причетність до організації роботи ботоферм спеціальних і розвідувальних органів Росії, уточнюють у СБУ». ***(Валерій Сааков. СБУ заявила про викриття масштабної мережі ботів для поширення фейків // Deutsche Welle (https://www.dw.com/uk/%D1%81%D0%B1%D1%83-%D0%B7%D0%B0%D1%8F%D0%B2%D0%B8%D0%BB%D0%B0-%D0%BF%D1%80%D0%BE-%D0%B2%D0%B8%D0%BA%D1%80%D0%B8%D1%82%D1%82%D1%8F-%D0%BC%D0%B0%D1%81%D1%88%D1%82%D0%B0%D0%B1%D0%BD%D0%BE%D1%97-%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96-%D0%B1%D0%BE%D1%82%D1%96%D0%B2-%D0%B4%D0%BB%D1%8F-%D0%BF%D0%BE%D1%88%D0%B8%D1%80%D0%B5%D0%BD%D0%BD%D1%8F-%D1%84%D0%B5%D0%B9%D0%BA%D1%96%D0%B2/a-52404981). 7.02.2020).***

***

«Міністр внутрішніх справ Арсен Аваков та виконавчий директор CEPOL Детлеф Шрьодер підписали Угоду між Міністерством внутрішніх справ України та Агентством Європейського Союзу з підготовки співробітників правоохоронних органів (CEPOL).

Про це повідомляє Міністерство внутрішніх справ України.

Відтепер українські правоохоронці зможуть проходити тренінги, обмінюватися новітніми практиками з колегами з ЄС та отримають доступ до відкритих освітніх ресурсів електронної мережі e-Net CEPOL.

Виконавчий директор CEPOL Детлеф Шрьодер зазначив, що основним напрямком двостороннього співробітництва вбачає кібербезпеку.

Співпрацю з CEPOL реалізовуватимуть заклади вищої освіти МВС. Підписана Угода відкриває можливості для більш плідної співпраці. Зокрема буде створено Національний контактний пункт в МВС для регулювання співробітництва, значно більше українських поліцейських зможуть взяти участь у заходах CEPOL…». ***(Українські поліцейські навчатимуться за міжнародними стандартами CEPOL // Євроінтеграційний портал (https://eu-ua.org/novyny/ukrayinski-policeyski-navchatymutsya-za-mizhnarodnymy-standartamy-cepol). 10.02.2020).***

***

«Поки більшість українських фахівців з інформаційних технологій тримають курс на Захід, група чеських ІТ-спеціалістів приїжджають в Україну, при чому не у комфортний Київ, а на лінію фронту – проводити курси кібербезпеки для місцевих та збирати інформацію про те, які методи гібридної війни Росія випробовує на українцях. Те, про що його колеги будуть дізнаватися з газет за кілька років, один з провідних чеських аналітиків Томаш Флідр, має вже зібрано та проаналізовано та незабаром опубліковано. Більше про те, що можна дізнатися про сучасні методи війни, подорожуючи лінією фронту разом з експертами з «Команди для України», TEAM4Ukraine, Томаш Флідр розповів у розмові з Радіо Свобода.

– У листопаді ми вже вдесяте повернулися з України. Наш проєкт, у рамках якого ми проїхали майже цілу лінію фронту та проводили курси кібербезпеки для місцевого самоврядування, поліції та широкої громадськості, підтримує Вишеградський фонд.

Ми дізнавалися про те, що українці на лінії фронту зазнають небезпеки не лише з боку військових російських сил, але і з боку кіберзлочинців. На лінію фронту ми їздили вдруге, і ми побачили, що місцеві люди дуже зацікавлені дізнатися більше про кібербезпеку, бо вони бачать, що інформаційний простір та кіберпростір також перетворюються на зброю проти них. Відчуття небезпеки посилюється тим, що вони перебувають у безпосередній близькості території, де не діє закон.

– Коли людина перебуває у ситуації прямої загрози своєму життю, наскільки її може турбувати проблема кібербезпеки?

– Нас це також здивувало на початку. Я також не думав, що наші лекції заберуть достатньо зацікавлених, бо люди мають думати про фізичне виживання. Але я помилявся. Людей це дійсно цікавить, бо відбувається конвенційна війна, інформаційна війна та кібервійна. Часто все це пов'язано – від інформаційної війни до заблокування в соціальних мережах, до пограбування банківських рахунків через інтернет.

– З чим до вас приходили люди, в яких ділянках найбільше відчували небезпеку?

– В Україні поширені різні форми шахрайства за допомогою інформаційних технологій. У людей вимагають, чи видурюють гроші, грабують їхні банківські рахунки, використовуючи соціальні мережі, наприклад. У соціальних мережах, наприклад, намагаються заблокувати опонентів, або ж вкрадуть їхній профіль на соціальній мережі і з неї поширюють фейкову інформацію. У нинішній час це також велика небезпека, бо інформація, правильна, чи ні, як лавина шириться потім у соціальних мережах.

– Що може людина зробити самостійно, а де вже відповідальність лежить на державних інституціях, на компаніях-власниках соціальних мереж?

– Звичайна людина може зробити досить багато для власної безпеки. Достатньо знати і виконувати досить прості правила – вчасно оновлювати програмне забезпечення своїх пристроїв. Також ми радимо використовувати різні та складні для вгадування паролі до всіх служб. І цим ви зможете ускладнити хакерам пробратися до ваших рахунків, чи зловживання соціальних мереж.

– А які знання в Україні почерпнули ви?

– Ми в Україні дізнаємося багато цікавого. По-перше, Україна та простір колишнього Радянського Союзу є територією, де набагато більш поширеною є кібернетична злочинність. Тож нас цікавить, які методи використовують самі злочинці та те, як їх вирішують місцеві криміналісти.

А по-друге, для нас неоціненним досвідом є можливість вивчати напади на українську життєво важливу інфраструктуру.

Ми бачили напади на інформаційну базу аеропортів, банків, енергетичних компаній. Тут для нас надзвичайно важливою є співпраця з українськими фахівцями, які ці проблеми вирішували. Ми аналізуємо їхній досвід та намагаємося поширити його серед чеських спеціалістів.

– Ви згадали, що в Україні дуже поширеною є кіберзлочинність. Чим ви це пояснюєте, забагато сильних програмістів, які не можуть знайти собі іншого застосування, ніж піти у кібербандити?

– Це відомий факт, що російськомовна кіберзлочинність поширена по цілому світу. Спеціалістів дійсно багато, але і ділянок, де вони можуть застосувати свої знання у злочинному світі, є також дуже багато. Наприклад, вони створюють нові кримінальні ринки – продаж краденої інформації з платіжних карт. Умови для цього бізнесу там дуже сприятливі тому, що звичайні традиційні злочинці, що вже мали захист від переслідування органів правопорядку, об'єдналися свої зусилля зі спеціалістами в ІТ.

На Заході так часто з цією проблемою ми не стикаємося, бо на ІТ-спеціалістів є великий попит і вони можуть заробити достатньо грошей, займаючись легальною діяльністю, і боячись кримінального переслідування.

А друга причина полягає у тому, що в Росії та в країнах навколо неї було дуже важко забезпечити виконання закону, особливо у справі кіберзлочинів. Вигідним для злочинців було те, що на території Росії вони почувалися цілком безпечно. І якщо вони пограбували когось за кордоном, то їх неможливо було притягнути до відповідальності. А тому проблема розширилася настільки, що нині російськомовна кіберзлочинність стала загальносвітовою загрозою.

– Публікації про кіберзлочини читаємо ледь не щодня, інколи дізнаємося, що Росія намагається не допустити екстрадиції своїх хакерів з Ізраїлю – нещодавно, чи з Чехії, трохи раніше. В чому є ваша перевага перед колегами, тим що ви їздите на схід та дізнаєтеся прямо на місці про те, що вони там роблять?

– Цей досвід роботи на місці нічим не можна замінити. Там ми працюємо разом з українськими експертами, які розслідують ці злочини. Також в Україні не дуже поширені є знання англійської мови, тож той, хто хоче знати деталі розслідування, мусить їхати туди і там розпитувати українців.

– То ці знання потім поширюють через вас? Яким чином?

– Ми надаємо послуги з кібернетичної безпеки, консультуємо різні компанії, проводимо для них тренінг. У рамках Чеського інституту менеджерів інформаційної безпеки ми готуємо круглі столи та тренінг для експертів, які займаються безпекою критичної інфраструктури в Чехії і для яких український досвід є надзвичайно цінним». ***(Марія Щур. Чеські фахівці з кібербезпеки вивчають український досвід захисту аеропортів, банків, енергетичних компаній // Радіо Свобода (https://www.radiosvoboda.org/a/rosijska-hybrydna-vijna-i-hackery/30410622.html). 11.02.2020).***

***

«Японські військово-морські сили вперше візьмуть участь у навчаннях "Sea Breeze - 2020" у Чорному морі

Міністри оборони України та Японії Андрій Загороднюк та Таро Коно домовилися продовжувати співпрацю у сфері безпеки та зосередяться на проблемах кібербезпеки.

Ці питання вони обговорили під час зустрічі в рамках міжнародної конференції з безпеки, що проходить у Мюнхені, повідомив український міністр у Facebook.

"Сьогодні зустрічався із делегацією Японії. Останнім часом ми активно нарощуємо наше співробітництво. Ми вже зустрічали у Києві голову японського Генштабу і сьогодні зі своїм колегою Таро Коно обговорили подальшу співпрацю. Перед нами багато спільних завдань – ми продовжуємо втілювати у життя Меморандум між нашими оборонними відомствами щодо співробітництва та обмінів у сфері безпеки", – повідомив Загороднюк.

Він зазначив, що спершу сторони зосередяться на проблемах кібербезпеки, співробітництві у високотехнологічних проєктах та діджиталізації, а також обмінюватимуться досвідом протистояння гібридним загрозам.

"Особливо приємно, що цього року ми вперше побачимо дружні нам японські військово-морські сили в нашому Чорному морі на міжнародних навчаннях "Sea Breeze - 2020",– додав міністр.

Він подякував "друзям зі Сходу за принципову підтримку".» ***(У Мюнхені зустрілися міністри оборони України та Японії – які акценти співпраці обговорили // 5 канал (https://www.5.ua/polityka/u-miunkheni-zustrilysia-ministry-oborony-ukrainy-ta-yaponii-iaki-aktsenty-spivpratsi-obhovoryly-208376.html)/. 16.02.2020).***

***

«Апарат Ради національної безпеки та оборони України повідомив чудові новини. Очільник Радбезу Олексій Данілов заявив, що РНБО буде співпрацювати з найбільшими приватними американськими та ізраїльськими компаніями у протидії кіберзагрозам.

"Кібербезпека не є проблемою кожної окремої держави. У разі виявлення загрози ми розуміємо, що вона може зачепити не одну окремо взяту країну. Спільними зусиллями боротися з такими загрозами набагато ефективніше. Тому нині нам необхідно налагодити механізм співпраці у питанні захисту від кіберзагроз", — заявив Олексій Данілов.

Варто звернути увагу на те, що Національний координаційний центр кібербезпеки РНБО на постійній основі співпрацюватиме з американськими компаніями-виробниками технологій та обладнання для кібербезпеки та захисту: Cisco, Fortinet, IBM, MicroFocus, Microsoft та ізраїльською компанією Radware.

Що важоиво розуміти, нещодавно українська поліція звернулася до Федерального бюро розслідувань США та до компанії "Area1" з важливим та терміновим прохання. НПУ закликає надати дані про хакерську атаку студії "Квартал 95", холдингу "Burisma" та інших українських компаній. Окрім того, офіційний Київ запрошує ФБР приєднатися до спільної слідчої групи»… ***(РНБО несподівано звернулася по допомогу до США // ONLINE.UA (https://novyny.online.ua/817355/rnbo-nespodivano-zvernulasya-po-dopomogu-do-ssha/). 14.02.2020).***

***

«Военная помощь Соединенных Штатов для Украины была предоставлена с той целью, чтобы Киев сумел защитить себя от агрессии Москвы. Об этом заявил госсекретарь США Майл Помпео во время выступления на Мюнхенской конференции по безопастности, сообщает пресс-служба Госдепартамента.

Также Помпео отметил, что с той же целью США оказывают помощь Украине в сфере кибербезопасности.

"Соединенные Штаты вооружили Украину, чтобы помочь этой храброй нации защитить себя от российской агрессии, и совместно с балтийскими странами работали над кибербезопасностью, чтобы защититься от повторных кибератак Москвы", - сказал Помпео. Госсекретарь также подчеркнул, что США не признают окупацию украинских территорий, а бадут поддерживать суверенитет Украины».

(Помпео: США вооружили Украину, чтоб она защитилась от агрессии Москвы // информационный портал "ua.today" (http://ua.today/news/politics/pompeo_ssha_vooruzhili_ukrainu_chtob_ona_zashitilas_ot_agressii_moskvy). 17.02.2020).

***

«В Тбилиси (Грузия) состоялась конференция по планированию мероприятий международных учений «Noble Partner – 2020».

В работе конференции приняли участие представитли пяти стран НАТО: Великобритания, Германия, Словения, Турция и США, а также страны-партнеры Альянса — Грузия, Украина и Армения. Украину представили офицеры командования морской пехоты ВМС ВСУ…

На конференции рассматривались вопросы безопасности и стабильности в Черноморском регионе, а также темы повышения уровня готовности и взаимодействия между Грузией, США и странами-партнерами.

В текущем году учения «Noble Partner» будут включать полевую и штатную компоненты. Одними из основных направлений учений станут кибербезопасность и информационные операции…». ***(Учения «Noble Partner – 2020»: Украина представит на учениях 100 морпехов ВМС // Чорноморські новини (https://www.blackseanews.net/read/160811). 14.02.2020).***

***

«Швейцарская страховая компания Zurich Insurance объявила о сотрудничестве в сфере кибернетической и страховой защиты с израильской компанией CYE.

Как сообщает интернет ресурс УкрСтрахование со ссылкой на пресс-релиз Zurich, преимущества Zurich Cyber Security Services заключаются в выявлении уязвимостей в кибербезопасности, снижении риска и воздействия киберинцидентов, в проактивной защите критически важных бизнес-активов.

«Наше сотрудничество с CYE, мировым лидером в сфере услуг кибербезопасности, предоставит клиентам современное решение, которое сочетает в себе преимущества страхования и повышение уровня их киберзащиты», — прокомментировали в Zurich.

В компании также отметили, что приобретение автономной программы киберзащиты позволит клиентам использовать преимущества сотрудничества с CYE. Так, страховая программа включает в себя детальную оценку риска в отношении киберугроз.

Ранее Zurich Insurance сообщила о росте чистой прибыли за минувший год на 12% до $4,1 млрд, что является самым высоким результатом с 2010 года». ***(Zurich Insurance совершенствует киберстрахование совместно с компанией CYE // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/zurich-insurance-sovershenstvuet-kiberstrahovanie-sovmestno-s-kompaniej-cye). 26.02.2020).***

***

«IT-фахівці вашої організації, ймовірно, доклали багато зусиль для того, щоб ваші внутрішні акаунти, логіни, паролі та системи були надійно захищені. Але що відбувається, коли працівник компанії, який не сильно розбирається в тонкощах кібербезпеки, створює зовнішній акаунт? Цей процес відомий під назвою тіньове IT (Shadow IT), і на думку експертів з 1Password, такі речі становлять ризики для безпеки компанії.

Проілюструємо IT Shadow на прикладі наступної історії. Скажемо, співробітник хоче скористатися певним зовнішнім сервісом всередині корпоративної мережі. Можливо, ваш колега хоче використати Amazon, щоб придбати певні продукти для свого департаменту, або Uber для замовлення таксі для інших співробітників, Grammarly для перевірки внутрішніх документів на помилки або Constant Contact для побудови електронних кампаній. Співробітник створює свій власний обліковий запис у зовнішній службі, ймовірно, використовуючи слабкий або незахищений пароль.

Далі цей працівник починає ділитися внутрішніми документами та інформацією із зовнішнім сервісом. Якщо одна з цих служб зазнає порушення даних або витоку пароля, це наражає на небезпеку працівника та потенційно вашу організацію, оскільки відкриває ваші конфіденційні дані. І все це відбувається без участі вашої команди з інформаційної безпеки.

Під час опитування понад 2100 дорослих у США, які працюють в офісі з персоналом IT та користуються комп'ютером, дослідники 1Password виявили, що 63% респондентів створили принаймні один обліковий запис за останні 12 місяців, не маючи відповідного знання в IT. Крім того, 52% з них згенерували від двох до п'яти акаунтів, тоді як 16% створили понад п'ять таких облікових записів.

За підсумками опитування тіньові IT-акаунти можуть стати джерелом інших проблем. Близько 37% респондентів сказали, що вони ділилися зовнішнім обліковим записом з колегами. Але спосіб обміну інформацією про акаунт може бути ризиковим. Майже 40% сказали, що вони повідомляли дані облікового запису колезі електронною поштою, тоді як 17% сказали, що вони поділилися ним через засіб обміну миттєвими повідомленнями.

Але якщо інформацію про акаунт нікому не повідомити, а власник облікового запису категорії Shadow IT звільняється з компанії, то інші люди можуть опинитися без доступу до необхідного сервісу. Крім того, цей працівник, ймовірно, все ще матиме доступ до облікового запису, і така інформація може навіть опинитися в руках конкурента.

Співробітники, які створюють так звані тіньові IT-акаунти, не обов'язково генерують надійні та безпечні паролі для кожного сайту. Близько 33% респондентів сказали, що вони повторно використовують паролі, які легко запам'ятати, тоді як 48% сказали, що вони використовують шаблон схожих паролів для усього спектру сервісів чи сайтів. Менш як 3% сказали, що вони використовують унікальний пароль для кожного сайту.

Розв'язанням цієї проблеми може стати повна заборона тіньових облікових записів. Але цей захід уповільнить продуктивність працівників, оскільки

вимагатиме, щоб кожна людина погоджувала з командою кібербезпеки створення такого зовнішнього облікового запису.

Ще одним рішенням може стати використання менеджерів паролів. Чимало таких додатків пропонують широкий спектр сервісів, за допомогою яких можна керувати політикою паролів. До того ж, існують різноманітні менеджери паролів. Крім 1Password, іншими ефективними програмами є LastPass, Dashlane, RoboForm та Keeper Password Manager. Хоча менеджери паролів не є ідеальними, все ж вони є цілком життєздатним рішенням, як мінімум до того моменту, поки більш ефективні методи біометричної аутентифікації не стануть універсальними». ***(Чим тіньове IT небезпечне для вашої організації? // Blog Imena.UA (https://www.imena.ua/blog/shadow-it-is-dangerous-for-your-organization/). 11.02.2020).***

***

«Компания Check Point Software Technologies объявила финансовые результаты за четвертый квартал 2019 г. и подвела итоги 2019 финансового года. Выручка в четвертой четверти 2019 г. выросла на 3% в годовом сопоставлении и достигла 544 млн долл. Операционный доход по GAAP составил 249 млн долл., а non-GAAP – 280 млн долл. Выручка за 2019 финансовый год повысилась на 4% и достигла 1,995 млн долл. Операционный доход по GAAP составил 882 млн долл., соответственно non-GAAP – 1,003 млн долл.

«Мы завершили десятилетие с выручкой почти в два миллиарда долларов в год и более чем одним миллиардом долларов операционного дохода (non-GAAP). За десять лет мы представили новую модель Security-as-a-Service, которая предоставляет самые продвинутые технологии в области кибербезопасности. В 2019 г. доход от подписок достиг более шестисот миллионов долларов, чему способствовали облачные, мобильные и иные ведущие технологии предотвращения угроз нулевого дня, – отмечает Гил Швед (Gil Shwed), основатель и исполнительный директор Check Point Software Technologies. – Новое десятилетие мы начали с представления Infinity Next, самой комплексной в отрасли платформы кибербезопасности с более чем 60 технологиями защиты, которые поддерживают более 50 типов активов, включая операционные системы, облачные рабочие нагрузки, сети любого типа, IoT и мобильные устройства» ***(Выручка Check Point за 2019 г. выросла на 4% и вплотную приблизилась к 2 млрд. долл. // Компьютерное Обозрение (https://ko.com.ua/vyruchka_check_point_za_2019_g_vyrosla_na_4_i_vplotnuyu_priblizilas_k_2_mlrd_doll_131856). 11.02.2020).***

***

«Майк О'Коннор, один из первых инвесторов в области доменных имен, в 90-е владел очень популярными адресами, многие из которых впоследствии продал. Но одно на первый взгляд обычное доменное имя он выставил на продажу только сейчас, установив стартовую цену в 1,7 миллиона долларов. Продавец утверждает, что с учетом особенностей товара его цена не такая уж и большая.

Такие известные домены, как bar.com, cafes.com, pub.com, grill.com, place.com ушли с молотка уже давно. И только сейчас предприниматель выставил на аукцион доменное имя corp.com, сообщает gizmodo.

Дело в том, что компьютеры под управлением версий Windows с поддержкой технологии Active Directory по умолчанию обращаются к домену corp, находясь в локальной сети. Если же такой ПК попадает в общественную сеть, то различные приложения продолжают обращаться по тому же адресу, раскрывая корпоративные данные стороннему серверу.

Речь идет о проблеме, известной как "коллизия пространства имен", когда доменные имена, предназначенные для использования исключительно во внутренней сети компании, в общем итоге пересекаются с доменами, которые находятся в открытом интернете, – пояснил специалист по кибербезопасности Брайан Кребс.

По данным экспертов, владелец такого домена сможет подключиться к "бесконечному потоку конфиденциальной информации, включая адреса электронной почты и пароли крупных корпораций со всего мира. Сам О'Коннор надеется, что домен будет куплен корпорацией Microsoft, а не киберпреступниками или хакерскими группами». ***("Самый опасный в мире" домен выставили на аукціон // Телеканал новостей «24» (https://24tv.ua/techno/ru/samyj_opasnyj_v_mire_domen_vystavili_na_aukcion_n1278824). 11.02.2020).***

***

«Официально объявлено о продаже производителя программного обеспечения для кибербезопасности Forescout Technologies частной инвестиционной компании Advent International за 1,9 млрд долларов.

В пересчете на одну акцию Forescout стоимость сделки составила 33 доллара. Это примерно на 30% больше курса ценных бумаг к закрытию биржи 18 октября 2019 года - накануне появления первых данных о выставлении компании на продажу.

Решения ForeScout представляют собой автоматизированную платформу для обеспечения информационной безопасности компаний, которая позволяет отслеживать и контролировать все устройства, подключенные к корпоративной сети, в режиме реального времени. Технология ForeScout CounterACT автоматически идентифицирует все подключения к сети, контролирует доступ в рамках установленных политик безопасности и требований стандартов, блокирует сетевые угрозы, исправляет нарушения в безопасности конечных точек.

Закрыть сделку по продаже ForeScout компании Advent планируется во втором квартале 2020 года. Однако у ИБ-вендора есть 30 дней на то, чтобы рассмотреть другие предложения от потенциальных покупателей.

В случае оформления сделки с Advent компания Forescout перестанет быть публичной. Ее президент и генеральный директор Майкл ДеЧезаре останется во главе». ***(Владимир Смирнов. ИБ-компанию Forescout продают за $1,9 млрд // ChannelForIT (http://channel4it.com/publications/-IB-kompaniyu-Forescout-prodayut-za-19-mlrd-36653.html#). 10.02.2020).***

***

«Кибербезопасность стала основным направлением цифровых инвестиций нефтяных и газовых добывающих компаний. Это следует из седьмого международного отчета Accenture о цифровых технологиях в нефтегазовой отрасли (Accenture Upstream Oil and Gas Digital Trends Survey 2019), основанного на опросе 255 профессионалов отрасли, включая топ-менеджеров, функциональных лидеров и технических специалистов.

Среди направлений цифровых инвестиций респонденты чаще всего упоминали кибербезопасность: ее отметили 61% опрошенных, что в 5 раз выше, чем в 2017 году (12%). В отчете также отмечается, что инвестиции в эту сферу резко возросли из-за стремления нефтяных компаний защитить свои активы и репутацию. Помимо этого, среди всех цифровых технологий именно кибербезопасность была отмечена наибольшим количеством респондентов (16% против 9% в 2017 году) как оказывающая максимальное влияние на эффективность бизнеса.

Несмотря на возросшие инвестиции в кибербезопасность, лишь 5% опрошенных считают уязвимость к кибератакам самым большим риском недостаточного финансирования в области цифровых технологий — это лишь треть от уровня 2017 года (18%). Возможно, это объясняет, почему лишь 35% респондентов планируют инвестировать в информационную безопасность в течение ближайших трех-пяти лет.

«По мере того, как работа нефтяных компаний подвергается все большей угрозе, киберустойчивость становится особенно важной для заинтересованных сторон, потребителей и правительства. Управление атаками — не только вопрос защиты репутации, стоимости акций и деятельность компаний, но и часть ответственности за безопасность государства. Добывающие предприятия должны продолжать осознанно инвестировать в кибербезопасность, поскольку они часто недооценивают свою уязвимость перед атаками, которые становятся изощреннее с технической точки зрения», — рассказал Рич Холсман, управляющий директор, руководитель направления цифровых технологий в нефтегазовом комплексе Accenture…

На вопрос о том, в какие цифровые технологии нефтяные и газовые компании планируют инвестировать в течение ближайших 3-5 лет, большинство респондентов (51%) указали ИИ и машинное обучение (30% в 2017 году). Следом идут большие данные/аналитика (50%), интернет вещей (43%) и мобильные/носимые технологии (38%).

Почти половина (47%) респондентов самым большим риском, связанным с отсутствием инвестиций в цифровые технологии, назвали потерю конкурентных преимуществ. А 42% опрошенных назвали снижение затрат самой значительной бизнес-задачей, которую могут решить цифровые технологии…». ***(Accenture: кибербезопасность — основное цифровое направление инвестиций для нефтегазовых добывающих компаний // Сервис размещения пресс-релизов (https://pr.adcontext.net//20/02/14/305007). 14.02.2020).***

***

«В конце января 2020 года Министерство внутренних дел США приостановило работу всего парка беспилотных летательных аппаратов, за исключением чрезвычайных ситуаций, из-за угрозы национальной безопасности.

Министерство сообщило, что намерено основать собственный парк беспилотников для «обеспечения кибербезопасности и использования американских технологий беспилотных авиационных систем» без привлечения иностранных компаний.

Приказ предписывает правительственным чиновникам поддерживать беспилотники отечественного производства, поскольку информация, собранная беспилотниками иностранных компаний, «потенциально может использоваться иностранными организациями и правительствами». Правительственные чиновники признали, что все действующие беспилотники департамента были сделаны в Китае или используют детали китайского производства.

«Защита национальных ресурсов США требует постоянных мер по обеспечению безопасного доступа, сбора и хранения информации, значительная часть которой является конфиденциальной… Департамент принимает меры по обеспечению кибербезопасности и развития внутреннего производственного потенциала», — говорится в приказе.

В нынешнем виде флот беспилотников будет использоваться только в чрезвычайных ситуациях, таких как борьба с лесными пожарами, проведение спасательных поисково-спасательных операций и борьба со стихийными бедствиями. Помимо чрезвычайных ситуаций, министерство внутренних дел ранее использовало свои беспилотники для различных целей, в том числе для исследования федеральных земель, сбора исследовательских данных и оказания помощи правоохранительным органам.

Китайский производитель дронов DJI, который поставлял беспилотники для правительства США, отметил, что «крайне разочарован» принятым решением». ***(В США приостановлена работа всего флота дронов из-за угрозы нацбезопасности // (IKSMEDIA.RU (http://www.iksmedia.ru/news/5642872-V-SSHA-priostanovlena-rabota-vsego.html). 04.02.2020).***

***

«Прокуратуре штата Флорида пришлось отозвать 11 дел о производстве и торговле запрещенными веществами, возбужденных против шести подозреваемых, в связи с недостатком доказательств. В ходе расследования, длившегося в течение полутора лет, сотрудники полицейского управления города Стюарт собрали всю необходимую доказательную базу, однако она была уничтожена в результате заражения компьютерных сетей управления вымогательским ПО.

В апреле прошлого года полицейское управление Стюарта стало жертвой атаки нашумевшего вымогателя Ryuk, попавшего в компьютерные сети через фишинговое электронное письмо с вредоносной ссылкой. За расшифровку файлов киберпреступники требовали $300 тыс., но администрация города отказалась

платить. В течение шести недель все 46 сотрудников полицейского управления писали отчеты по старинке – с помощью ручки и бумаги.

Полицейским удалось восстановить некоторые файлы из резервных копий, но фото- и видеодоказательства в 11 делах о сбыте запрещенных веществ были утеряны безвозвратно, сообщил детектив-сержант полиции Стюарта Майк Геруэн (Mike Gerwan) в интервью журналистам телеканала WPTV. В результате утери доказательств уголовные дела были отозваны, с шестерых подозреваемых сняты обвинения по 28 пунктам, а сами подозреваемые были отпущены на свободу.

Случившееся заставило полицейское управление использовать другой способ хранения вещественных доказательств, а городская администрация теперь активно проводит обучение правилам кибергигиены, в частности учит сотрудников распознавать фишинговые письма». ***(Вымогательское ПО Ryuk освободило шестерых уголовников // SecurityLab.ru (https://www.securitylab.ru/news/505443.php). 28.02.2020).***

***

«Компания Google намерена вывести учетные записи своих пользователей в Великобритании из-под действия европейского законодательства в области защиты данных и применять к ним законодательство США. Об этом информагентству Reuters сообщили осведомленные источники.

Данный шаг продиктован выходом Великобритании из Евросоюза, в результате которого конфиденциальная информация десятки миллионов британцев лишится надежной защиты, а британские правоохранительные органы будут иметь к ней легкий доступ.

Как сообщают источники, Google намерена обязать пользователей в Великобритании ознакомиться с новыми условиями пользования, включающими в том числе новую юрисдикцию.

«В наших сервисах и подходе к приватности ничего не изменится, в том числе то, как мы собираем или обрабатываем данные и отвечаем на запросы правоохранительных органов на выдачу информации пользователей. Действие британского «Общего регламента по защите данных» также будет распространяться на этих пользователей», - сообщается в письменном заявлении представителей Google.

Ирландия, где у Google и других технологических компаний есть свои офисы, остается в составе Европейского союза, чье законодательство в области защиты данных является очень жестким. Google решила вывести британских пользователей из ирландской юрисдикции, так как пока неизвестно, будет ли Великобритания придерживаться «Общего регламента по защите данных» (GPDR), или примет новые законы». ***(Google выведет британских пользователей из-под действия европейских законов // SecurityLab.ru (https://www.securitylab.ru/news/505227.php). 20.02.2020).***

***

«Киберполиция обсудила с представителями Совета Европы улучшения законодательства и имплементацию Будапештской конвенции о киберпреступности.

Представители Совета Европы выразили готовность к сотрудничеству с украинскими правоохранителями в сфере реализации положений Будапештской конвенции, обеспечивающих повышение уровня противодействия и расследования киберпреступлений.

Об этом заявил председатель отдела киберпреступности Совета Европы Александр Сегера по итогам встречи с руководством департамента киберполиции, сообщает пресс-служба Национальной полиции Украины…

Департамент киберполиции представил свою концепцию имплементации отдельных положений конвенции, которые на текущий момент отсутствуют в украинском законодательстве, которая была поддержана экспертами.

Отмечается, что киберполиция совместно с другими органами исполнительной власти проводит работу с комитетами Верховной Рады Украины по приведению украинского законодательства в соответствие с европейским…

Глава департамента киберполиции Александр Гринчак сообщил, что для качественного документирования и расследования уголовных правонарушений в Украине должен быть создан механизм сбора цифровых доказательств…

Конвенция о киберпреступности является необходимой для остановки действий, направленных против конфиденциальности, целостности и доступности компьютерных систем, сетей и компьютерных данных, а также злоупотребления такими системами, сетями и данными, путем установления уголовной ответственности за такое поведение.» ***(Усовершенствование киберзащиты в Украине: Совет Европы заявил о полной поддержке // Телеграф (https://telegraf.com.ua/ukraina/obshhestvo/5329997-usovershenstvovanie-kiberzashhityi-v-ukraine-sovet-evropyi-zayavil-o-polnoy-podderzhke.html). 01.02.2020).***

***

«Компания Mastercard организовала работу нового Центра обеспечения кибербезопасности на базе своей европейской штаб-квартиры в Бельгии. Сотрудники подразделения будут способствовать региональному сотрудничеству и инновациям в области информационной безопасности между промышленностью, государственным сектором и регулирующими органами.

Новый центр обеспечения кибербезопасности является для Mastercard первым за пределами Северной Америки. Согласно официальным данным, компания намерена объединить специалистов, работающих в данной сфере, для борьбы с угрозами, с которыми сталкивается платёжная экосистема в Европе. Сотрудники нового подразделения будут сотрудничать с национальными агентствами по кибербезопасности, отраслевыми органами, правоохранительными органами и центральными банками стран, входящих в состав Евросоюза. В компании считают, что новый центр поможет «сократить линии связи» между

внутренними подразделениями кибербезопасности и внешними клиентами, партнёрами и другими заинтересованными сторонами.

Также отмечается, что благодаря новому подразделению Mastercard рассчитывает получить ряд преимуществ, в частности, сокращение времени реагирования на различные глобальные события в сфере кибербезопасности. Кроме того, компания рассчитывает установить базовый уровень обмена разведданными с правоохранительными органами и спецслужбами, чтобы совместными усилиями бороться с киберпреступностью на территории Европы.

«Финансовые услуги всегда будут оставаться на вершине целевого списка для злоумышленников из-за огромного объёма конфиденциальных данных клиентов, находящихся под нашей ответственностью. Наш европейский Центр обеспечения кибербезопасности позволит повысить эффективность сотрудничества между ключевыми организациями, а также поможет обеспечить безопасность бизнеса и частных лиц при обмене информацией в сети Интернет», — сказал президент европейского подразделения Mastercard Хавьер Перес (Javier Perez)». ***(У Mastercard появилось европейское подразделение по обеспечению кибербезопасности // SmartPhone.ua (http://www.smartphone.ua/news/u_mastercard_poyavilos_evropeyskoe_podrazdelenie_po_obespecheniyu_kiberbezopasno_63752.html). 18.02.2020).***

***

«Агентство Европейского Союза по кибербезопасности (ENISA) выпустило руководство Procurement Guidelines for Cybersecurity in Hospitals («Руководство по закупкам для обеспечения кибербезопасности в больницах»).

Больницы представляют собой обширные экосистемы, состоящие из сетей устройств, оборудования и систем, которые часто требуют подключения к внешним системам. В связи с важностью медицинских данных и потенциальными уязвимостями, с которыми может столкнутся медицинское учреждение, кибербезопасность должна применяться на каждом этапе для обеспечения конфиденциальности данных пациента, а также доступности и устойчивости служб здравоохранения одновременно.

Разработанное ENISA руководство предоставляет информацию, которая должна быть включена в запросы на закупки больницами IT-оборудования.

В документе изложены передовые практики и рекомендации по включению кибербезопасности в процессе закупок в больницах. В нем представлен набор больничных активов и наиболее известные угрозы кибербезопасности, связанные с ними.

После разделения процесса закупок на три этапа («Планирование», «Источник» и «Управление») руководство определяет требования кибербезопасности, связанные с каждым из них.

Документ предназначен для IT-директоров, руководителей по информационной безопасности предприятия (CISO), технических директоров, IT-команд, а также заведующих закупками в организациях здравоохранения». ***(ENISA выпустило руководство по закупкам для кибербезопасности в больницах // SecurityLab.ru (https://www.securitylab.ru/news/505340.php). 25.02.2020).***

***

Китай

«Компания Huawei сделала официальное заявление в связи с публикацией в Wall Street Journal информации о наличии в ее телекоммуникационном оборудовании, так называемых, бекдоров.

Американское издание, ссылаясь на свои источники, опукбликовало статью, в которой утверждается, что китайская компания Huawei обладает скрытым доступом к сетям мобильных телефонов по всему миру. И якобы происходит это последние 10 лет.

“Обвинения США в сторону Huawei относительно использования законного перехвата данных являются ничем иным, как дымовой завесой, поскольку такие заявления не соответствуют ни одной из форм общепринятой логики в сфере кибербезопасности. Компания Huawei не имела и не будет иметь скрытого доступа к телекоммуникационным сетям, а также не имеет возможностей для этого”, говорится в заявлении компании.

Производитель подчеркивает, что задача Huawei, как и любого другого поставщика коммуникационных услуг, заключается в обеспечении оборудованием, соответствующим международным стандартам 3GPP/ETSI. “Мы обязаны соответствовать общепринятым стандартам правомерного перехвата данных, в том числе, стандарту 3GPP TS 33.107 для сетей 3G и TS 33.128 для 5G. Именно в этом состоят обязательства Huawei относительно правомерного перехвата данных”, отмечает китайская компания.

Фактическое администрирование и использование интерфейсов правомерного перехвата данных осуществляется исключительно поставщиками коммуникационных услуг и контролирующими органами. Интерфейсы перехвата данных всегда размещены в защищенных помещениях оператора. Ими руководят квалифицированные сотрудники, которых тщательно проверяют компетентные органы страны, на территории которой оператор связи осуществляет деятельность. Правила работы и технической поддержки интерфейсов у таких операторов связи очень строгие. Компания Huawei, официально заявляет, что не занимается разработкой или производством какого-либо другого оборудования для перехвата данных.

Huawei уверяет, что является исключительно поставщиком оборудования. А для поставщика оборудования доступ возможен только при условии, если оператор связи предоставляет авторизированный доступ к сети и контролирует такой доступ. “Компания не может действовать в обход операторов связи, получать контроль и данные с их сетей без обнаружения всеми обычными брандмауэрами и системами безопасности. Фактически, даже Wall Street Journal признает, что официальные представители правительства США не в состоянии предоставить никаких конкретных подробностей этих, так называемых, «бэкдоров» (несанкционированного доступа к данным)”, продолжает в своем заявлении Huawei». ***(Huawei отрицает существование «бекдоров» // Компьютерное Обозрение (https://ko.com.ua/huawei_otricaet_sushhestvovanie_bekdorov_131912). 14.02.2020).***

***

«В министерстве иностранных дел Китая назвали США "крупнейшим шпионом в мировом киберпространстве" и "империей хакеров"

Так официальный представитель МИД КНР Гэн Шуан в понедельник в ходе онлайн-брифинга прокомментировал сообщения СМИ о масштабной операции американских и германских спецслужб, якобы проводившейся под прикрытием швейцарской компании Crypto AG, передает "ДС" со ссылкой на ТАСС.

"Факты в очередной раз доказали, что США являются крупнейшим государством-перехватчиком в международном киберпространстве и в полном смысле слова империей хакеров. Их прослушка уже достигла уровня настоящего бесчинства, беззакония и беспредела", - сказал дипломат.

"Каждый день они перехватывают 5 млрд телефонных звонков по всему миру, уже более 10 лет прослушивают телефон канцлера ФРГ Ангелы Меркель, ежегодно захватывают контроль над 3 млн компьютеров в Китае и встраивают троянские программы более чем в 3,6 тысячи китайских сайтов. Но в то же время они силятся выставить себя жертвой кибератак, многократно разыгрывая спектакль, когда вор кричит "держи вора". Это глупые и бестолковые фокусы", - указал Гэн Шуан.

"Не закрыв старые долги, США открывают новые. Соединенным Штатам еще предстоит закрыть свой должок перед миром по делу [организации] WikiLeaks и [бывшего сотрудника Агентства национальной безопасности США Эдварда] Сноудена", - резюмировал он…» ***("Империя хакеров": в МИД Китая дали характеристику США // DsNews (https://www.dsnews.ua/world/-imperiya-hakerov-v-mid-kitaya-dali-harakteristiku-ssha-17022020173300). 17.02.2020).***

***

Російська Федерація та країни ЄАЕС

«В Минкомсвязи разработан порядок установки и эксплуатации средств для поиска признаков кибератак на критические информационные инфраструктуры (КИИ). Проект документа размещен на портале общественного обсуждения.

Новый порядок поможет сформировать единый подход к установке и эксплуатации средств, предназначенных для поиска признаков кибератак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ.

Устройства для поиска атак будут устанавливаться в специальных помещениях с ограниченным доступом персонала. Таким образом будет обеспечиваться защита и неприкосновенность оборудования.

Необходимость и места установки данного оборудования будут определены уполномоченным органом Государственной службы определения и противостояния кибератакам (ГосСОПКА) на основании оценки безопасности КИИ.

Как сообщается в документе, приобретенное за бюджетные средства оборудование и контроль за его работой будут переданы ГосСОПКА. Любые мероприятия будут проводиться после согласования с операторами и письменного уведомления собственников сетей». ***(Разработан порядок установки устройств***

для выявления атак на КИИ // SecurityLab.ru (https://www.securitylab.ru/news/505476.php). 28.02.2020).

***

Інші країни

«Більшість банків, які працюють у Японії, визнали, що вони не готові протистояти кібератакам…

«Проведене Центробанком Японії опитування виявило, що приблизно 60% фінансових інститутів країни не мають достатньої кількості працівників для проведення заходів протидії кібератакам», – ідеться в повідомленні.

Як зазначається, Центробанк Японії опитав 402 фінансових установ щодо того, чи зазнавали вони кібератакам і яких заходів у зв'язку з цим уживали.

39% опитаних заявили, що вони стали об'єктами кібернападів у період між 2017-м і 2019 роками.

Водночас 59% установ визнали, що не мають достатньої кількості працівників для розвитку системи захисту і протидії кібератакам…». ***(Банки Японії не готові протистояти кібератакам // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/banky-yaponiyi-ne-gotovi-protystoyaty-kiberatakam.html). 02.02.2020).***

***

Протидія зовнішній кібернетичній агресії

«Міністерство юстиції США звинуватило чотирьох військовослужбовців Визвольної армії Китаю в організації кібератаки в 2017 році проти Equifax, яка отримала доступ до особистої інформації 147 мільйонів користувачів, за даними американських ЗМІ.

Сьогодні на прес-конференції генеральний прокурор США і міністр юстиції Вільям Бар і заступник директора ФБР Девід Боуік оголосили обвинувачення. Боудіч назвав вхід в Equifax «найбільшої крадіжкою конфіденційної особистої інформації від будь-коли зареєстрованих за підтримки держави хакерів» і подякував Equifax за співпрацю в розслідуванні.

«Це було навмисне і широкомасштабне порушення особистої інформації американського народу. Сьогодні ми несемо відповідальність за хакерів Китайської армії звільнення за їх злочинну діяльність і нагадуємо китайському уряду, що у нас є можливість видалити плащ анонімності в Інтернеті і знайти хакерів, яких країна неодноразово використовує проти нас», – підкреслив Бар.

В результаті злому, однією з найгірших кібератак в історії, мільйони людей застигли на кредитних рахунках, оскільки хакери можуть продавати номери соціального страхування і іншу незмінну ідентифікаційну інформацію, відкривати кредити на своє ім'я. В результаті був поданий гігантський позов проти Equifax за нездатність захистити інформацію. Виявлення хакерів і то, як вони використовували дані, було величезною загадкою за останні кілька років.

Equifax – одне з найбільших агентств по звітності про споживчі кредити в США, в якому зберігаються імена, номери соціального страхування, кредитна історія і інша особиста інформація більше 800 мільйонів чоловік. Компанії використовують послуги Equifax для моніторингу кредитної історії клієнтів та запобігання спробам шахрайства». ***(Оксана Савчук. США звинуватили чотирьох китайських солдатів у великій хакерській атаці // ІА "ЄУРАБОТА" (https://news.eurabota.ua/uk/usa/developments/ssha-zvinuvatili-chotiroh-kitajskih-soldativ-u-velikij-hakerskij-ataci/). 11.02.2020).***

***

«Після масивної DDoS-атаки в Ірані активували систему кіберзахисту "Цифрова фортеця". Перебої з доступом в мережу фіксувалися протягом семи годин. В цей же період Іран з невідомої причини не зміг запустити свій супутник.

Атака на іранські ресурси відбулася 8 лютого, після чого місцева влада активували механізм кіберзахисту "Цифрова фортеця", також відомий як DZHAFA. Інтернет-обсерваторія NetBlocks підтверджує масштабні проблеми в інтернет-системі Ірану. Це призвело до зниження національного підключення до мережі до 75 відсотків від звичайного рівня. Через годину робота мережі була частково відновлена, але в основних іранських операторів мобільного та фіксованого зв'язку проблема збереглася ще кілька годин.

У місцевому Міністерстві ІКТ повідомили, що активували "Цифрову фортецю" після DDoS-атаки. При цьому довелося частково відключити діючі мережі. За даними іранських чиновників, немає ознак підтримки атаки з боку будь-якої держави. Це вже не перша спроба порушити роботу урядових серверів Ірану. Подібні інциденти були зафіксовані NetBlocks в листопаді і грудні минулого року.

8 лютого Іран планував вивести на орбіту супутник спостереження Зафар, але переніс час старту. У космічному відомстві країни стверджували, що запуск відбудеться "при першій нагоді". Пізніше державне телебачення Ірану повідомило, що ракета-носій "Симорг" не змогла вивести супутник на орбіту. Поки невідомо, чи пов'язані проблеми космічного апарату з кібератакою». ***(Через кібератаки «ліг» іранський інтернет // portaltele (https://portaltele.com.ua/news/events/cherez-kiberataki-lig-iranskij-internet.html). 11.02.2020).***

***

«Участники палестинского исламистского движения ХАМАС пытались взломать мобильные телефоны израильских солдат через приложения для флирта.

Как сообщается на сайте Армии обороны Израиля, начиная с января нынешнего года представители ХАМАС под видом привлекательных молодых девушек знакомились с солдатами в соцсетях Facebook, Instagram, а также мессенджерах WhatsApp и Telegram. Фотографии и персональные данные женщин были взяты с реальных аккаунтов.

Преступники от имени девушек отправляли текстовые и голосовые сообщения, предлагая загрузить по ссылке приложение для обмена фотографиями по типу Snapchat, которое на самом деле являлось вредоносной программой для

хищения данных с телефонов. Ссылки вели на три вредоносных приложения — Catch & See, ZatuApp и GrixyApp. Как сообщили в пресс-службе Армии обороны Израиля, данное вредоносное ПО было связано с серверами ХАМАСа, и по крайней мере один из профилей злоумышленников в социальных сетях уже использовался в предыдущих вредоносных кампаниях.

После установки приложения ХАМАС получал доступ к хранящейся на смартфоне информации, а само устройство начинало использоваться злоумышленниками для прослушки. Солдаты вовремя сообщили о подозрительной активности, что позволило армии и израильской службе внутренней безопасности Шабак пресечь действия преступников и предотвратить ущерб национальной безопасности страны…». ***(Флирт оказался опасным для израильских солдат // SecurityLab.ru (https://www.securitylab.ru/news/505110.php). 17.02.2020).***

***

«Кібератаку на міністерство закордонних справ Австрії, про яку вперше стало відомо ще 4 січня, здійснили за допомогою іноземних державних установ.

Про це 13 лютого заявив міністр закордонних справ Александр Шаленберг…

Шаленберг заявив, що IT-системи міністерства успішно очищені, "максимальна безпека даних" відновлена і що ніяких пошкоджень системи більше не виявлено.

Розслідування походження нападників, однак, триває. Міністерство поки що лише розкрило, що масштаб операції передбачає, що до неї був залучений державний суб'єкт…». ***(МЗС Австрії відновилося після кібератаки, підозрює іноземну державу // Європейська правда (https://www.eurointegration.com.ua/news/2020/02/14/7106382/). 14.02.2020).***

***

«Входящие в Европейский союз государства рассматривают возможность введения санкций в отношении некоторых структур и лиц в России и Китае в связи с их возможной причастностью к кибератакам.

…представители стран ЕС начнут обсуждение данной меры на этой неделе. Данный шаг станет первым применением так называемого режима киберсанкций ЕС — набора инструментов, включающего запреты на поездки и замораживание активов, предназначенного для предотвращения кибератак.

Для введения указанных санкций нужно согласие всех 27 членов ЕС. По словам источников, сначала будут проведены консультации с экспертами по кибербезопасности до того, как правительства стран ЕС подпишут конечное соглашение. Обсуждения могут продлиться около двух месяцев.

Получить согласие всех членов ЕС будет проблематично, поскольку власти некоторых стран не намерены портить отношения с Китаем или рассчитывают на нормализацию отношений с РФ, отметило издание». ***(ЕС может ввести санкции против причастных к кибератакам китайских и российских лиц // SecurityLab.ru (https://www.securitylab.ru/news/505423.php). 27.02.2020).***

***

«Правительства США и Великобритании опубликовали официальные заявления. в которых обвинили Россию в осуществлении координированной кибератаки на тысячи грузинских сайтов в октябре 2019 года.

Инцидент считается крупнейшей хакерской атакой на постсоветском пространстве. Неизвестные взломали сети как минимум одного хостинг-провайдера и осуществили дефейс 15 тыс. сайтов, в том числе правительственных, новостных, коммерческих и некоммерческих организаций. Злоумышленники опубликовали на них фото бывшего президента Грузии Михаила Саакашвили с надписью «I'll be back». Из-за взлома провайдера некоторые теле- и радиостанции не могли выйти в эфир.

Согласно заявлению США и Великобритании, за атакой стоит Россия. «США призывают Россию прекратить такое поведение в Грузии и где-либо еще. Стабильность киберпространства зависит от ответственной реакции нации», - заявил госсекретарь США Майк Помпео.

Министерство иностранных дел РФ незамедлительно отреагировало на обвинения и заявило о непричастности России к кибератаке.

«Россия не имеет к этому никакого отношения. Мы никуда не вмешиваемся и вмешиваться не собираемся», - заявил замминистра иностранных дел Андрей Руденко на встрече с журналистами». ***(США и Великобритания обвинили РФ в кибератаке на Грузию // SecurityLab.ru (https://www.securitylab.ru/news/505264.php). 21.02.2020).***

***

Створення та функціонування кібервійськ

«Исполнительный офис президента США запросил для Министерства обороны на 2021 год бюджет в $9,8 миллиардов. Эти деньги пойдут на проведение операций в цифровом пространстве и на реализацию мер кибербезопасности.

Соответствующую информацию можно найти на сайте Минобороны в документе под названием «DOD Releases Fiscal Year 2021 Budget Proposal»…». ***(Екатерина Быстрова. США планируют потратить на кибербезопасность в 2021 году $5,4 млрд // ООО «АМ-МЕДИА» (https://www.anti-malware.ru/news/2020-02-17-111332/31996). 17.02.2020).***

***

Кіберзахист критичної інфраструктури

«Всемирный экономический форум призвал повысить кибербезопасность авиаотрасли. Анализ показал, что лишь 3 крупнейших аэропорта проходят все тесты

Только у 3 из 100 крупнейших аэропортов мира хороший уровень кибербезопасности. У остальных 97 есть проблемы с веб-сайтом, мобильным приложением, «облаком», доступностью в «темном» интернете или утечкой кода, сообщает исследование ImmuniWeb.

Отчет о кибербезопасности показал следующее состояние основного веб-сайта аэропортов:

97% сайтов имеют устаревшее программное обеспечение;

24% сайтов содержат известные и используемые уязвимости;

76% сайтов не соответствуют европейскому закону о приватных данных GDPR;

24% сайтов не имеют шифрования SSL или используют устаревший SSLv3;

55% сайтов используют защиту файрвола веб-приложений.

Безопасность мобильных приложений аэропортов имеет такие проблемы:

100% приложений содержат как минимум пять внешних фреймворков;

100% мобильных приложений имеют минимум две уязвимости;

15 проблем безопасности в среднем имеет каждое приложение;

33,7% приложений не шифруют исходящий трафик.

Проблемы из-за «облаков», репозиториев кода и доступности в «темном» интернете:

66% аэропортов оголены в «темном» интернете;

72 из 325 таких случаев имеют высокий или критический риск, позволяя серьезные взломы;

87% аэропортов имеют утечки данных из публичных репозиториев кода;

503 из 3184 утечек имеют критический или высокий уровень;

3% имеют публичные «облака» с незащищенными чувствительными данными.

Только три из 100 крупнейших мировых аэропортов прошли все тесты на кибербезопасность:

аэропорт Амстердама Схипхол

аэропорт Хельсинки-Вантаа

аэропорт Дублина…». ***(Евгений Радченко. 97 из 100 крупнейших аэропортов имеют плохую кибербезопасность // Независимый Регион (https://nr2.com.ua/tehnologii/2020/02/08/97-iz-100-krypneishih-aeroportov-imeut-plohyu-kiberbezopasnost/). 08.02.2020).***

***

Захист персональних даних

«Через додаток Elector стався витік даних 6,5 млн виборців

В Ізраїлі стався найбільший в історії витік даних виборців через недоліки додатку партії "Лікуд", яку очолює прем'єр Біньямін Нетаньяху. Про це пише місцеве видання Haaretz.

Повідомляється, що "Лікуд" завантажив у додаток Elector повний реєстр ізраїльських виборців, і це призвело до витоку персональних даних майже 6,5 млн осіб. Інформація включає імена, номери посвідчень особи, адреси й стать кожного виборця, а також номери телефонів і інші особисті дані.

Розробник Elector вже повідомив, що вразливість у програмі була "одноразовим інцидентом, який вже усунуто". За даними Haaretz, вразливість

дозволяла будь-якому завантажити весь реєстр виборців. До цього відомий витік аналогічної величини стався у 2006 році, коли співробітник МВС Ізраїлю викрав реєстр населення і незаконно опублікував.

Вразливість полягає в тому, що у вихідному коді Elector зафіксовано імена користувачів і паролі, які дозволили зайти в систему і завантажити реєстр. На даний момент невідомо, скільки людей отримали доступ таким чином.

Додаток Elector є комп'ютеризованою системою управління виборами. Система дозволяє відправляти текстові повідомлення та управляти даними про виборців і ділянках…» ***(Партія Нетаньяху потрапила в скандал з найбільшим витоком даних виборців // РБК-Україна (https://www.rbc.ua/ukr/news/partiya-netanyahu-popala-skandal-krupneyshey-1581352299.html)/ 10/.02.2020).***

***

«Популярные почтовые приложения для iOS и Android извлекают данные из почтовых ящиков пользователей и затем продают созданные на основе этой информации продукты клиентам в сфере финансов, туризма и электронной коммерции, сообщило издание Motherboard. Ресурс провел исследование популярных программ Edison Mail, Foxintelligence Cleanfox и Rakuten Slice в попытке выяснить, какие данные они собирают.

На web-сайте почтового сервиса Edison Mail указывается, что программа «обрабатывает» электронные письма пользователей, однако компания не упоминает об извлечении данных из почтовых ящиков для дальнейшей продажи. По словам некоторых пользователей, компания могла бы быть более открытой относительно того, как использует полученные данные.

Edison является лишь одним из поставщиков бесплатных почтовых приложений, которые затем продают анонимные иди псевдонимизированные почтовые данные пользователей. Другой такой компанией является разработчик приложения для очистки входящих электронных писем Cleanfox Foxintelligence. Как сообщило издание, клиентами Foxintelligence является компания PayPal, консалтинговые гиганты Bain & Company и McKinsey & Company и пр.

«В прошлом мы пользовались услугами Foxintelligence для анализа туризма во Франции. Мы не использовали приобретенную информацию для других целей и больше не являемся ее клиентами», — сообщили представители европейского приложения Bolt, которое также было указано в качестве клиента под прежним названием Txfy.

Приложение Slice от Rakuten позволяет пользователям отслеживать покупки и отправляет уведомления об изменении цен на электронную почту. Как оказалось, программа извлекает информацию из почтовых ящиков пользователей, в том числе данные о приобретенных товарах у определенного бренда, а также уникальный идентификационный код для каждого покупателя. Как сообщило издание, цена за доступ к информации Rakuten в одной из категорий продуктов превышает $100 тыс.» ***(Популярные приложения извлекают данные из почтовых ящиков пользователей // SecurityLab.ru (https://www.securitylab.ru/news/504853.php). 11.02.2020).***

***

«Датское агентство по развитию и симплификации (Udviklings- og Forenklingsstyrelsen) обнаружило утечку данных, вызванную ошибкой в работе сервиса TastSelv Borger, которым управляет американская компания DXC Technology. Сервис TastSelv позволяет налогоплательщикам в Дании просматривать и изменять свои налоговые декларации, годовые отчеты и платить налоги.

Данные, в том числе персональные идентификационные номера (CPR-nummer), находились в открытом доступе на протяжении почти пяти лет, прежде чем была обнаружена утечка, сообщила датская телерадиокомпания Danmarks Radio.

Проблема содержалась в сервисе Tastselv Borger. Когда пользователи выбирали опцию «Исправить контактную информацию», ошибка в приложении приводила к отправке персональных идентификаторов на серверы Google и Adobe в виде части web-адреса.

Сервис Google Hosted Libraries предназначен для удаления всей информации, позволяющей идентифицировать пользователей перед входом в систему. Таким образом, никакая пользовательская информация не должна была передаваться компании Google в процессе. По словам агентства, утекшие данные были зашифрованы, и компании Google и Adobe не имели к ним доступ. Однако эксперт Питер Крузе (Peter Kruse) из компании CSIS пояснил, что Google имела доступ к 1,2 записей персональных иденификаторов, поскольку информация хранилась в незашифрованном виде.

DXC признала наличие уязвимости и исправила ее. Как сообщили представители компании, информация не была скомпрометирована.

Google Hosted Libraries (API библиотек Google) — сеть распространения контента и архитектура загрузки для самых популярных библиотек JavaScript с открытым исходным кодом». ***(1,2 млн идентификационных номеров жителей Дании оказались в Сети // SecurityLab.ru (https://www.securitylab.ru/news/504850.php). 11.02.2020).***

***

«Компания Twitter раскрыла подробности о кибератаках, в ходе которых посторонние лица использовали официальный API компании для сопоставления телефонных номеров с именами пользователей социальной сети.

Об инциденте стало известно 24 декабря 2019 года. Напомним, в тот же день исследователь безопасности Ибрагим Балич (Ibrahim Balic) обнаружил уязвимость в приложении Twitter для Android, эксплуатация которой позволила ему сопоставить 17 млн телефонных номеров с учетными записями в Twitter.

Вслед за этим компания обнаружила и немедленно приостановила работу крупной сети фейковых учетных записей, которые использовались для эксплуатации уязвимости в социальной сети. По словам Twitter, некоторые из IP-адресов, использованных во время атак, были связаны со спонсируемыми государством группировками. Особенной большой объем запросов поступал с IP-адресов в Иране, Израиле и Малайзии.

Эксплуатация осуществлялась через функцию загрузки контактов в приложении. При загрузке пользователем своего номера телефона система отправляла пользовательские данные. Функция загрузки контактов в Twitter не разрешает загружать список номеров в последовательном порядке во избежание злоупотребления.

Как отметила Twitter, данные атаки могли затронуть только тех пользователей соцсети, кто разрешил в настройках сопоставление по номеру телефона.» ***(Киберпреступники эксплуатировали уязвимость в API Twitter // SecurityLab.ru (https://www.securitylab.ru/news/504645.php0. 04.02.2020).***

***

«Підприємець опублікував інструкцію зі створення сайтів на платформі TON. Експерти застерігають про те, що там можуть створювати сайти для ведення протизаконної діяльності, а прослідкувати авторів таких ресурсів буде вкрай складно.

Команда Telegram Павла Дурова запустила інструмент TON Sites, який дозволяє створювати і отримувати доступ до сайтів в децентралізованої мережі TON (Telegram Open Network), повідомляється на сайті бета-тестування TON, передає Liga Tech.

У цій мережі сайти може створювати практично кожен.

В силу особливостей архітектури мережі, її користувачів значно складніше ідентифікувати. Передбачається, що обмежити доступ до сайту в ній теж буде непросто, пояснюють у виданні.

«З технічної точки зору сайти TON майже не відрізняються від звичайних веб-сторінок. Але доступ до них здійснюється за допомогою мережі TON, яка працює поверх інтернету — так звана оверлейна мережа. За таким самим принципом функціонують відомі проєкти анонімних тимчасових мереж на зразок I2P і Tor», — пише Liga Tech.

Подібні мережі залучають різну аудиторію: від анонімів до великих підпільних майданчиків, які займаються в тому числі протизаконною діяльністю, застерігають у виданні. Наприклад, сайти по торгівлі наркотиками чи зброєю.

До того ж, у популярній соцмережі Telegram, яку раніше створив Павло Дуров, є велика кількість каналів, які активно ведуть таку подібну діяльність. Такі канали регулярно викривають правоохоронні органи, проте їх точна кількість все ж залишається невідомою. Наприклад, ми недавно писали, що українські користувачі Telegram за допомогою бота заблокували понад 200 наркокрамниць.

Для доступу до існуючих і створення нових сайтів потрібні спеціальні шлюзи між «звичайним» інтернетом і мережею TON. ***(Засновник Telegram Павло Дуров запускає анонімний інтернет. Чому це небезпечно? // MEDIASAPIENS» (https://ms.detector.media/kiberbezpeka/post/24191/2020-02-11-zasnovnik-telegram-pavlo-durov-zapuskae-anonimnii-internet-chomu-tse-nebezpechno/). 11.02.2020).***

***

«За прошлый год злоумышленниками было украдено свыше 8,5 млрд записей, что в три раза больше, чем в 2018 году. Из-за проблем с

безопасностью и настройками облачных сервисов в 2019 году было совершено свыше 85% краж, что также значительно выше, чем за 2018 год, когда таких случаев было не больше половины.

Такие данные опубликованы в докладе X-Force Threat Intelligence Index 2020 о киберугрозах в 2019 году, подготовленном компанией IBM…

По данным доклада, общее количество взломов сократилось на 14%, однако при этом количество украденных данных за один случай возросло.

Так, в прошлом году почти три четверти случаев краж персональных данных раскрыли свыше 100 млн записей. В двух случаях счет шел на миллиарды украденных данных.

IBM пришла к выводу, что 60% взломов были осуществлены при помощи ранее украденных учетных данных и известных уязвимостей ПО. Это позволяло злоумышленникам меньше полагаться на обман пользователей, чтобы получить доступ к данным. Таким образом, количество фишинговых атак сократилось с половины от всех случаев взлома в 2018 году до 31% в 2019 году.

Использование уязвимостей ПО было причиной 30% взломов в прошлом году, что на 22% больше, чем в 2018 году. По данным IBM, давно известные уязвимости в Microsoft Office и Windows Server Message Block до сих пор успешно и масштабно эксплуатируются. Всего же в настоящее время известно о более чем 150 тыс. уязвимостях ПО.

В 29% случаев взломов были использованы ранее украденные учетные записи пользователей. Злоумышленники используют эти данные, чтобы сливаться с законным трафиком, что делает их обнаружение еще более сложным.

Атаки «грубой силы», когда взломщик подбирает пароль путем перебора всех возможных вариантов, составляют только 6% от всех кибератак в 2019 году. Выросло применение программ-стирателей, что в среднем стоит компаниям и государствам $239 млн за один случай — это в 60 раз больше, чем в среднем один случай взлома учетных записей. Такие программы часто используют государства на национальном уровне.

Вирусы-шифровальщики стали еще более распространены в 2019 году, а атаки с целью вымогательства поражают как общественный, так и частный сектор.

В прошлом году свыше 100 госслужб США подверглись атакам вирусов-шифровальщиков, в 80% случаев злоумышленники находили уязвимости в Windows Server Message Block, как это было в случае с WannaCry в 2017 году. В конце 2019 года чаще всего атаки производились новым вирусом под названием ZeroCleare. В банковской сфере среди вирусов были распространены TrickBot, Ramnit, Gozi и QaBot. Среди банковских вирусов рост появления новых программ составил 45%, среди других финансовых программ-вымогателей — 36%. В целом атаки с использованием программ-шифровальщиков стоили организациям свыше $7,5 млрд в 2019 году.

Спам также является повсеместной проблемой. В IBM выяснили, что чаще всего спам рассылают из США (26,5%), Франции (7,6%) и Нидерландов (6,3%). Россия в этом списке находится на четвертом месте с 6,1%. Самыми крупными получателями спама являются США (11,7%), Индия (6,4%) и Индонезия (5,9%).

Россия в этом списке также находится на четвертом месте с 5,8%. Большая часть (69,5%) всех рассылок представляла из себя зараженные ссылки.

Крупные технологические компании в 2019 году подверглись наибольшему количеству кибератак. На первом месте в этом списке Google, на который пришлось 39% угроз. Далее идет YouTube (17%), Apple (15%) и Amazon (12%). В десятку также входят Spotify, Netflix, Microsoft, Facebook, Instagram и WhatsApp.

В 2019 году финансовый сектор становился наиболее частой мишенью киберпреступников. Далее идут ритейл, транспортный сектор, СМИ, профессиональные онлайн-сервисы, правительства стран.

Если смотреть на географию направления всех кибератак, то на Северную Америку пришлось 44% всех угроз, на Азию — 22%, на Европу — 21%. На Ближний Восток были направлены 7% атак, на Южную Африку — 5%.» ***(Облачные сервисы являются причиной большинства утечек персональных данных // IKSMEDIA.RU (http://www.iksmedia.ru/news/5644556-Oblachnye-servisy-yavlyayutsya-pric.html). 12.02.2020).***

***

«Специалист компании Security Discovery Иеремия Фаулер (Jeremiah Fowler) обнаружил в открытом доступе базу данных косметической компании Estee Lauder, содержащую 440 336 852 записей.

«30 января я обнаружил не защищенную паролем базу данных, которая содержала огромное количество записей — 440 336 852. После дальнейшего изучения я смог увидеть связи с нью-йоркской косметической компанией Estée Lauder. Я мог получить доступ к журналам аудита, которые содержали большое количество адресов электронной почты в каждом документе», — сообщил специалист.

В архиве также содержалась техническая информация, включая IP-адреса, порты и пути, которые могли быть использованы злоумышленниками для сбора информации об инфраструктуре компании.

«В архиве также были миллионы записей, связанных с промежуточным программным обеспечением, которое использует компания Estee Lauder, в том числе управление данными, сервисы приложений, обмен сообщениями, аутентификация и управление API. Промежуточное ПО может создать дополнительный путь для вредоносного ПО, посредством которого приложения и данные могут быть скомпрометированы», — отметил эксперт.

В базе данных не хранилась информация о платежах или конфиденциальная информация о сотрудниках компании, однако остается неизвестным, как долго незащищенная база данных Estée Lauder находилась в открытом доступе или кто мог ею воспользоваться…». ***(440 млн записей компании Estee Lauder оказались в открытом доступе // SecurityLab.ru (https://www.securitylab.ru/news/504992.php). 12.02.2020).***

***

«Одна из крупнейших гостиничных сетей Лас-Вегаса была взломана, открыв доступ к персональным данным миллионов людей.

MGM Resorts пострадали от хакеров, о которых впервые сообщила ZDNet. Киберпреступники украли персональные и контактные данные 10,6 млн. гостей отеля, включая знаменитостей, сотрудников и государственных служащих. Среди полученной информации были полные имена, домашние адреса, номера телефонов, электронные письма и даты рождения.

Вероятно, что финансовая информация не была украдена во время атаки.

MGM Resorts имеет более 20 отелей по всему миру, но больше всего отелей расположено в Лас Вегасе, где ему принадлежит 13 точек, в том числе Белладжио, Мандалай Бэй, Ария, Вдара и Мираж.

Несмотря на то, что этот взлом является значительным, он все же меркнет в сравнении со взломом Marriott в 2018 году, когда в открытй доступ попали данные 500 млн. гостей.

Информация была размещена на хакерском форуме в понедельник. Неясно, какие отели пострадали от нападения, хотя одна новостная служба, которая отсканировала имена, заметила, что в данные была включена информация о Стивене Пэддоке, человеке, который 1 октября 2017 года открыл огонь из Mandalay Bay Resort, убив 58 человек.

«Прошлым летом мы обнаружили несанкционированный доступ к облачному серверу, который содержал ограниченный объем информации для некоторых предыдущих гостей MGM Resorts», - сказали в компании. «Мы уверены, что никакой финансовой информации, платежных карт или паролей в этом секторе не было. … MGM Resorts очень серьезно относится к защите персональных даннях своих гостей, поэтому мы усилили и повысили безопасность нашей сети, чтобы этого не повторилось».

MGM Resorts заявляет, что уведомляет пострадавших гостей «в соответствии с применимыми законами штата», но во многих штатах не требуется, чтобы жертвы были уведомлены, когда взломанная информация ограничивается такими данными, как адрес, номер телефона и т. д., возможно, взломщик, не подозревал, что они были включены…». ***(Романов Роман. Персональные данные более 10 млн. гостей крупной отельной сети украдены в результате хакерской атаки // InternetUA (https://internetua.com/personalnye-dannye-bolee-10-mln-gostei-krupnoi-otelnoi-seti-ukradeny-v-rezultate-hakerskoi-ataki). 20.02.2020).***

***

«Конфіденційність даних — це тільки ілюзія? Чи справді відстежувати нас в інтернеті може будь-хто? Як захистити особисту інформацію? Про це у книзі «Мистецтво залишатися непоміченим. Хто ще читає ваші імейли?» пише фахівець з кібербезпеки Кевін Митник.

В епоху розвитку технологій світ усе частіше переймається тим, що розвинені технології дозволяють вистежити буквально кожного. І це не конспірологія: глобальні компанії самі визнають, що кількість даних про людей в інтернеті зростає щодня. Певна конфіденційність у нас є, але часом це тільки ілюзія. Адже більшість із наявних у мережі особистих даних можна відстежувати буквально за хвилини. Часом це не означає нічого загрозливого, а ваші дані потрібні просто для того, щоб показувати вам рекламу. Та іноді їх можуть вкрасти,

оприлюднити на весь світ, взяти на вас кредит, продати ваші дані або вимагати за них винагороду.

Навіть якщо ви не знаменитість, алгоритми все одно вистежують, у який магазин ви ходили та що їли на сніданок. Добре це чи погано? Чи живемо ми в ілюзії конфіденційності? Чи справді за нами може шпигувати будь-хто, і якщо так, то які наслідки для нас це може мати? Як від цього захиститися? На ці та інші питання у своїй книзі «Мистецтво залишатися непоміченим. Хто ще читає ваші імейли?» дає відповіді колишній хакер Кевін Митник.

«У цій книжці колишній хакер Кевін Митник доступно розповідає, як залишатися непоміченим в інтернеті, дає поради, яких паролів краще не використовувати та як запобігти викраденню особистих даних. Кевін Митник — провідний консультант і спікер з питань кібербезпеки, колишній хакер та автор низки книжок. Засновник Mitnick Security Consulting, його клієнтами є компанії з Fortune 500 та інші», — йдетсья у описі книги.

MediaSapiens із дозволу видавництва «Наш Формат», де вийшла друком книга, публікує її уривок.

«Мистецтво залишатися непоміченим. Хто ще читає ваші імейли?»

Здавалося б, регулярні новини про витік даних та урядові «шпигунські» програми мають обурити нас до нестями. Здавалося б, події розгортаються так стрімко (за якихось кілька років), що свіжі рани мають спонукати нас протестувати на вулиці. Але все навпаки. Купа людей (і навіть деякі з тих, хто зараз читає цю книжку) уже певною мірою примирилися з тим, що за всіма нашими діями — телефонними дзвінками, повідомленнями, імейлами, активністю в соцмережах — можуть спостерігати.

І це розчаровує.

Можливо, ви не порушили жодних законів. Живете собі тихим, середньостатистичним життям, такі непримітні серед гігантського натовпу інтернет-користувачів. Але повірте мені: ви — не невидимка. Принаймні поки що.

Я обожнюю фокуси. І недарма: кажуть, що хакерові таки не завадить хоч якась спритність рук. Певно, усі бачили фокус зі зникненням предмета? Секрет у тому, що предмет насправді не зникає і не стає невидимим — він просто ховається десь на задньому плані: за завісою, у рукаві, у кишені. Бачимо ми його чи ні, він однак там.

Те саме відбувається і з купою особистих даних, які невпинно збираються і зберігаються, хоча ми цього навіть не помічаємо. Більшість із нас і гадки не має, як легко знайти цю інформацію і де її шукати. Ми її не бачимо, тож вважаємо себе невидимими для колишніх, батьків, навчальних закладів, начальників, навіть уряду.

Однак якщо знати, де шукати, можна знайти будь-яку інформацію. Про будь-кого.

Я часто виступаю з промовами. І байдуже, наскільки велика аудиторія: завжди є одна людина, яка намагається заперечити вищезгаданий факт. Якось після такого виступу сумніви висловила одна вкрай скептична журналістка.

Пам’ятаю, як ми сиділи за окремим столиком у барі готелю в одному американському мегаполісі. Саме тоді вона і заявила мені, що ніколи не була жертвою витоку даних. Через юний вік у неї майже нема майна на власне ім’я, а

отже, у реєстрах є мінімум записів. Вона ніколи не розголошує особистих даних у статтях і соцмережах — усе суто професійно. Вона вважала себе невидимкою. Тож я попрохав дозволу розшукати її номер соціального страхування та інші особисті дані в інтернеті. Хоча й неохоче, дівчина погодилася.

За тим самим столиком я зайшов на сайт для приватних детективів, до яких належу і я через свою роботу у сфері хакерських розслідувань у всьому світі. Я вже знав ім'я журналістки, тож спитав у неї лише адресу (хоча можна було і без цього: адресу легко знайти на іншому сайті). Уже за кілька хвилин я знав її номер соціального страхування, місто народження і навіть дівоче прізвище матері. Знав усі місця, з яких вона телефонувала додому, і всю історію її мобільних номерів. Дівчина шоковано втупилася в екран і врешті-решт визнала, що вся інформація більш-менш правдива.

Сайт, яким я скористався, доступний лише перевіреним компаніям чи особам. Щомісяця він стягує фіксовану, але невелику плату плюс додаткові витрати на пошук інформації. Також час від часу мене перевіряють стосовно законної мети для проведення конкретного пошуку. Але базову інформацію можна знайти фактично за копійки. І все це абсолютно законно.

Ви коли-небудь заповнювали онлайн-форму? Надсилали інформацію до школи чи іншого закладу, який зберігає її в інтернеті? Чи, може, подавали заяву на розгляд судової справи через сайт? Якщо так, то вітаю: ви добровільно передали особисту інформацію третій стороні, яка може робити з нею що завгодно. Існує ймовірність того, що деякі з цих даних (ба навіть усі) вже в мережі і доступні компаніям, які заробляють на тому, що збирають особисту інформацію по всьому інтернету. Установа Privacy Rights Clearinghouse називає понад 130 таких компаній, які мають на вас «досьє» (і байдуже, правдиве воно чи ні).

І не забувайте про дані, які ви в інтернет добровільно не завантажуєте, але які все одно зберігаються в архівах приватних та урядових компаній: інформація про те, кому ми пишемо чи телефонуємо, що шукаємо в мережі, що купуємо (як у звичайних, так і в інтернет-магазинах) і куди подорожуємо (хай там як: на машині чи пішки). Кількість даних на кожного з нас зростає з кожним днем у геометричній прогресії.

Вважаєте, що хвилюватися вам нічого? Повірте мені: дарма. Сподіваюся, що наприкінці книжки ви будете достатньо проінформовані й готові покласти цьому край.

Усі ми живемо з ілюзією конфіденційності. І жили так, мабуть, десятиліттями.

У певну мить нам стає некомфортно від того, який необмежений доступ до нашого особистого життя має уряд, робота, керівники, вчителі, батьки. Але позаяк цей доступ розширюється поступово, позаяк ми самі приймаємо кожну нову цифрову дрібницю без огляду на її втручання в приватне життя, повернути час назад стає дедалі важче. Тим паче, хто добровільно відмовиться від своїх електронних іграшок?

Небезпека цифрового спостереження полягає не в тому, що дані збирають (із цим ми мало що здатні зробити), а в тому, що з ними роблять опісля.

Уявіть, що надто завзятий прокурор може зробити з вашим товстим досьє необробленої інформації за кілька років. Дані, зібрані сьогодні (і часто поза контекстом), житимуть вічно. Навіть член Верховного суду США Стівен Браєр погоджується, що «важко здогадатися заздалегідь, які ваші слова чи дії видадуться (прокуророві) актуальними в контексті конкретного розслідування і коли». Інакше кажучи, ваше фото в нетверезому стані на фейсбуці — найменша з проблем.

Усе ще вважаєте, що вам нічого приховувати? Впевнені? В одній переконливій статті для журналу Wired відомий дослідник кібербезпеки Моксі Марлінспайк зазначає, що федеральним злочином у США може стати навіть дрібниця. Наприклад, звичайний невеличкий лобстер. «Байдуже, купили ви його в магазині чи хтось подарував, живий він чи мертвий, знайшли ви його після того, як той помер із природних причин, чи вбили під час самозахисту. Ви можете сісти у в'язницю через лобстера». Суть у тому, що існує купа незначних і маловідомих законів, які ви можете порушити, навіть про це не підозрюючи. А цифровий слід, що веде до доказів, доступний кожному всього в кілька кліків.

Конфіденційність — річ складна. Вона не є універсальною. В усіх нас різні причини якоюсь інформацією вільно ділитися з незнайомцями, а якусь залишати приватною. Може, ви просто не хочете, щоб друга половинка знала про вас кожну дрібницю. Може, хочете відокремити особисте життя від роботи. А може, дійсно боїтеся, що уряд за вами шпигує.

У кожного свій сценарій, тож жодна з порад у книжці не підійде на всі випадки життя. Позаяк наше ставлення до конфіденційності досить складне і, як наслідок, унікальне, ми зануримося в найголовніше — те, що зараз відбувається з таємним збором даних. А ви вже самі зможете вирішувати, що пасуватиме до вашої ситуації.

Як мінімум, ця книжка розкриє вам способи зберігання конфіденційності в цифровому світі і запропонує рішення, на які ви можете пристати чи не пристати. Оскільки конфіденційність — справа особиста, ступінь невидимості теж коливатиметься від людини до людини. Ця книжка доведе вам, що спостерігають абсолютно за кожним: вдома чи на вулиці, у кафе чи в машині по дорозі на роботу. Ваш комп'ютер, телефон, автомобіль, домашня сигналізація, навіть холодильник — усе це потенційні точки доступу до приватного життя.

Але не хвилюйтеся, я не збираюся лише лякати вас. Я також розповім, що робити з відсутністю конфіденційності, яка зараз уже стала нормою.

Книжка навчить вас:

• шифрувати і надсилати захищені імейли;
• захищати дані надійним паролем;
• приховувати реальну IP-адресу в публічних місцях;
• убезпечувати комп'ютер від стеження;
• захищати свою анонімність;
• тощо.

А тепер приготуйтеся опановувати мистецтво невидимості». ***(Як нас відстежують у мережі: уривок із книги колишнього хакера // MediaSapiens (https://ms.detector.media/knigi-pro-media/post/24269/2020-02-28-yak-nas-vidstezhuyut-u-merezhi-urivok-iz-knigi-kolishnogo-khakera/). 28.02.2020).***

***

«Нью-Йоркская компания Clearview AI, занимающаяся разработкой системы распознавания лиц, сообщила об утечке данных. В результате инцидента был скомпрометирован список клиентов компании, среди которых есть правоохранительные органы и даже ФБР, а также информация о количестве поданных ими запросов и зарегистрированных учетных записей. Как уверяют в компании, база данных, насчитывающая 3 млн изображений, в результате взлома не пострадала.

«К сожалению, утечки данных являются неотъемлемой частью жизни в 21 веке. Доступ к нашим серверам злоумышленники не получили. Мы исправили уязвимость и продолжаем работать над усилением безопасности», - сообщил юрист Clearview AI Top Экеланд (Tor Ekeland) изданию Daily Beast.

В заявлении компании не сказано, что утечка произошла в результате взлома. Тем не менее, инцидент может иметь неприятные последствия для правоохранительных органов, являющихся клиентами Clearview AI и полагающихся на нее как на надежный сервис. Clearview AI была создана в 2017 году, но широкой общественности о ней стало известно в прошлом месяце. По данным издания New York Times, компания создала ПО, «сканирующее» соцсети (в том числе Facebook и Twitter) в поисках фотографий людей для своей базы данных. Технология сразу же привлекла внимание правоохранительных органов, ФБР и Министерства внутренней безопасности США. В Сан-Франциско и других крупных американских городах полиции запрещено использовать данную технологию, однако в других местах правоохранители по-прежнему прибегают к Clearview AI в ходе расследований». ***(Разработчик нашумевшей системы распознавания лиц сообщил об утечке данных // SecurityLab.ru (https://www.securitylab.ru/news/505438.php). 27.02.2020).***

***

Кібербезпека Інтернету речей

«С развитием экосистем умного дома, растет и количество киберугроз для пользователей передовых бытовых приборов. Как оказалось, даже с помощью электролампы злоумышленники могут без особых сложностей взломать домашнюю сеть владельца такой электроники…

Согласно отчету компании Check Point, которая специализируется на вопросах кибербезопасности, под угрозой оказались владельцы популярных смарт-лампочек Philips Hue. Они подключаются к экосистеме умного дома на базе протокола Zigbee.

Обнаруженная уязвимость позволяет хакерам получить доступ к чужим компьютерам, используя ноутбук и несложное радиооборудование. Доступ осуществляется через концентратор, который объединяет различные приборы в локальную сеть…

Philips уже подтвердила наличие проблемы и выпустила специальный патч для фирменных осветительных приборов. При этом компания по умолчанию не обновляет прошивку умных ламп в автоматическом режиме – пользователям необходимо активировать функцию апдейта самостоятельно.

Список других устройств с поддержкой Zigbee – потенциально уязвимых для взлома – еще не опубликован.

Сообщается, что Amazon начала внутреннее тестирование собственной смарт-продукции, включая умные колонки Echo. О подготовке перехода на универсальный протокол ранее также сообщали Google и Apple». ***(Хакеры научились взламывать компьютеры через умные лампы: детали // Телеканал новостей «24» (https://24tv.ua/techno/ru/hakery_nauchilis_vzlamyvat_kompjutery_cherez_umnye_lampy_detali_n1276227). 06.02.2020).***

***

Кіберзлочинність та кібертероризм

«…26 січня 2020 року в авіакатастрофі загинув баскетболіст Кобі Брайант. Хакери, схоже, вирішили скористатися трагедією для поширення шкідників. Експерти з кібербезпеки Microsoft виявили, що під виглядом шпалер для робочого столу із зображенням спортсмена користувачі отримували шкідливий файл.

Про це фахівці розповіли в Twitter-акаунті Microsoft Security Intelligence. Шкідливий HTML-файл містить скрипт з криптовалютним майнером. Він призначений для видобутку токенів Monero (XMR).

Джерела також повідомляють, що скрипт містить згадку CoinHive – сервісу для видобутку криптовалюти, який вже закрився в березні 2019 року. Експерти Microsoft це поки не прокоментували.

«Поки світ оплакує втрату легенди NBA, кіберзлочинці, як і очікувалося, користуються цією трагедією». – пишуть вони в твіті». ***(Лужна Софія. Хакери скористалися загибеллю баскетболіста для поширення вірусу // TechnoPortal.com.ua (https://technoportal.com.ua/programi/41091). 02.02.2020).***

***

«Кибератаки на российские компании случаются в два раза чаще, чем в среднем по миру. К такому выводу пришли в компании Check Point.

За последние шесть месяцев российские организации были атакованы в среднем 893 раза в неделю, тогда как в мире этот показатель равен 465, следует из документа. По данным Check Point, основными источниками киберугроз для России выступают отечественные (39%) и американские (30%) хакеры. Среди путей нападения лидирует электронная почта — через нее было получено 86% вредоносных файлов. При этом 42,8% подобных файлов, детектированных в России, упаковывались в формат .exe, тогда как в мире основная часть (47,7%) была в формате .doc.

По подсчетам Check Point, 13% атак на российские компании приходятся на крипотомайнер XMRig, который используется для создания криптовалюты Monero, 12% атак исходят от похитителя паролей AgentTesla, который отслеживает и собирает данные с клавиатуры жертвы.

В мире на них приходится примерно в два раза меньшая доля атак — 7% и 6% соответственно.

Статистика атак на Россию сильно зависит от методики сбора данных и того, как классифицируются те или иные атаки, отмечает бизнес-консультант по безопасности Cisco Systems Алексей Лукацкий. Еще несколько лет назад Россия не была в топе стран, которую атаковали, но зато была в топе стран, с чьих IP-адресов атаки проводились, напоминает он. Факт учащения атак на российские организации вызывает вопросы, потому что обычно хакеры атакуют богатые организации или богатых людей, но Россия здесь не является кандидатом номер один, заключает господин Лукацкий.

Интернет не имеет границ, поэтому количество кибератак массовым вредоносным софтом будет примерно одинаковым для всех стран, указывает ведущий аналитик «Лаборатории Касперского» Сергей Голованов.

«Если, например, говорить про майнеров, то, по статистике «Лаборатории Касперского», Россия примерно в середине по доле атакованных устройств», — отмечает он.

Зато при этом количество инцидентов в финансовых организациях России за последние пять лет значительно сократилось, подчеркивает Сергей Голованов. По его словам, после всплеска атак в 2013–2016 годах в сфере финансов существенно улучшили системы защиты, поэтому злоумышленники переключились на другие страны.

«Например, в январе мы видели, что русскоговорящие злоумышленники Silence переключились на африканские страны», — рассказал аналитик.

Сегодня атаки на российские банки в целом обходятся хакерам дороже, чем атаки на иностранные финансовые организации, говорит и вице-президент группы InfoWatch Рустэм Хайретдинов. Руководитель CERT Group-IB Александр Калинин объясняет это тем, что многие хакерские группировки — русскоязычные и они долгое время тестировали инструменты и схемы целевых атак именно на российских банках, от которых те в итоге научились успешно защищаться.

Стоит отметить, что киберпреступники предпочитают скрытый майнинг…» ***(Исследование: скрытые майнеры предпочитают российские компании // «LetKnow OÜ (https://letknow.news/news/issledovanie-skrytye-maynery-predpochitayut-rossiyskie-kompanii-36390.html). 06.02.2020).***

***

«Маастрихтский университет, который в декабре 2019 года стал жертвой кибератаки, заплатил хакерам выкуп – 197 тысяч евро.

Об этом в комментарии корреспонденту Укринформа в Гааге сказал представитель Маастрихтского университета Фонс Эльберсен.

"Я могу подтвердить, что Маастрихтский университет заплатил выкуп в размере 30 биткоинов, то есть 197 тысяч евро", – сказал он.

Эльберсен также отметил, что после долгих дискуссий университет решил заплатить злоумышленникам ради студентов и преподавателей.

В ходе расследования стало известно, что хакеры в течение двух месяцев собирали данные и информацию университета, в частности, имена пользователей, пароли учетных записей. После исследования специалисты компании FOX-IT предоставили университету рекомендации относительно лучшей защиты.

Свой отчет и рекомендации специалисты компании FOX-IT предоставили университету 5 февраля 2020 года.

Отмечается, что жертвой кибератаки Маастрихтский университет стал 23 декабря 2019 года и уже на следующий день обратился к специалистам с FOX-IT.

Маастрихтский университет в свою очередь заявил, что в настоящее время работает над повышением цифровой безопасности.

Ранее нидерландский NOS сообщал, что не исключают, что за кибератакой могут стоять российские хакеры.

На сегодняшний день Маастрихтский университет эту информацию не подтверждает.

…опасное программное обеспечение попало в Маастрихтский университет в декабре 2019 года, сделав компьютерные файлы недоступными с целью, чтобы жертва атаки заплатила хакерам.» ***(Университет в Нидерландах после кибератаки заплатил выкуп 30 биткоинов // Новости онлайн 24 (https://newsonline24.com.ua/universitet-v-niderlandax-posle-kiberataki-zaplatil-vykup-30-bitkoinov/). 07.02.2020).***

***

«Кибернападение на МИД Австрии: хакеры искали документы, связанные с политикой ЕС.

Целью хакеров, которые в январе совершили мощное кибернападение на МИД Австрии, могли быть документы, связанные с политикой ЕС.

Об этом сообщает австрийский портал Futurezone со ссылкой на информированный источник.

"3 января 2020 года была выявлена кибератка на IT-систему австрийского МИД. Вебсайты не были затронуты, поскольку нападавшие были сфокусированы на другом, как сейчас стало известно. Просочились первые указания на мотив: Futurezone узнал от хорошо информированного источника, что во время кибератаки имел место целенаправленный поиск документов, связанных с политикой ЕС", - говорится в сообщении.

Отмечается, что имеются в виду документы, которые формулируют позиции Еврокомиссии, Европарламента и отдельных стран ЕС по определенным вопросам.

"Особый интерес для злоумышленников представляют документы, касающиеся позиции Австрии в отношении других стран", - добавляет Futurezone.

Вместе с тем спикер МИД Петер Гушельбауер в ответе на запрос по этому поводу заявил: "Прошу отнестись с пониманием, что мы не можем рассуждать по поводу злоумышленников и мотива".

В министерстве также заверили, что работа над "решением проблемы" – ликвидацией шпионского программного обеспечения – "идет полным ходом"…»

(Стало известно, что искали хакеры в МИД Австрии // Телеграф (https://telegraf.com.ua/mir/europa/5331729-stalo-izvestno-chto-iskali-hakeryi-v-mid-avstrii.html). 03.02.2020).

***

«Специалисты из компании IBM опубликовали ежегодный анализ угроз «IBM X-Force Threat Intelligence Index 2020», демонстрирующий изменения в методах киберпреступников за последний год.

Согласно исследованию, 60% первичных проникновений в инфраструктуру жертвы были осуществлены при помощи ранее украденных учетных данных и известных уязвимостей в ПО. Таким образом, в 2019 году в качестве первоначального метода проникновения фишинг использовался в 31% случаев, тогда как в 2018 году данная цифра достигала почти 50%.

По словам специалистов, в 29% случаев злоумышленники использовали ранее украденные учетные данные. Только в 2019 году было скомпрометировано более 8,5 млрд записей, что на 200% больше по сравнению с предыдущим годом. По результатам исследования, 39% сотрудников компаний применяли один и тот же пароль для нескольких учетных записей, а 28% вовсе не меняли свои пароли. Подобная тенденция вместе с растущим количеством утечек данных дают преступникам возможность проводить масштабные атаки.

Как отметили эксперты, компании продолжают сталкиваться с проблемами безопасности облачных сервисов. Из более чем 8,5 млрд взломанных записей в 2019 году 7 млрд (более 85%) были связаны с неправильной настройкой облачных серверов и других систем.

Банковские трояны, как, например, TrickBot, стали чаще использоваться для проведения масштабных вымогательских кампаний. Шифровальщики и новые коды, которые используют банковские трояны, возглавили рейтинг новых вредоносных программ, появившихся в прошлом году. Новый вредоносный код был замечен в 45% банковских троянов и в 36% шифровальщиков.

Вместе с некоммерческой организацией Quad9 специалисты IBM отметили усиливающуюся тенденцию в сфере фишинга: преступники выдают себя за крупные потребительские бренды, пользующиеся наибольшим доверием пользователей и подделывают ссылки на их сайты с целью фишинга. В числе наиболее крупных брендов, используемых в мошеннических схемах оказались, такие компании, как Google, YouTube и Apple. 6 из 10 наиболее часто используемых мошенниками брендов относились к доменам Google и YouTube. Бренды Apple (15%) и Amazon (12%) также использовались мошенниками для хищения данных пользователей.

Facebook, Instagram и Netflix также вошли в десятку наиболее подделываемых брендов, но со значительно меньшей долей использования.» ***(Мошенники стали чаще выдавать себя за крупные бренды // SecurityLab.ru (https://www.securitylab.ru/news/504859.php). 11.02.2020).***

***

«Киберпреступники организовали фишинговую кампанию, нацеленную на пользователей Android-устройств, в ходе которой заражают смартфоны и планшеты банковским трояном Anubis. Вредонос способен украсть финансовую информацию из более чем 250 банковских программ и приложений для шопинга.

Злоумышленники отправляют жертвам фишинговые письма со встроенной ссылкой, которая загружает замаскированный под счет-фактуру APK-файл. Когда ссылка на электронную почту открывается с Android-устройства, происходит загрузка APK-файла. После открытия файла пользователю якобы предлагается включить «Google Play Protect», но вместо этого пользователь дает приложению все необходимые разрешения, одновременно отключая защитный сервис.

Оказавшись на Android-устройстве, Anubis начинает собирать информацию об установленных приложениях и сравнивает результаты со списком целевых программ. Anubis в основном нацелен на банковские и финансовые приложения, но также ищет популярные программы для покупок, такие как приложения eBay или Amazon.

Как только Anubis обнаруживает необходимую программу, он заменяет оригинальное окно авторизации на поддельное, чтобы похитить учетные данные пользователя.

В ходе анализа вредоноса специалисты из компании Cofense обнаружили, что банковский троян обладает различными функциями, включая захват скриншотов, отключение и изменение настроек администрирования, отключение встроенной защиты Google Play Protect, запись звука, совершение звонков и отправка SMS-сообщений, доступ к контактам в адресной книге, получение команд от операторов через Telegram и Twitter, управление устройством через систему удаленного доступа к рабочему столу VNC и пр.

Вредоносное ПО также содержит кейлоггер, способного перехватывать нажатия клавиш из любого приложения, установленного на скомпрометированном Android-устройстве. Однако сначала данный модуль должен быть активирован операторами с помощью команды с C&C-сервера.

Anubis также может шифровать файлы во внутреннем хранилище и на внешних дисках с помощью специального модуля-вымогателя, добавляя расширение .AnubisCrypt к зашифрованным файлам и отправляя их на C&C-сервер.» ***(Киберпреступники заражают Android-устройства банковским трояном Anubis // SecurityLab.ru (https://www.securitylab.ru/news/504806.php). 07.02.2020).***

***

«Десятки принадлежащих ООН серверов были скомпрометированы через известную уязвимость в SharePoint. Об этом сообщается в конфиденциальном отчете, с которым ознакомился известный ИБ-эксперт Кевин Бомон (Kevin Beaumont).

По словам Бомона, точкой входа для кибератаки стала уязвимость CVE-2019-0604 в платформе для совместной работы SharePoint от Microsoft. Уязвимость позволяет выполнить произвольный код в контексте пула приложения SharePoint и

учетной записи сервера SharePoint. Microsoft выпустила исправления для нее в феврале, марте и апреле прошлого года.

Первый PoC-эксплоит для уязвимости был опубликован обнаружившим ее исследователем безопасности Маркусом Вульфтанге (Markus Wulftange) в марте 2019 года, и вскоре в Сети стали появляться эксплоиты от других разработчиков. В мае того же года ИБ-эксперты зафиксировали массовые атаки на серверы SharePoint.

Атаки на гуманитарные организации ООН в Женеве и Вене имели место в середине июля, но были обнаружены лишь спустя месяц. Руководство приняло решение не сообщать сотрудникам о компрометации их данных и лишь попросило сменить пароли. Об атаке было известно только служащим IT-отделов и руководителям гуманитарных организаций ООН. Широкой общественности о случившемся стало известно лишь на этой неделе.

Через уязвимую установку SharePoint злоумышленники проникли в компьютерные сети организаций ООН в Вене, а затем, вооружившись привилегиями администратора и перемещаясь по сети, получили доступ к системам в организациях в Женеве.» ***(Кибератака на ООН была осуществлена через уязвимость в SharePoint // SecurityLab.ru (https://www.securitylab.ru/news/504608.php). 02.02.2020).***

***

«Зловмисники запускають з різних акаунтів у YouTube відео, де обіцяють компенсувати «злив» у мережу персональних даних. Гроші продовжують виманювати до тих пір, доки людина не запідозрить, що це обман.

На початку 2020 року в мережі почали поширювати відео з інформацією про те, що нібито будь-який громадянин може швидко отримати від $ 50 до $ 3000 на свою карту. Кошти користувачам мають виплатити нібито за те, що їх персональні дані «витекли» в мережу з вини американських компаній, таких як Facebook, WhatsApp і інших.

Багато українців досі вірять в «безкоштовний сир» і клацають на рекламу з гучними обіцянками. Насправді це шахраї, які таким чином крадуть гроші у довірливих громадян, попереджають журналісти.

Видання Ain.ua пояснило, як працює ця шахрайська схема.

Як влаштоване шахрайство

На YouTube публікують відео. Голос за кадром, який представляється програмістом з Санкт-Петербурга на ім'я Євген Миронов. Він обіцяє пояснити, як лише за 15 хвилин отримати від $ 50 до $ 1500 на картку банку. Наразі відео, помітив MediaSapiens, має майже 800 тисяч переглядів.

«Зазвичай я записую відео тільки про програмування, але сьогодні особливий випадок», — запевняє шахрай.

Гроші обіцяють виплатити всім користувачам, чиї персональні дані нібито були скомпрометовані в інтернеті. А виплачує їх недавно заснована організація в США, яка займається розподілом компенсаційних виплат, пише видання.

На відео навіть показують сайт цієї організації, виконаний в стилі урядових порталів США. Весь текст на ньому — англійською, що має викликати довіру. Але при переході на сайт для «зручності» українських користувачів вам видасть російськомовну версію сторінки.

Під відео нібито вдячні користувачі залишають безліч схвальних коментарів та пишуть, що все «прекрасно» працює.

«Автор маніпулює фактами, призводить скріншоти про витоки з реальних новин, а на обкладинці відео — нібито сюжет телеканалу «1 + 1» про можливість отримати компенсацію від Федерального уряду. Під роликами — безліч вдячних коментарів від користувачів, які нібито отримали гроші», — йдеться у статті.

Таких відео в мережі багато. Той самий ролик поширюють по YouTube з різних акаунтів. Їх також активно рекламують в мережі.

Докладний розбір цієї схеми опублікував Telegram-канал під назвою badlistua, що займається викриттям шахраїв в українському сегменті інтернету.

Користувача просять зайти на сайт, вказати свої дані, а потім система прорахує суму компенсації для вашого конкретного випадку. Сума може бути від $ 300 до кількох тисяч. Щоб отримати їх, досить просто натиснути на кнопку.

Платіж нібито вже сформований і готовий до відправки. Але в певний момент система видає «помилку», тому що у вас немає SSN-номера (номер соціального страхування), який є обов'язковим атрибутом кожного громадянина США, SSN використовується для податкового і пенсійного обліку, по суті це американський ІПН. Зрозуміло, у користувачів з України, Росії та інших країн його бути не може. І тут користувачам пропонують отримати цей «важливий документ» за символічні 5-10 доларів.

При цьому неясно, чи використовують шахраї персональні дані користувачів, які вони самі ж добровільно вводять в формі заради розрахунку компенсації: ПІБ і платіжні реквізити. Але сервіс «розрахунку» прекрасно працює, навіть якщо ввести в форму випадковий набір букв, йдеться у публікації. Така схема з минулого року діє і в Росії. Там, пише автор каналу, всього за тиждень шахраї виманили у росіян більше $ 2500.

Що ж робити?

Точні збитки від шахрайської схеми, у яку вірять немало користувачів, невідомі. Та гроші у цій схемі будуть виманювати, доки людина не зрозуміє, що це насправді обман.

«Незважаючи на те, що багато хто вже знає про схему, довірливі люди все ще трапляються. Якщо ви стали жертвою шахраїв, зверніться до правоохоронних органів. Проінформуйте якомога більше друзів і знайомих про існування такої схеми. І перестаньте вірити в подібні способи «заробітку» в інтернеті. Безкоштовний сир буває тільки в мишоловці», — наголошують у статті Ain.ua.» ***(Шахраї обіцяють українцям понад $ 2000 «компенсації» за витік персональних даних // MEDIASAPIENS (https://ms.detector.media/manipulyatsii/post/24174/2020-02-06-shakhrai-obitsyayut-ukraintsyam-ponad-2000-kompensatsii-za-vitik-personalnikh-danikh/). 06.02.2020).***

***

«На початку року в мережі Інтернет було розповсюджено відео, в якому розповідається, що кожен громадянин, зареєструвавшись на відповідному американському сайті, може отримати компенсацію за виток його персональних даних з вини американських компаній.

Співробітники кіберполіції проаналізували роботу даного сайту з інформацією про виплату компенсацій та встановили, що він має явні ознаки шахрайського.

Окрім цього, спеціалісти кіберполіції під час огляду сайту виявили, що перевірка персональних даних на предмет їхнього витоку взагалі не відбувається.

Так, якщо заповнити поля для перевірки будь-якими вигаданими даними, все одно буде запропоновано виплату для компенсації. Для її виплати необхідно отримати тимчасовий SSN номер (номер соціального страхування). Для цього пропонується сплатити грошові кошти за допомогою форми оплати від платіжного сервісу E-PAY. Слід зазначити, що даний сервіс створений для країн СНД.

Також зазначимо, що державні органи при виявленні подібних порушень притягають до відповідальності або накладають штрафні санкції, які стягуються до бюджету країни, а не пропонують одразу сплатити компенсацію потерпілим.

З огляду на вищевикладене, Департамент кіберполіції Національно поліції України закликає користувачів мережі Інтернет бути уважними та відмовитись від таких операцій на подібних сайтах. Крім цього, під час переказу коштів радимо користуватися перевіреними та відомими платіжними системами.

Якщо ви все ж таки стали жертвою шахраїв, зверніться до нас з відповідною заявою, заповнивши форму зворотного зв'язку на нашому сайті https://ticket.cyberpolice.gov.ua.» ***(Кіберполіція перевірила ресурс, на якому обіцяють грошову винагороду за виток даних // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-pereviryla-resurs-na-yakomu-obiczyayut-groshovu-vynagorodu-za-vytok-danyx-4995/). 11.02.2020).***

***

«Киноновинки привлекают внимание не только обычных зрителей, но и злоумышленников, которые часто маскируют под их видом вредоносного ПО. «Лаборатория Касперского» проанализировала, как часто названия девяти фильмов, которые были номинированы на «Оскар-2020», использовались фишерами и авторами зловредов в прошлом году.

Всего по миру эксперты обнаружили более 20 фишинговых сайтов, которые заманивали пользователей возможностью бесплатно посмотреть громкие премьеры 2019 года, и ещё 925 вредоносных файлов, связанных с названиями этих фильмов.

С помощью фишинговых сайтов, на которых предлагается посмотреть новинки бесплатно, злоумышленники собирали личные и финансовые данные пользователей.

Кроме того, эксперты подсчитали количество вредоносных файлов, соответствующих двум условиям: они появились в течение четырёх недель после официальных премьер каждого из девяти указанных фильмов и включали в себя их названия. Выяснилось, что наибольшей популярностью у злоумышленников

пользовались «Джокер» (304 вредоносных файла), «1917» (215 вредоносных файлов) и «Ирландец» (179 вредоносных файлов).

«Злоумышленники следят за актуальными трендами, в том числе в киноиндустрии. Они расставляют свои ловушки как незадолго до громкой премьеры, так и вскоре после неё, на пике зрительского интереса. Чтобы избежать возможных рисков, мы советуем любителям кино пользоваться только официальными стриминговыми платформами», — комментирует Антон Иванов, антивирусный эксперт «Лаборатории Касперского».

Чтобы не получить на устройства зловред вместо фильма, «Лаборатория Касперского» рекомендует пользователям:

проверять официальные даты кинопремьер и не доверять предложениям увидеть фильм до того, как он вышел в прокат;

проверять расширение файла перед тем, как его скачать: это может быть .avi, .mkv или .mp4, но ни в коем случае не .exe;

использовать надёжное защитное решение для всесторонней защиты от киберугроз». ***(Как злоумышленники использовали названия киноновинок в зловредах в 2019 году // IKSMEDIA.RU (http://www.iksmedia.ru/news/5644511-Kak-zloumyshlenniki-ispolzovali-naz.html). 12.02.2020).***

***

«Команда исследователей Check Point Research, подразделение Check Point Software Technologies ведущего поставщика решений в области кибербезопасности по всему миру, опубликовала свой новый отчет о брендах, которые наиболее часто используются в попытках фишинга за 4 квартал 2019. Злоумышленники чаще всего имитировали бренды, чтобы украсть личную информацию или учетные данные пользователей в течение последнего квартала — именно он содержит самое большое количество распродаж в течение года.

При фишинговых атаках злоумышленники пытаются создать сайт-копию официального сайта известного бренда, используя доменное имя или URL-адрес, дизайн веб-страницы, аналогичные подлинному сайту. Ссылка на фальшивый веб-сайт может быть отправлена жертвам по электронной почте или в сообщениях, перенаправлена во время просмотра веб-страниц или запущена из фальшивого мобильного приложения. Поддельный веб-сайт часто содержит форму, предназначенную для кражи учетных данных пользователей, платежных реквизитов или другой личной информации.

Топ брендов, которые злоумышленники пытались использовать в попытках фишинга в 4 квартале 2019 года:

Ранжируются по количеству их общих появлений в попытках фишинга:

1. Facebook (18% фишинговых атак в мире)
2. Yahoo (10%)
3. Netflix (5%)
4. PayPal (5%)
5. Microsoft (3%)
6. Spotify (3%)
7. Apple (2%)

8. Google (2%)
9. Chase (2%)
10. Ray-Ban (2%)

Топ способов распространения фишинговых сообщений

В течение четвертого квартала исследователи наблюдали различия в распространении фишинговых страниц: каждая категория брендов распространялась по-своему. Например, через мобильные устройства в основном распространялись фишинговые страницы социальных сетей и банков. Через электронную почту, как правило, распространялись фишинговые письма, приуроченные к периоду распродаж, например таких, как черная пятница в ноябре 2019 года.

Электронная почта (27% всех фишинговых атак в 4 квартале)

1. Yahoo!
2. Rbs (Ray-Ban Sunglasses)
3. Microsoft
4. DropBox

Веб-сайты (48% всех фишинговых атак в 4 квартале)

1. Spotify
2. Microsoft
3. PayPal
4. Facebook

Через мобильные устройства (25% всех фишинговых атак в 4 квартале)

1) Chase Mobile Banking
2) Facebook
3) Apple
4) PayPal

«Киберпреступники используют разные способы атак, чтобы обманом заставить своих жертв ввести личную информацию, учетные данные или перевести деньги. Часто ссылки на фишинговые сайты приходят через спам, но иногда злоумышленники, получив учетные данные пользователя, тщательно изучают жертву в течение нескольких недель и работают над целенаправленной атакой на партнеров, клиентов компании от лица своей жертвы для кражи денег, — рассказывает Василий Дягилев, глава представительства Check Point Software Technologies в России и СНГ. — Такой способ позволяет хакерам замаскироваться под доверенное лицо. За последние два года количество атак такого типа возросло, и в 2020 году фишинг по-прежнему будет представлять серьезную угрозу».

Отчет Check Point Phishing Report основан на данных ThreatCloud intelligence, самой большой совместной сетью по борьбе с киберпреступностью, которая предоставляет данные об угрозах и тенденциях атак из глобальной сети датчиков угроз. База данных ThreatCloud содержит более 250 миллионов адресов, проанализированных на предмет обнаружения ботов, более 11 миллионов сигнатур вредоносных программ и более 5,5 миллионов зараженных веб-сайтов, а также ежедневно идентифицирует миллионы типов вредоносных программ». ***(Facebook чаще всего используется для фишинговых атак // IKSMEDIA.RU***

(http://www.iksmedia.ru/news/5643820-Facebook-chashhe-vsego-ispolzuetsya.html). 07.02.2020).

***

«В ушедшем году зафиксированы три новых типа DDoS-атак, увеличился средний размер ботнета, злоумышленники все чаще используют для организации вторжений уязвимости в устройствах интернета вещей.

«По нашим оценкам, общее количество распределенных атак, направленных на отказ в обслуживании (Distributed Denial of Service, DDoS), за 2019 год выросло примерно в полтора раза», – констатировал технический директор компании Qrator Labs Артем Гавриченков. Наиболее атакуемые индустрии – платежные системы, электронная коммерция и беттинг (ставки на исход спортивных матчей и иных событий). Банки теряют свою привлекательность для преступников благодаря широкому применению средств защиты, хотя число DDoS-атак на них по-прежнему велико. Лидерами по росту числа атак стали платежные системы (+187%) и криптосервисы (+487%).

Новации в DDoS-атаках

В 2019 году были выявлены новые типы DDoS-атак с использованием техники amplification («усиление», когда атакующий от имени жертвы отправляет поддельный запрос, в ответ на который жертва получает значительно большее количество данных и вынуждена потом разгребать образовавшиеся завалы). Такие распределенные атаки, направленные на отказ в обслуживании, проводят даже школьники. Но в минувшем году были зафиксированы атаки на основе TCP-амплификации (реплицированный SYN/ACK-флуд). Возможность задействования протокола TCP для проведения масштабных атак типа amplification впервые была описана в исследовательской работе немецких ученых пять лет назад, но до прошлого года оставалась лишь теорией.

Атаки с запросами на подключение по протоколу TCP привели в августе 2019 года к недоступности ряда хостингов по всему миру. Трафик амплификации SYN/ACK достигал пиковых значений в 208 млн пакетов в секунду, а наиболее длительный период атаки с непрерывной бомбардировкой «мусорным» трафиком составил 11,5 ч.

При таких атаках метод защиты путем сброса всего UDP-трафика, который позволяет справиться с большей частью атак с использованием амплификации, часто не помогает нейтрализовать вектор SYN-ACK. Требуются комплексные меры защиты, которые небольшим интернет-компаниям реализовать нелегко.

Другие новые способы организации DDoS-атаки, появившиеся в 2019 году: эксплуатация уязвимости в Web.Services.Discovery и сервисе удаленного управления компьютерами Apple (Apple ARMS), позволившая достигнуть коэффициента амплификации 35,5.

DDOS-атаки можно разделить на три класса. Атаки нижнего уровня (L2–L3 модели OSI) осуществляются за счет исчерпания полосы пропускания. Если представить канал как водопроводную трубу, пропускающую ограниченное количество воды, то труба забивается злоумышленником. На среднем уровне (L4–L6) атакуются криптографические и транспортные протоколы, создаются

проблемы в инфраструктуре, некоторые узлы которой даже не контролируются оператором связи (СОРМ). На высоком уровне (L7) организуются узкие места в сайтах, платежных системах и мобильных приложениях.

Чаще атакуют нижний и верхний уровень, подобно тому, как в многоквартирном доме самые обворовываемые этажи – первый и последний. Особенность прошедшего года – рост DDoS-атак на СМИ, сайты которых нередко имеют слабую защиту от этого вида угроз. Причем атаки идут преимущественно на высоком уровне (L7).

Все больше устройств под чужим контролем

Средний размер управляемой преступниками сети (ботнета) вырос на 20%. Во многом это обусловлено использованием устройств с не обновляемым ПО, например, старых мобильных телефонов, и с распространением интернета вещей.

Так, недавно сообщалось об обнаружении встроенного бэкдора в платах, программируемых китайской компанией Xiongmai, которые многие бренды устанавливают в системах видеонаблюдения. В такой системе удаленный доступ к видеорегистратору можно получить, подключившись через интернет с помощью логина root и одного из шести опубликованных паролей. Программа организации DDoS-атаки, эксплуатирующая этот бэкдор, выложена на GitHub. Как правило, компании объясняют такие уязвимости халатностью разработчиков, забывших убрать фрагменты отладочного кода». ***(Николай НОСОВ. Число DDoS-атак продолжает увеличиваться // IKSMEDIA.RU (http://www.iksmedia.ru/articles/5644178-Chislo-DDoSatak-prodolzhaet-uvelich.html). 10.02.2020).***

***

«Офіційні Twitter-акаунти Олімпійських ігор та Міжнародного олімпійського комітету було зламано. Про це компанія повідомила в пресрелізі…

У повідомленні Twitter ідеться про те, що акаунти зламали через сторонню платформу, однак не уточнили деталей.

«Щойно нам стало відомо про проблему, ми заблокували скомпрометовані акаунти і наразі тісно працюємо з нашими партнерами, аби відновити їх», — ідеться в заяві.

Окрім того, речник Міжнародного олімпійського комітету повідомив, що відомство окремо розслідує інцидент.

У заяві Twitter не вказано, хто причетний до зламу акаунтів. Утім hromadske бачило повідомлення на одному зі зламаних акаунтів до того, як його видалили (посилання). Там згадувалася хакерська група OurMine. Раніше вона була причетна до «зламів» акаунтів відомих осіб у соціальних мережах.

Крім того, про злам своїх акаунтів у Twitter повідомив і футбольний клуб «Барселона». У повідомленні також зазначається причетність до інциденту OurMine. У 2017 році гакери вже зламували акаунти клубу.

Про OurMine відомо небагато. Як повідомляв Business Insider, вона складається з трьох осіб і базується в Саудівській Аравії. OurMine заявляють, що зламують акаунти для того, щоб перевірити їхню захищеність. Якщо гакерам

вдається це зробити, то вони залишають в акаунті «жертви» повідомлення, де закликають перейти на їхній сайт і перевірити свою кібербезпеку.

Зокрема, OurMine вдалося свого часу зламати акаунти Марка Цукерберга, Джимі Вейлза, ютубера Pewdiepie тощо. У 2017 році OurMine зламали сайт «Вікілікс». ***(Олег Павлюк. Офіційні Twitter-акаунти Олімпійських ігор (і не тільки) зламали. Ми знаємо, хто саме // Громадське Телебачення (https://hromadske.ua/posts/oficijni-twitter-akaunti-olimpijskih-igor-i-ne-tilki-zlamali-mi-znayemo-hto-same). 16.02.2020).***

***

«Судоходная отрасль стала мишенью новой группы хакеров, которые рассылают на электронные ящики письма с файлами с якобы важной информацией о коронавирусе и тем самым заносят вирус в компьютер получателя.

По данным калифорнийских специалистов по кибербезопасности «Proofpoint», в письмах содержится вредоносный документ «Microsoft Word».

Когда получатель открывает прикрепленный файл, на его компьютер устанавливается AZORult – вредоносное программное обеспечение. Оно может красть различные пользовательские данные (информацию из файлов, пароли, куки, историю браузеров, банковские учетные данные и информацию о криптовалютных кошельках).

Специалисты подчеркнули, что угрозе подвержены все компьютеры, на которых Microsoft Office не обновлялся с ноября 2017 года.

Всем компаниям и экипажам торговых судов рекомендуют с предельной осторожностью относиться к любым электронным сообщениям, ссылкам и вебсайтам, которые в том числе касаются коронавируса.

В «Proofpoint» подчеркнули:

«Злоумышленники прекрасно понимают экономические проблемы, связанные с коронавирусом. Срывы поставок в связи с распространением болезни окажут негативное влияние на судоходные компании, и те, кто стоит за атаками, хорошо знают, какие побочные последствия это будет иметь для индустрии. Это демонстрирует не только их техническую, но и экономическую искушенность». ***(Дмитрий Одесский. Хакеры заражают суда документом с информацией о «коронавирусе» // Одесса-Главная https://odessanews.net/news/xakery-zarazhayut-suda-dokumentom-s-informaciej-o-koronaviruse/). 17.02.2020).***

***

«Киберпреступники атаковали крупнейшую в Хорватии нефтяную компанию INA Group. В ходе кибератаки злоумышленники, предположительно, использовали вымогательское ПО CLOP, зашифровавшее данные некоторых внутренних серверов компании, сообщило издание ZDNet.

Данный инцидент не затронул поставки бензина клиентам и не повлиял на работоспособность платежных систем компании. Однако в результате атаки компания не смогла выставлять счета-фактуры, фиксировать использование карт

лояльности, выпускать новые мобильные ваучеры и новые электронные виньетки, а также принимать от клиентов оплату за топливо.

Хотя INA Group не раскрыла подробностей о том, какое вредоносное ПО использовалось в атаках, предполагается, что речь идет о вымогательском ПО CLOP. О причастности вымогателя свидетельствует несколько факторов. В частности, за несколько часов до того, как INA Group опубликовала заявление об инциденте, аналитик из компании Sophos сообщил о начале активности нового C&C-сервера, используемого в кибератаках CLOP. Кроме того, на этой неделе исследователи безопасности обнаружили новые версии вымогателя CLOP на сервисе VirusTotal…». ***(Преступники атаковали крупнейшую в Хорватии нефтяную компанию // SecurityLab.ru (https://www.securitylab.ru/news/505288.php). 21.02.2020).***

***

«Одно из оборонных агентств США, обеспечивающее безопасность коммуникаций для президента США Дональда Трампа, сообщило о возможной компрометации своих компьютерных систем. В результате инцидента могли пострадать номера социального страхования и другая персональная информация сотрудников, сообщило издание Reuters.

Агентство оборонных информационных систем (Defence Information Systems Agency, DISA) США разослало электронные письма людям, чьи персональные данные могли быть скомпрометированы в период с мая по июль 2019 года в результате инцидента. В письмах не указывается, какая часть сети DISA была скомпрометирована или кто мог быть причастен к утечке. Белый дом не прокомментировал данный инцидент.

«DISA провела тщательное расследование этого инцидента и приняла соответствующие меры по защите сети», — сообщил представитель агентства Чарльз Причард (Charles Prichard).

DISA обеспечивает прямую телекоммуникационную и IT-поддержку президенту, вице-президенту Майку Пенсу, их сотрудникам, Секретной службе США, председателю Объединенного комитета начальников штабов и другим старшим военнослужащим». ***(Оборонное агентство США сообщило о возможной утечке данных // SecurityLab.ru (https://www.securitylab.ru/news/505268.php). 21.02.2020).***

***

«Вымогатели рассылают владельцам web-сайтов, использующих рекламный сервис Google AdSense, письма с угрозами и требованием выкупа. Неизвестные угрожают с помощью ботов сгенерировать фейковые просмотры баннеров и таким образом спровоцировать блокировку сайта, сообщил KrebsOnSecurity.

«Очень скоро вы получите предупреждающее уведомление на панели управления вашей учетной записи AdSense! Мы собираемся наполнить ваш сайт огромным количеством сгенерированного ботами прямого web-трафика со 100% показателем отказов и тысячами IP-адресов — кошмар для любого пользователя

AdSense. Мы настроим наших ботов так, чтобы они в бесконечном цикле с различной продолжительностью открывали каждый баннер AdSense, который запускается на вашем сайте», — сообщается в письме от злоумышленников

Увеличение трафика за счет фейковой активности грозит владельцам сайтов установлением лимита на показ рекламы и возвращением дохода рекламодателю, а также полной блокировкой аккаунта сайта в сервисе.

В одном из случаев преступники потребовали $5000 в биткойнах и начали осуществлять свои угрозы — количество недействительного трафика AdSense на ресурсе одного из пользователей за последний месяц существенно возросло.

Компания Google отказалась комментировать данную ситуацию и призвала пользователей игнорировать любые сообщения с требованием выкупа, а также сообщать о подобных случаях представителям компании». ***(Злоумышленники угрожают пользователям рекламного сервиса AdSense // SecurityLab.ru (https://www.securitylab.ru/news/505181.php). 19.02.2020).***

***

«Киберпреступники атаковали оператора газопровода и заразили его компьютерные сети вымогательским ПО. Агентство по кибербезопасности и безопасности инфраструктуры (CISA) США не указало название оператора, но поделилось подробностями кибератаки. Злоумышленники использовали фишинговую ссылку для получения первоначального доступа к информационным компьютерным сетям организации, а затем нацелились на OT-сеть (Operational Technology).

После получения доступа к OT-сети преступники загрузили вымогательское ПО, зашифровали данные одновременно в IT- и OT-сетях для нанесения максимального ущерба, и только потом потребовали выкуп.

Вымогательское ПО не затронуло программируемые логические контроллеры (ПЛК), напрямую взаимодействующие с заводским оборудованием. По словам специалистов, данные других промышленных процессов, таких как человеко-машинные интерфейсы (HMI), программы Data Historian и серверов опроса, не могли быть прочитаны, что привело к частичной потере работоспособности персонала на объекте.

В качестве меры предосторожности оператор трубопровода решил осуществить «преднамеренное и контролируемое прекращение работы». Остановка длилась приблизительно два дня, после чего нормальные операции были возобновлены.

Как отметили представители CISA, преступник не получил возможность контролировать или манипулировать промышленными операциями, поскольку жертва отключила ЧМИ. Американские чиновники не раскрыли название вида вымогательского ПО». ***(Вымогатели атаковали американского оператора газопровода // SecurityLab.ru (https://www.securitylab.ru/news/505178.php). 19.02.2020).***

***

«Японские оборонные подрядчики Pasco Corporation (Pasco) и Kobe Steel (Kobelco) сообщили о взломе компьютерных систем, которые произошли в мае 2018 года, а также в июне 2015 года и августе 2016 года соответственно.

Поставщик спутниковых данных Pasco и крупнейший производитель стали Kobelco подтвердили несанкционированный доступ к их внутренней сети во время двух инцидентов, а также заражение вредоносными программами, затронувшими их вычислительные системы после атак.

Согласно официальному заявлению компании Pasco, в ходе проведения расследования не было обнаружено каких-либо утечек данных.

Однако Pasco и Kobelco далеко не единственные связанные с Министерством обороны компании, которые стали жертвами кибератак. Напомним, ранее японский гигант в сфере информационных технологий и производства электроники NEC подвергся многочисленным кибератакам, в результате которых было похищено почти 27 тыс. файлов, включая документы, связанные с контрактами Минобороны страны.

А в прошлом году злоумышленники скомпрометировали переписку Mitsubishi Electric с представителями Министерства обороны и Агентства по ядерному регулированию, а также документы, относящиеся к совместным проектам с частными фирмами, в том числе с коммунальными предприятиями, железнодорожными операторами, автопроизводителями и операторами связи.

В компаниях предполагают, что за данными кибератаками могут стоять китайские киберпреступные группировки, такие как Tick и BlackTech.» ***(Киберпреступники атаковали японских оборонных подрядчиков Pasco и Kobelco // SecurityLab.ru (https://www.securitylab.ru/news/504779.php). 07.02.2020).***

***

Вірусне та інше шкідливе програмне забезпечення

«В компании по кибербезопасности Kaspersky заявляют о том, что многие PDF-файлы, документы и видео, которые содержат рекомендации по защите от коронавируса, на самом деле являются скрытыми троянами и вредоносным ПО… Таких пока насчитали не больше десятка, но эксперты по кибербезопасности не исключают увеличения их количества.

В компании обращают внимание на то, что по Интернету распространяется много информации о заболевании коронавирусом с сообщением о том, как себя обезопасить от заражения. Эти файлы на самом деле являются троянами и вредоносными программами, которые маскируются с помощью заголовков о коронавирусе.

"Коронавирус, который широко обсуждается как важная новость, уже использовался киберпреступниками как приманка. До сих пор мы видели только 10 уникальных файлов, но поскольку такого рода деятельность часто происходит с популярными темами в СМИ, то мы ожидаем, что эта тенденция может возрасти.

Поскольку люди продолжают беспокоиться за свое здоровье, мы можем видеть все больше и больше вредоносных программ, скрытых внутри поддельных

документов о распространении коронавируса ", - заявляет аналитик Kaspersky Антон Иванов.

Он также сообщает о том, что в подобных сообщениях кроются трояны, вымогатели и другие вредные черви, которые способны блокировать устройство, копировать и редактировать данные на устройстве или даже воровать их из папок пользователя.

Эксперты компании по кибербезопасности Kaspersky определили наиболее популярные вредоносные файлы и советуют обратить внимание на следующие:

Worm.VBS.Dinihou.r,
Worm.Python.Agent.c,
DangerousObject.Multi,
Worm.WinLNK.Agent. gg,
Worm.WinLNK.Agent.ew,
Trojan.WinLNK.Agent.gen,
Trojan.PDF.Badur.b.» ***(Ольга Калинина. Kaspersky: PDF-файлы, документы и видео с информацией по защите от коронавируса используют хакеры // Зоряный (https://zoryanyy.tv/articles/technology/kaspersky_pdf_fayly_dokumenty_i_video_s_informatsiey_po_zashchite_ot_koronavirusa_ispolzuyut_khakery/). 03.02.2020).***

***

«Антивирусные компании довольно часто публикуют статистику касаемо количества зараженных устройств. Подобный отчет недавно представили специалисты ESET. В нем содержится много интересного, хотя бы то, что 99% всех вирусов в мире заражают Android-смартфоны. Кстати, статистику заражений системы iOS также раскрыли.

Касаемо мобильной операционки Android, такое положение вещей не удивительно, учитывая масштабы ее популярности. Однако специалисты называют ее – идеальной целью для кибератак. Причины этого обозначены три:

положительная динамика роста числа пользователей;
обширный комплекс сервисов экосистемы;
устаревшие патчи безопасности (в 90% гаджетов Android они неактуальные).

Довольно интересно выглядит статистика обнаруженных вредоносов в географическом выражении. Так, наибольшее количество вирусов в 2019 году обнаружили в России – 15,2% от общемирового показателя. За ней последовали Иран (14,7%) и Украина (7,5%). Стоит заметить, что Google активно борется с проблемой, что подтверждается фактом. Сравнивая общее количество обнаруженных вирусов в 2018 году с 2019 годом, заражений стало на 9% меньше.

Теперь расскажем о системе iOS. В целом, она безопаснее Android, но зарегистрированные случаи вредоноса с каждым годом увеличиваются. Допустим, сопоставив показатели 2018 года с 2019-м, вирусы чаще заражали систему на 98%. А если сопоставить аналогичные данные 2017 года с прошлым – это увеличение составило целых 158%. Географическое заражение iOS-гаджетов от общего числа таково – 44% приходится на китайских пользователей, 11% устройств в США и 5% в Индии.

Подытожили специалисты ESET тем, что новые виды угроз появляются довольно редко. То есть, злоумышленники пользуются «старыми тропами», которые антивирусными компаниями изучены достаточно глубоко.» ***(В Украине и России самый большой показатель заражения Android-систем вирусами // ProstoMob (https://prostomob.com/15708-v-ukraine-i-rossii-samyj-bolshoj-pokazatel-zarazheniya-android-sistem-virusami). 01.02.2020).***

***

«Специалисты из компании Binary Defense обнаружили и проанализировали вредоносную программу, которая способна распространять троянское ПО Emotet через близлежащие беспроводные Wi-Fi сети и компрометировать подключенные компьютеры.

Напомним, в сентябре нынешнего года Emotet вернулся к жизни после 4 месяцев бездействия. Операторы отправляли электронные письма, содержащие вредоносные файлы и ссылки на вредоносные загрузки. Жертвами кампании стали пользователи, говорящие на польском и немецком языках.

По словам исследователей, теперь у Emotet есть еще один более опасный способ распространения, который позволяет ему проникать в другие сети Wi-Fi и компрометировать компьютеры в них.

После заражения компьютера, подключенного к Wi-Fi сети, вредонос использует wlanAPI для обнаружения любых ближайших сетей Wi-Fi.

«Даже если данные сети защищены паролем, необходимым для подключения, вредоносная программа попробует подобрать из списка возможных вариантов правильный, и в случае успеха подключает зараженный компьютер к сети. Затем вредоносное ПО сканирует сеть на предмет компьютеров под управлением Windows с включенным общим доступом к файлам. Вредонос добывает список всех учетных записей пользователей на этих компьютерах и пытается взломать их методом брутфорса. Если пароль подобран правильно, вредоносная программа копирует себя на данный компьютер и запускает процесс установки с помощью удаленной команды на другом компьютере», — пояснили эксперты.

Затем вредонос посылает запрос C&C-серверу для подтверждения установки.

Как отметили эксперты, основной исполняемый файл Worm.exe, который вредоносная программа использует для распространения по беспроводной сети, имеет временную метку, относящуюся к апрелю 2018 года. Файл впервые был загружен на VirusTotal в мае того же года. Он содержал встроенный IP-адрес C&C-сервера, который использовал Emotet. Предположительно, подобное распространение вредоноса через Wi-Fi сеть тайно осуществляется в течение почти двух лет.» ***(Emotet распространяется через слабо защищенные сети Wi-Fi // SecurityLab.ru (https://www.securitylab.ru/news/504816.php). 10.02.2020).***

***

«Эксперты из ИБ-компании TrapX Security предупредили о новой вредоносной кампании, нацеленной на крупных производителей, которые используют подсистемы Windows 7 для запуска конечных точек IoT-

устройств. Преступники используют самораспространяющееся вредоносное ПО из семейства Lemon Duck.

Операторы вредоноса атакуют IoT-устройства и используют их для добычи криптовалюты Monero с помощью инструмента XMRig. Исследователи предупреждают, что интенсивный процесс майнинга негативно сказывается на работе оборудования и вызывает сбои работе, а также подвергает устройства проблемам безопасности, приводит к нарушению цепей поставок и потере данных.

В каждом из описанных исследователями случае злоумышленники эксплуатировали уязвимости в Windows 7 в качестве отправной точки. Напомним, 14 января корпорация Microsoft официально прекратила техническую поддержку операционной системы Windows 7. Microsoft больше не будет предоставлять техническую поддержку по любым вопросам, обновления программного обеспечения, а также обновления и исправления системы защиты, поэтому безопасность устройств под управлением данной операционной системой находится под угрозой.

«Образец вредоносного ПО, проанализированный TrapX, является частью семейства Lemon Duck. Вредонос сканировал сеть на предмет потенциальных целей, в том числе с открытыми сетевым протоколом SMB (порт 445) или системой управления реляционными базами данных MSSQL (порт 1433). Найдя потенциальную цель, вредоносная программа запускала несколько модулей с различными функциями», — пояснили исследователи.

Одна из таких функций включала брутфорс-атаки для взлома сервисов и дальнейшей загрузки и распространения вредоносных программ через SMB-протокол или MSSQL. Другая включала «запуск invoke-mimikatz через import-модуль для получения NTLM-хэшей и дальнейшей загрузки и распространения вредоносного ПО через SMB-протокол».

Как отметили эксперты, вредоносное ПО Lemon Duck сохранило персистентность на зараженных системах с помощью запланированных задач, которые включали PowerShell-скрипты, вызывавшие дополнительные Lemon Duck PowerShell-скрипты для установки XMRig.» ***(Операторы вредоносного ПО Lemon Duck атаковали IoT-производителей // SecurityLab.ru (https://www.securitylab.ru/news/504769.php). 06.02.2020).***

***

«Злоумышленники используют сервис для web-хостинга проектов и их совместной разработки Bitbucket для хранения семи типов вредоносного ПО, используемого в ходе вредоносной кампании. По данным компании Cybereson, преступники уже заразили 500 тыс. компьютеров по всему миру. Жертвы данной вредоносной кампании были заражены множеством полезных нагрузок, в том числе инфостилерами, майнерами криптовалюты и вымогательским ПО STOP.

Злоумышленники создали несколько учетных записей на Bitbucket для размещения вредоносного программного обеспечения и постоянно обновляют его. Специалисты из компании Cybereason выяснили, что в ходе кампании распространяется следующее вредоносное ПО: инфостилеры Predator, Vidar и Azorult; загрузчик Evasive Monero Miner для многоэтапного майнера XMRig;

вымогатель STOP с открытым исходным кодом; троян Amadey; программа IntelRapid для похищения криптовалюты.

Регулярные обновления, а также использование защитных программ Themida и CypherIT в качестве упаковщика помогают вредоносам избегать обнаружения.

По словам экспертов, целью злоумышленников являются пользователи, загружающие взломанные версии коммерческого программного обеспечения, такого как Adobe Photoshop, Microsoft Office и пр. Программы-приманки содержали инфостилеры Azorult и Predator the Thief — первый собирал необходимые данные, а второй устанавливал соединение с Bitbucket, чтобы загружать дополнительные вредоносные программы.» ***(Преступники заразили с помощью сервиса Bitbucket более 500 тыс. копьютеров // SecurityLab.ru (https://www.securitylab.ru/news/504733.php). 06.02.2020).***

***

«Киберкомандование США обнародовало подробности о шести новых вредоносных инструментах из арсенала северокорейской хакерской группировки Lazarus (она же Hidden Cobra). По мнению американских властей, данное вредоносное ПО применяется в новой фишинговой кампании, направленной на кражу денежных средств.

Список инструментов включает «полнофункциональный RAT» BISTROMATH. загрузчик под названием SLICKSHOES. вредонос CROWDEDFLOUNDER. служащий для распаковки бинарного кода трояна для удаленного доступа в памяти, полнофункциональный имплант HOTCROISSANT для «рекогносцировки, загрузки/выгрузки файлов и выполнения команд», имплант ARTFULPIE для загрузки DLL-библиотек, а также инструмент BUFFETLINE. применяемый для загрузки/выгрузки, удаления и выполнения файлов, доступа к интерфейсу командной строки Windows, создания и завершения процессов.

Кроме прочего, ведомство обновило данные о бэкдоре HOPLIGHT. информация о котором была обнародована в прошлом апреле…» ***(Опубликованы новые данные об инструментах APT- группы Lazarus // SecurityLab.ru (https://www.securitylab.ru/news/505101.php). 16.02.2020).***

***

«Вредоносное ПО Xhelper продолжает заражать Android-устройства и способно возвращаться даже после удаления или сброса настроек до заводских.

Впервые исследователи обнаружили Xhelper в марте 2019 года. На тот момент функционал вредоносного ПО был относительно простым, и его основной функцией было посещение рекламных страниц с целью монетизации. С тех пор большинство приложений безопасности для Android-устройств добавили функцию обнаружения xHelper, но оказалось, что избавиться от вредоноса не так просто.

По словам специалистов из компании Malwabytes, xHelper распространяется не в составе предварительно установленного вредоносного ПО, содержащегося в прошивке, а использует магазин Google Play для повторного заражения после полной перезагрузки устройства или очистки с помощью антивирусного ПО. Как

предполагают эксперты, вредонос только создает видимость того, что источником заражения является Google Play, тогда как на самом деле установка осуществляется из другого места.

В ходе анализа файлов, хранящихся на скомпрометированном Android-смартфоне одной из жертв, было обнаружено, что троянский загрузчик был встроен в APK, расположенный в каталоге com.mufc.umbtts.

Специалистам пока не удалось выяснить, каким образом Google Play используется для инфицирования. Пользователям рекомендуется отключить магазин Google Play, а затем запустить сканирование устройства антивирусной программой. В противном случае вредоносное ПО продолжит возвращаться, несмотря на удаление с устройства». ***(«Неудаляемый» троян Xhelper вновь заражает Android-устройства // SecurityLab.ru (https://www.securitylab.ru/news/505082.php). 14.02.2020).***

***

«Сотрудники Dr. Web, занимающиеся кибербезопасностью, изучали приложения Google Play и обнаружили в них присутствие не удаляемого Android-вируса. Вредоносная программа распространяется в нескольких модификациях. Когда на смартфоне загружается приложение, происходит ее установка. Оператор, запустивший вирус, зарабатывает на программах, которые берут деньги за установку.

Действие второй версии трояна более опасно. Из-за нее происходит заражение приложений и сбор данных владельца гаджета – контактных номеров, паролей и другой информации.

Данную вирусную программу разработали под операционной системой Android 5.1 и ее предыдущими версиями.

Их доля в общем количестве пользователей Android превышает 25%. Dr. Web не может даже приблизительно определить, сколько гаджетов заражено этим трояном на сегодняшний день, но в компании подчеркивают, что вероятность инфицирования 25% устройств и выше вполне обоснованная.

Этот хищник заразил уже четверть всех смартфонов мира

Согласно уточнению специалистов, Android.Xiny.5260 никуда не денется из гаджета, даже если удалить с него зараженные приложения. Единственным способом избавления от трояна, по мнению экспертов Dr. Web, может стать полная перепрошивка операционной системы Android, но только в том случае, если будут использованы официальные источники.

В начале 2020 г. от компании, которая разрабатывает антивирусное программное обеспечение, можно было получить информацию о наиболее вредоносных приложениях для гаджетов. Каталог Google Play был исследован экспертами, которые нашли там около восемнадцати программ запуска рекламы, перегружающей процессор и способствующей тому, что аккумулятор гаджета быстро разряжается…». ***(На Android появился бессмертный вирус-убийца: как уберечься от напасти // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/361420-***

na_android_pojavilsja_bessmertnyj_virus-ubijtsa_kak_uberechjsja_ot_napasti). 26.02.2020).

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Житель Пенсильвании Дэвид Букоски (David Bukoski) был приговорен к пяти годам лишения свободы условно за управление сервисом по осуществлению заказных DDoS-атак.

Как сообщает журналист Брайан Кребс, Quantum Stresser работал как минимум с 2012 года и насчитывал порядка 80 тыс. подписчиков. В 2018 году с помощью сервиса было осуществлено порядка 50 тыс. кибератак по всему миру. Его сайт (quantumstress[.]net) вместе с четырнадцатью другими сервисами был ликвидирован в ходе международной правоохранительной операции в декабре 2018 года.

Поскольку Quantum Stresser является одним из старейших сервисов подобного рода, из-за долгой безнаказанности 24-летний Букоски по-видимому потерял бдительность и попался на мелочной ошибке – заказал любимую пиццу с беконом и курицей с того же электронного адреса, на который был зарегистрирован сервис.

По данным прокуратуры Аляски, электронный адрес Букоски был внесен в черный список несколькими компаниями, чьими услугами он пользовался для рекламы своего сервиса и получения платежей. Письма, отправленные Букоски с требованием объяснить причины внесения его в черный список, помогли правоохранителям установить его настоящее имя, а заказ пиццы на дом раскрыл домашний адрес…». ***(Заказ на пиццу выдал местоположение оператора одного из старейших DDoS-сервисов // SecurityLab.ru (https://www.securitylab.ru/news/504770.php). 06.02.2020).***

***

«Региональный отдел по борьбе с организованной преступностью в Уэст-Мидлендсе (Великобритания) выпустил плакат, в котором рекомендует родителям обратиться к сотрудникам правоохранительных органов, если их ребенок установил на персональном компьютере ОС Kali Linux, виртуальную машину, браузер Tor, ПО Metasploit или мессенджер Discord, сообщило издание The Register.

«Если вы обнаружили что-либо из данного списка на своем компьютере или если у вас есть ребенок, которого вы подозреваете в киберпреступных действиях, дайте нам знать, чтобы мы могли дать совет и рассказать им о более позитивных способах развлечений», — указывается на плакате.

Наряду с логотипом управления Уэст-Мидлендса на памятке также находится логотип Национального агентства по борьбе с преступностью (National Crime Agency, NCA) Великобритании. Как заявили в Twitter представители ведомства, NCA не имеет никакого отношения к производству данного плаката.

«Существует много инструментов, которые могут использовать дети с развитыми техническими навыками. Некоторые из которых могут использоваться как в легальных, так и в незаконных целях, поэтому очень важно, чтобы родители и дети знали, как данные инструменты можно безопасно использовать», — ответили в ведомстве.

Сотрудники WMROCU пока не прокомментировали данную ситуацию». ***(Использующих Kali Linux и Tor детей предложили «сдавать» полиции // SecurityLab.ru (https://www.securitylab.ru/news/505096.php). 14.02.2020).***

***

«К солидной коллекции открытых ею способов извлекать информацию из компьютера, физически изолированного от Сети, неутомимая команда Лаборатории кибербезопасности Университета Бен-Гуриона (Израиль) добавила ещё один. На этот раз исходящие двоичные данные кодируются в незаметных для невооруженного глаза колебаниях яркости экрана ПК.

Для создания «скрытого оптического канала» в изолированный компьютер нужно внедрить вредоносное ПО, управляющее яркостью ЖК-монитора. После этого, злоумышленник может сделать видеозапись дисплея скомпрометированного компьютера, используя локальную камеру наблюдения, встроенную камеру смартфона или веб-камеру, и затем может восстановить отфильтрованную информацию с применением методов обработки изображений.

На выложенном 6 февраля видео продемонстрировано извлечение с компьютера через экран текста книги «Винни-Пух и все, все, все» Александра Милна.

Как и большинство атак на компьютер с «воздушным зазором» (air-gapped), способ, описываемый в статье Мордехая Гури (Mordechai Guri), Димы Буковски (Dima Bykhovsky) и Йувала Эловичи (Yuval Elovici), имеет в основном академическое значение — его нельзя отнести к числу эффективных или практичных.

Тем не менее, авторы публикации на сервере arXiv предложили несколько мер для противодействия данной угрозе, таких как запрет на размещение и использование любых камер внутри охраняемого периметра или применение поляризационной накладки на экран, уменьшающей его видимость на больших расстояниях». ***(Утечка данных с ПК возможна через манипуляции яркостью экрана // Компьютерное Обозрение (https://ko.com.ua/utechka_dannyh_s_pk_vozmozhna_cherez_manipulyacii_yarkostyu_jekrana_131851). 10.02.2020).***

***

«Как всем известно, 14 января 2020 года компания Microsoft официально прекратила поддержку всем полюбившейся операционной системы Windows 7. Поддержка «семерки» прекращается из-за ее уязвимости перед киберугрозами…

Такое рано или поздно случается со всей продукцией компании, в связи с ее устареванием – например, поддержка Windows XP, которую пользователи с любовью называли «Хрюша» была прекращена спустя 13 лет после ее выпуска – в 2014 году.

Прекращение поддержки означает, что Microsoft больше не будет заниматься обновлением программного обеспечения «семерки», обновлением и исправлением безопасности. Пользоваться Windows 7 можно и без обновления, однако это сопряжено с повышенным риском киберугроз.

В Microsoft рассказали, что решение о прекращении поддержки «семерки» принято из-за того. Что она была разработана более десяти лет назад, когда еще не существовало современных киберугроз. В то же время, основная на сегодняшний день операционная система, Windows 10, была разработана в соответствии с современным развитием технологий. Компания сосредотачивает внимание на поддержке «десятки» и рекомендует всем пользователям обновить свои компьютеры до нее. В компании намекают, что, возможно, для такого обновления понадобится купить и новые, более современные компьютеры, ведь Windows 10 более требовательна к ресурсам, чем ее предшественница.

В то же время, разработчики некоторых программ, специализирующиеся на кибербезопасности, объявили о том, что будут продолжать разрабатывать программы для «семерки» вплоть до 2022 года. Таким образом, с помощью неофициальной поддержки, сторонники Windows 7 смогут пользоваться любимой операционной системой еще два года…» ***(Компания Microsoft расстроила фанатов // Ukrainianwall.com (https://ukrainianwall.com/society/26441-kompaniya-microsoft-rasstroila-fanatov). 04.02.2020).***

***

«Специалисты израильского Университета имени Бен Гуриона изобрели новый метод хищения данных с инфицированных, но физически изолированных компьютеров, не требующий подключения к сети или физического доступа к устройству. Как пояснили исследователи, новая техника основана на отслеживании невидимых глазу небольших изменений в яркости ЖК-экрана.

Для этой цели они создали скрытый оптический канал, который может использоваться даже в том случае, если пользователь работает за компьютером. Метод работает следующим образом: вредоносное ПО на скомпрометированном компьютере извлекает важные данные (пароли, файлы, изображения, ключи шифрования и т. д.), кодирует их, а затем модулирует информацию в виде сигналов «0» и «1». Далее атакующий использует незаметные глазу изменения в яркости экрана для модуляции двоичной информации в виде подобному морзе кода.

«В ЖК-экранах каждый пиксель представляет собой комбинацию цветов RGB, которые производят требуемый составной цвет. В предложенной модуляции цветовой компонент RGB каждого пикселя немного изменяется», - поясняют авторы исследования.

Данные изменения незаметны для пользователя, однако злоумышленник может отслеживать этот поток данных, используя видеозапись экрана

скомпрометированного компьютера, сделанную при помощи местной камеры наблюдения, камеры смартфона или web-камеры, а затем воссоздать извлеченную информацию, используя техники обработки изображений. Работа нового метода продемонстрирована в видео ниже.» ***(Ученые смогли украсть данные с физически изолированного ПК, отслеживая яркость экрана // SecurityLab.ru (https://www.securitylab.ru/news/504726.php). 06.02.2020).***

***

«Студенты Гарвардской школы инженерных и прикладных наук им. Джона А. Полсона Даша Метрополитански (Dasha Metropolitansky) и Киан Аттари (Kian Attari) разработали инструмент, анализирующий огромные массивы наборов пользовательских данных, утекших в Сеть в результате взломов. С его помощью они смогли доказать, что деанонимизировать пользователей гораздо проще, чем считается.

С помощью инструмента они проанализировали тысячи наборов данных и несмотря на то, что многие из записей содержали «анонимизированную» информацию, по словам студентов, найти реальных пользователей оказалось не так уж и сложно.

«Отдельная утечка данных похожа на кусочек головоломки. Сама по себе она не представляет опасность, но когда несколько утечек объединены, они образуют удивительно четкую картину личности пользователя», — сообщил исследователь.

Например, в то время как одна компания может хранить только логины, пароли, адреса электронной почты и другую основную информацию об учетной записи, другая компания может хранить данные web-браузинга или информацию о местоположении пользователя. По отдельности подобные записи не помогут идентифицировать конкретного человека, но в совокупности они раскрывают многочисленные персональные подробности.

Исследователи также обнаружили, что, несмотря на неоднократные предупреждения, пользователи по-прежнему не использует уникальные пароли или менеджеры паролей. Из 96 тыс. проанализированных паролей только 26 тыс. были уникальными.

«Киберпреступнику не обязательно искать конкретную цель. Теперь они могут искать пользователей, которые отвечают определенному набору критериев», — сказала Метрополитански.

Используя инструмент, исследователям за несколько секунд удалось создать набор данных с более чем 1 тыс. человек, которые обладают большим капиталом, состоят в браке, имеют детей, а также зарегистрированы на сайтах знакомств.» ***(Деанонимизировать пользователей гораздо проще, чем считается // SecurityLab.ru (https://www.securitylab.ru/news/504662.php). 04.02.2020).***

***

«Минулого місяця SpaceX стала оператором найбільшого в світі кількості активно працюючих супутників. Відомо, що за станом на кінець січня 2020 року, компанія мала 242 супутника, що обертаються навколо планети, і планувала запустити ще 42 000 протягом наступного десятиліття. Як заявив

засновник компанії SpaceX Ілон Маск, висновок на орбіту такого великого числа штучних супутників є лише частиною амбітного проекту щодо забезпечення глобального доступу в інтернет по всьому світу. Однак згідно з дослідженням, опублікованим на порталі livescience.com, величезна кількість супутників на орбіті може стати загрозою для всього людства. Так в чому ж полягає підступ активного розгортання орбітальних об'єктів, що використовуються переважно для зв'язку?

Чи можна зламати орбітальні супутники?

Початок XXI століття можна по праву назвати епохою завоювання орбітального простору Землі приватними підприємствами. Так, крім уже згаданої вище компанії SpaceX, на орбіту нашої блакитної планети вже вийшли пристрою таких гігантів, як Amazon, що базується у Великобританії OneWeb, а також ряду інших фірм, які готові вивести в космос ще тисячі супутників.

Ці нові пристрої здатні революціонізувати багато аспектів повсякденного життя людства – від забезпечення доступу до інтернету у віддалених куточках земної кулі до моніторингу навколишнього середовища. Разом з тим, відсутність стандартів і правил кібербезпеки для комерційних супутників ставить під загрозу безпеку більшості розвинених країн світу, які можуть стати по-справжньому уразливими при кіберконфліктах.

Так, якщо хакерам вдасться взяти під контроль навіть саме незначне кількість супутників, наслідки подібного інциденту можуть бути найжахливішими. Хакери могли б глушити або підробляти сигнали з супутників, створюючи хаос всередині заданого держави і порушуючи працездатність електричних, водопровідних і транспортних мереж.

Крім усього іншого, з огляду на те, що більшість нових супутників мають власні двигуни, що дозволяють пристроям переміщатися в просторі, хакери могли б змінювати орбіти супутників і змушувати їх врізатися один в одного або навіть в Міжнародну космічну станцію.

Складність виготовлення орбітальних супутників змушує брати участь в процесі їх створення кілька груп різних виробників. В даний час організації – прямі власники супутників – часто передають управління орбітальними пристроями в спеціальні аутсорсингові компанії. З кожним подібним кроком потенційна вразливість устаткування зростає, оскільки сучасні хакери мають велику кількість можливостей для проникнення навіть в саму захищену систему. Крім того, відомо, що найбільш уразливими до атак є крихітні супутники CubeSats, що використовуються в наукових і освітніх цілях поруч університетів і навіть шкіл. Злом цих пристроїв масою від 100 грам до 1 кілограма може бути неймовірно простим завданням навіть для не досвідченого хакера, який має в своєму розпорядженні спеціалізовану наземну антену.

Вперше випадок захоплення контролю над супутником стався в 1998 році, коли хакери захопили контроль над американо-німецьким супутником ROSAT. Тоді зловмисники проінструктували супутник направити свої сонячні батареї прямо на Сонце, що миттєво підсмажити його батареї і зробило супутник марним. Аналогічний випадок стався у Великобританії буквально через рік після першої пригоди. Тоді хакери утримували в "заручниках" супутники SkyNet з метою отримання викупу.

Через те, що в даний час не існує певних стандартів захисту супутників в орбітальному просторі, як і спеціального органу, що регулює забезпечення кібербезпеки, відповідальність за супутники лягає на їх компанії-виробники. Однак навіть для компаній, які надають великого значення кібербезпеки, витрати, пов'язані із забезпеченням безпеки кожного компонента, можуть бути непомірно високими і навіть можуть перевищувати вартість самого супутника.

Незалежно від того, чи будуть вжиті заходи щодо забезпечення супутникової безпеки чи ні, було б помилкою чекати, поки хакери отримають контроль над невеликим комерційним супутником. Наслідки такого кроку можуть загрожувати здоров'ю, майну і навіть життя не тільки окремої людини, але і суспільства в цілому». ***(Хакери можуть перетворити супутники планети в зброю // Portaltele (https://portaltele.com.ua/news/technology/hakeri-mozhut-peretvoriti-suputniki-planeti-v-zbroyu.html?utm_source=rss&utm_medium=rss&utm_campaign=hakeri-mozhut-peretvoriti-suputniki-planeti-v-zbroyu). 16.02.2020).***

***

«Учитывая, что эффективные, продолжительные и масштабируемые кибератаки требуют высокого уровня планирования и разработки, наиболее вероятным является сценарий, при котором используются существующие методы, такие как атаки с целью получения выкупа и атаки типа «отказ в обслуживании». Однако нельзя исключить возможность атак типа «Спящий агент» (Sleeper Agent), при которых вредоносный код помещается в ключевые системы в «мирное время» и активируются дистанционно во время кризиса.

Вопрос в том, как подготовиться к любому из подобных происшествий. Скорее всего, цели такой атаки будут варьироваться от правительственных объектов до крупных коммерческих организаций и критической инфраструктуры. Конечно, компании сталкиваются с уже знакомыми угрозами каждый день, поэтому любые действия, предпринимаемые для ее устранения, уже должны быть частью любой стратегии по обеспечению безопасности.

Существуют шесть основных шагов, которые должна предпринять организация, чтобы подготовиться к любой кибератаке и защитить свои цифровые активы:

сегментируйте свою сеть. Критические активы должны быть разделены по хорошо защищенным доменам. Кроме того, важно использовать сегментацию на основе целей, чтобы гарантировать, что устройства, активы и данные, которые постоянно перемещаются в сети и из нее, динамически распределяются по соответствующим сегментам, определенным внутренней политикой сети. Последняя гарантирует, что сбой в одном домене не станет катастрофическим в случае распространения на другие области;

наладить и поддерживать резервные варианты связи. Поддержание открытых коммуникаций с распределенными элементами вашей сети имеет важное значение. Традиционные модели WAN очень уязвимы к таким вещам, как DDoS-атаки. С другой стороны, возможности безопасной работы в сети SD-WAN позволяют организациям динамически изменять пути обмена данными в зависимости от различных факторов, включая доступность;

защитите критические данные. Учитывая высокий уровень атак с целью получения выкупа, каждая организация должна регулярно создавать резервные копии критических данных и хранить их в автономном (офлайн) режиме. Эти файлы также должны регулярно проверяться на наличие встроенных вредоносных программ. Кроме того, организациям следует периодически проводить учения для обеспечения возможности быстрого переноса резервных копий данных в критически важные системы и устройства, с тем чтобы сеть могла вернуться в нормальное состояние как можно быстрее;

интегрируйте и автоматизируйте. Подход, заключающийся в интеграции устройств в единую платформу безопасности, гарантирует, что все части системы смогут обмениваться и сопоставлять данные об угрозах, а также беспрепятственно становиться неотъемлемой частью любого скоординированного реагирования на угрозу. Кроме того, функции обнаружения и реагирования на конечных точках (Endpoint Detection & Response — EDR) и автоматического оркестрирования и реагирования системы безопасности (Security Orchestration Automation & Response — SOAR) обеспечивают возможность быстрого обнаружения, управления и автоматического реагирования на атаку;

проверьте средства электронной связи. Электронная почта остается наиболее распространенным вектором атаки для заражения устройств и систем вредоносным ПО. В дополнение к интенсивному обучению конечных пользователей методам обнаружения фишинговых атак и реагирования на них, защищенные почтовые шлюзы должны быть способны эффективно выявлять и проверять подозрительные вредоносные вложения в электронную почту в безопасной среде, например в песочнице. Аналогичным образом, межсетевые экраны следующего поколения (NGFW) должны быть развернуты внутри периметра сети для проверки внутренних зашифрованных коммуникаций на предмет обнаружения вредоносного ПО и скрытых командно-контрольных имплантатов;

подпишитесь на каналы, содержащие информацию об угрозах: Подписка на ряд каналов, содержащих информацию об угрозах, собранную от разных источников, наряду с принадлежностью к региональным или отраслевым ISAC позволяет вам быть в курсе актуальных векторов атак и новых вредоносных программ. Используя эти данные и внедряя их в интегрированную платформу безопасности, организации могут выделять индикаторы угроз — сигнатуры вредоносных программ, которые с наибольшей вероятностью повлияют на вашу сеть и отрасль. Таким образом, можно не только заблокировать их при обнаружении, но, в первую очередь, предотвратить их проникновение в вашу сеть.

Чтобы эффективно защититься от направленной кибератаки, все должны работать сообща, как команда, чтобы вовремя предотвратить и обнаружить угрозу, правильно отреагировать на нее. Это включает в себя все и вся, начиная с возможностей национальной обороны страны и заканчивая местными консорциумами предприятий и отраслей промышленности, сообществами поставщиков решений по обеспечению кибербезопасности, таких как Cyber Threat Alliance. Это необходимо сочетать с эффективной стратегией реагирования, которая задействует критически важных членов команды для защиты ресурсов, быстрого восстановления после атаки с использованием резервных копий данных и

изолированных ресурсов». ***(Fortinet: шесть условий защиты от надвигающихся киберугроз // ChannelForIT (http://channel4it.com/publications/Fortinet-shest-usloviy-zashchity-ot-nadvigayushchihsya-kiberugroz-36710.html#). 13.02.2020).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Серверы, работающие на базе платформы для автоматизации задач Jenkins, могут быть использованы для осуществления DDoS-атак. Данная возможность связана с наличием уязвимости CVE-2020-2100 (была исправлена в версии Jenkins 2.219) в кодовой базе Jenkins.

Согласно предупреждению разработчиков, установки Jenkins поддерживают два протокола сетевого обнаружения - UDP multicast/broadcast и DNS multicast, которые помогают кластерам Jenkins обнаруживать друг друга в сети. Оба эти протокола включены по умолчанию.

Протокол UDP часто используется злоумышленниками для усиления DDoS-атак. Как выяснил специалист Кембриджского университета Адам Торн (Adam Thorn), атакующие могут использовать протокол Jenkins UDP (порт 33848) для тех же целей.

«Единственный байтовый запрос к этому сервису вернет более чем 100 байтов метаданных Jenkins, что может быть использовано в DDoS-атаках на мастер Jenkins», - пояснили разработчики. Они полагают, что серверы Jenkins могут быть использованы в DDoS-атаках для трафика амплификации до 100 раз.

Тем не менее, когда специалисты протестировали атаку, оказалось, что она ненадежна, поскольку серверы выходят из строя.

Еще одна проблема заключается в том, что вышеупомянутая уязвимость позволяет вынудить серверы отправлять друг другу непрерывный поток пакетов и тем самым вызвать сбой в их работе.

Компаниям, использующим серверы Jenkins, рекомендуется обновиться до релиза 2.219 или заблокировать входящий трафик (порт 33848).

Jenkins — написанный на Java открытый инструмент, предназначенный для обеспечения процесса непрерывной интеграции программного обеспечения.» ***(Серверы Jenkins могут стать инструментом для проведения DDoS-атак // SecurityLab.ru (https://www.securitylab.ru/news/504941.php). 12.02.2020).***

***

«Исследователь безопасности Эран Шимони из компании Cyberark обнаружил уязвимость (CVE-2020-5316) в программном обеспечения клиента Dell SupportAssist. Ее эксплуатация позволяет злоумышленникам выполнять произвольный код с привилегиями администратора на уязвимых компьютерах.

SupportAssist представляет собой программное обеспечение для профилактического мониторинга с автоматическим обнаружением ошибок и уведомлениями для компьютеров и планшетов Dell. Как сообщается на web-сайте

компании, «приложение SupportAssist предварительно установлено на большинстве устройств Dell под управлением операционной системы Windows».

Аутентифицированный пользователь с низким уровнем привилегий может локально использовать данную уязвимость с целью вызвать загрузку произвольных DLL-библиотек двоичными файлами SupportAssist, что приведет к привилегированному выполнению произвольного кода. Уязвимость получила оценку в 7,8 балла по шкале CVSSv3. Проблема затрагивает версии Dell SupportAssist 2.1.3 и ниже для корпоративных ПК и Dell SupportAssist 3.4 и ниже для домашних ПК.

Компания исправила уязвимость в версиях SupportAssist 2.1.4 для корпоративных ПК и SupportAssist 3.4.1 для домашних ПК. Все версии SupportAssist будут автоматически устанавливать последние выпущенные версии, если включены автоматические обновления.» ***(Уязвимость в ПО Dell SupportAssist подвергает ПК риску атак // SecurityLab.ru (https://www.securitylab.ru/news/504935.php). 12.02.2020).***

***

«Компания Microsoft выпустила плановые обновления безопасности для своих продуктов, устраняющие почти сотню уязвимостей, в том числе уязвимость нулевого дня в браузере Internet Explorer, предположительно эксплуатируемую APT-группировкой DarkHotel.

О данной уязвимости (CVE-2020-0674) стало известно в середине января текущего года. Тогда компания предложила ряд мер по предотвращению ее эксплуатации и пообещала выпустить соответствующие патчи в рамках планового «вторника исправлений» в феврале.

Проблема связана с повреждением памяти в скриптовом движке в составе версий Internet Explorer 9, 10 и 11. В частности, уязвимость существует в библиотеке jscript.dll, обеспечивающей совместимость с устаревшими версиями JScript. Уязвимость может быть проэксплуатирована для удаленного выполнения кода в контексте целевого пользователя. Для этого атакующему необходимо убедить жертву посетить вредоносный сайт.

В общей сложности Microsoft устранила 99 уязвимостей в различных продуктах, включая ряд RCE-уязвимостей в Windows Shell, SQL Server, клиенте удаленного рабочего стола и пакете Microsoft Office. С полным списком исправленных проблем можно ознакомиться здесь». ***(Microsoft исправила 0Day-уязвимость в IE // SecurityLab.ru (https://www.securitylab.ru/news/504934.php). 12.02.2020).***

***

«В подсистеме инициализации Linux systemd обнаружена уязвимость (CVE-2020-1712). Ее эксплуатация позволяет злоумышленнику выполнить код с повышенными привилегиями путем отправки специально сформированного запроса по шине DBus.

Проблема представляет собой уязвимость использования после освобождения (use-after-free), которая возникает при асинхронном выполнении

запросов к Polkit-библиотеке во время обработки DBus-сообщений. Некоторые DBus-интерфейсы используют кэш для хранения объектов в течение короткого периода времени и очищают его, как только шина снова находится в состоянии ожидания. Но если DBus-метод использует bus_verify_polkit_async (), ему может понадобиться некоторое время, пока действие в Polkit-библиотеке не будет завершено. Когда это произойдет, снова будет вызван обработчик метода с ранее выделенными пользовательскими данными. Если запрос к Polkit занимает слишком много времени, очистка кэша освобождает хранимые объекты перед повторным вызовом метода, вызывая уязвимость использования после освобождения.

Уязвимость может быть проэксплуатирована через сервис systemd-machined, предоставляющий DBus API org.freedesktop.machine1.Image.Clone. Интерфейс org.freedesktop.machine1.Image.Clone доступен всем непривилегированным пользователям системы, которые могут инициировать сбой в работе systemd или потенциально добиться выполнения кода с правами суперпользователя.

Данная проблема исправлена в тестовом выпуске systemd 245-rc1. Уязвимость устранена в дистрибутивах Ubuntu, Fedora, RHEL, CentOS, SUSE/openSUSE и ROSA.» ***(Уязвимость в systemd позволяет выполнить код с повышенными правами // SecurityLab.ru (https://www.securitylab.ru/news/504843.php). 10.02.2020).***

***

«Спустя полтора месяца после публикации Positive Technologies информации о критически опасной уязвимости в ПО Citrix, угрожавшей 80 тысячам компаний в 158 странах, каждая пятая компания все еще не приняла меры для устранения уязвимости. Это следует из данных мониторинга актуальных угроз (threat intelligence), который проводит компания Positive Technologies.

Критически опасную уязвимость CVE-2019-19781 в Citrix Application Delivery Controller (NetScaler ADC) [1] и Citrix Gateway (NetScaler Gateway) в декабре обнаружил эксперт Positive Technologies Михаил Ключников. По данным Positive Technologies на конец 2019 года. лидерами по числу потенциально уязвимых организаций были США (более 38% всех уязвимых организаций), Германия, Великобритания, Нидерланды и Австралия. Восьмого января 2020 года был опубликован эксплойт. который позволяет гипотетическому злоумышленнику автоматизировать атаки на компании, не устранившие данную уязвимость.

«Полностью исключить проблему разработчики Citrix планировали с 27 по 31 января, но выпустили серию патчей для разных версий продукта на неделю раньше. Важно как можно скорее установить необходимое обновление, а до тех пор придерживаться рекомендаций по безопасности Citrix, которые были доступны с момента публикации информации об уязвимости», — предупреждает директор экспертного центра безопасности Positive Technologies (PT Expert Security Center) Алексей Новиков.

В целом динамика устранения уязвимости положительная, но в зоне риска все еще остаются 19% компаний. В топ стран по количеству потенциально уязвимых организаций сегодня входят Бразилия (43% от числа компаний, в

которых уязвимость была выявлена изначально), Китай (39%), Россия (35%), Франция (34%), Италия (33%) и Испания (25%). Лучшую динамику демонстрируют США, Великобритания и Австралия: в этих странах зафиксировано по 21% компаний, которые продолжают использовать уязвимые устройства и не принимают никаких мер защиты…» ***(Каждая 5 компания не устранила уязвимость в ПО Citrix, позволяющую за минуту проникнуть во внутреннюю сеть // SecurityLab.ru (https://www.securitylab.ru/news/504784.php). 07.02.2020).***

***

«Специалисты из компании SafeBreach Labs представили технические подробности и PoC-код уязвимости в пакете драйверов Realtek HD Audio Driver. Ее эксплуатация позволяет выполнять произвольные полезные нагрузки с повышенными привилегиями на уязвимом компьютере.

Уязвимость (CVE-2019-19705) может быть использована для обхода защиты и обеспечения персистентности на системе путем загрузки произвольной неподписанной DLL-библиотеки в подписанный процесс.

Пакет Realtek HD Audio Driver присутствует на всех компьютерах под управлением Windows, на которых установлена звуковая карта Realtek, что делает их уязвимыми для атак. Однако для осуществления атаки злоумышленнику необходимо обладать правами администратора.

В ходе анализа процесса RAVBg64.exe (фоновый процесс драйвера Realtek) исследователи обнаружили, что он работает с системными привилегиями, однако загружает некоторые DLL-библиотеки небезопасным способом.

Как отметили эксперты, проблема заключается не только в загрузке библиотек, которых нет в ожидаемом месте, но и в том, что они исполняются, хотя должны быть предназначены только для данных.

По словам специалистов, причина данной проблемы заключается в том, что Realtek использовала Visual Studio 2005 для компиляции двоичного файла, что привело к неправильному поведению процесса RAVBg64.exe. Также в загруженных библиотеках не выполняется проверка цифровой подписи, что позволяет загружать неподписанные произвольные библиотеки.

Исследователи сообщили поставщику о данной уязвимости в июле прошлого года, и разработчики устранили ее в версии Realtek HD Audio Driver 1.0.0.8856.» ***(Уязвимость в Realtek HD Audio Driver позволяла загружать DLL-библиотеки // SecurityLab.ru (https://www.securitylab.ru/news/504787.php). 07.02.2020).***

***

«Исследователь безопасности из аналитической команды Google Project Zero Янн Хорн (Jann Horn) сообщил. что некоторые функции безопасности, добавленные компанией Samsung в ядро Android, поставляемое в смартфонах Samsung Galaxy A50, не обеспечивают полноценную защиту и добавляет дополнительный вектор атаки.

Ядро Samsung реализована функция защиты от чтения или изменения пользовательских данных. Однако Хорн обнаружил, что она не только не

выполняет свое предназначение, но также представляет уязвимости, использование которых предоставляет возможность выполнения произвольного кода.

Как отметил эксперт, злоумышленник может получить доступ к базе данных учетных записей, содержащей конфиденциальные токены аутентификации. Цепочка эксплуатации также предполагает использование уязвимости раскрытия информации в ядре Linux (CVE-2018-17972), которая была исправлена в ядре Linux и ядре Android, но все еще содержится в ядре Android, поставляемых в смартфонах Samsung.

Исследователь сообщил Samsung об обнаруженных уязвимостях, и компания исправила их, в том числе CVE-2018-17972. По словам Хорна, он не проверял ядро в других телефонах Samsung, но отметил, что специфичные для поставщика модификации, внесенные в основные функции ядра, могут представлять уязвимости и препятствовать уменьшению поверхности атак.» ***(Новые защитные функции от Samsung подвергают ядро Android риску атак // SecurityLab.ru (https://www.securitylab.ru/news/505076.php). 14.02.2020).***

***

«У системы управления контентом Drupal появилась собственная программа вознаграждения за найденные уязвимости для обеспечения максимальной безопасности и конфиденциальности сайтов. Каждый пользователь имеет право участвовать в программе при условии соблюдения установленных условий и требований Drupal.

Программа вознаграждения за найденные уязвимости распространяется только на сайт drupal.org и охватывает следующие уязвимости: межсайтовый скриптинг (XSS), открытое перенаправление, подделка межсайтовых запросов (CSRF) и некорректное управление доступом.

Важным моментом является то, что к рассмотрению будут приниматься только аутентичные уязвимости, а не автоматизированные результаты тестирования на проникновение.

Напомним, в январе нынешнего года фонд Cloud Native Computing Foundation (CNCF), занимающийся управлением Kubernetes, совместно с Google и HackerOne также запустил программу вознаграждения за найденные уязвимости в данном ПО. Размер вознаграждения будет варьироваться от $100 до $10 тыс. Программа в течение нескольких месяцев работала в закрытом режиме, но теперь в ней могут принять участие все желающие исследователи безопасности.» ***(Платформа Drupal запустила свою программу bug bounty // SecurityLab.ru (https://www.securitylab.ru/news/505054.php). 14.02.2020).***

***

«В рамках февральского «вторника исправлений» компания Siemens выпустила более десятка предупреждений, информирующих пользователей о различных проблемах, затрагивающих ее продукты, в том числе серьезных уязвимостях отказа в обслуживании в ряде промышленных решений.

В частности, в продуктах SIMATIC PCS 7. SIMATIC WinCC и SIMATIC NET PC DoS-уязвимость проявляется при включенном шифровании коммуникаций.

Проблема может быть проэксплуатирована путем отправки специально сформированного сообщения на целевую систему. Атака не требует высоких прав или взаимодействия с пользователем.

DoS-уязвимости также подвержены некоторые решения SIMATIC S7 и S7-1500 . Злоумышленник может воспользоваться проблемой, отправив специально сформированные HTTP-запросы на порт 80 или 443 или, во втором случае, пакеты UDP на устройство.

Еще одна DoS-уязвимость затрагивает продукты, использующие протокол Profinet-IO (версии до 06.00). Проблема связана с «недостаточным ограничением внутреннего распределения ресурсов при отправке многочисленных легитимных диагностических запросов на интерфейс DCE-RPC».

Остальные DoS-уязвимости выявлены в цифровых устройствах защиты SIPROTEC 4 и SIPROTEC Compact. Проблемы проявляются в устройствах, использующих коммуникационные модули EN100 Ethernet.

В числе прочих проблем стоит отметить RCE-уязвимость в коммуникационных процессорах SIMATIC CP 1543-1 и clickjacking-уязвимость в коммутаторах SCALANCE X». ***(Siemens предупредила о DoS-уязвимостях в ряде промышленных продуктов // SecurityLab.ru (https://www.securitylab.ru/news/505038.php). 13.02.2020).***

***

«Эксперты Positive Technologies проанализировали состояние защищенности веб-приложений [1] и выяснили, что в 9 случаях из 10 злоумышленники могут атаковать посетителей сайта, 16% приложений содержат уязвимости, позволяющие получить полный контроль над системой, а в 8% случаев — атаковать внутреннюю сеть компании. Кроме того, получив полный доступ к веб-серверу, хакеры могут размещать на атакуемом сайте собственный контент (выполнять дефейс) или даже атаковать его посетителей, например заражая их компьютеры ВПО.

По данным исследования, в 2019 году существенно (на 17 процентных пунктов по сравнению с 2018 годом) снизилась доля веб-приложений, содержащих уязвимости высокого уровня риска. Число уязвимостей, которое в среднем приходится на одно приложение, снизилось по сравнению с прошлым годом почти в полтора раза. Несмотря на это, общий уровень защищенности веб-приложений оценивается как низкий.

82% всех выявленных уязвимостей обусловлены ошибками в коде. По словам экспертов, даже в случае продуктивных систем в каждой второй они находили уязвимости высокого уровня риска. Высокий процент ошибок в исходном коде свидетельствует о том, что код не проходит проверку на наличие уязвимостей на промежуточных этапах его создания, а также что разработчики по-прежнему уделяют недостаточно внимания безопасности, делая ставку на функциональность приложения.

В 45% исследованных веб-приложений эксперты обнаружили недостатки аутентификации (Broken Authentication); многие уязвимости из этой категории критически опасны.

«Большинство атак на аутентификацию связано с тем, что пользователи устанавливают только пароль, — считает Ольга Зиненко, аналитик компании Positive Technologies. — Отсутствие второго фактора делает атаки на аутентификацию простыми в реализации. Эта проблема усугубляется тем, что пользователи стараются придумать пароли попроще. Обход ограничений доступа обычно приводит к несанкционированному разглашению, изменению или уничтожению данных».

По данным экспертов, 90% веб-приложений подвержены угрозе атак на клиентов. Как и в предыдущие годы, существенную роль в этом играет уязвимость «Межсайтовое выполнение сценариев» (Cross-Site Scripting, XSS). Примерами атак на пользователей могут быть заражение компьютеров вредоносным ПО (доля этого метода атак на частных лиц в третьем квартале года увеличилось до 62% против 50% во втором), фишинговые атаки для получения учетных или других важных данных, а также выполнение действий от имени пользователя с помощью обманной техники clickjacking, в частности для накрутки лайков и просмотров.

[1] Были проанализированы 38 полнофункциональных веб-приложений IT-компаний (29% общего числа исследованных приложений), финансовых организаций (26%), организаций сферы телекоммуникаций (21%), промышленного сектора (16%) и госучреждений (8%)». ***(Positive Technologies: 82% уязвимостей веб-приложений содержится в исходном коде // SecurityLab.ru (https://www.securitylab.ru/news/505004.php). 13.02.2020).***

***

«Злоумышленники активно сканируют Сеть на предмет серверов Microsoft Exchange, содержащих критическую уязвимость CVE-2020-0688. Ее эксплуатация позволяет выполнить произвольный код с привилегиями SYSTEM на сервере и полностью скомпрометировать его.

Риску потенциальных атак подвержены все версии Exchange Server, включая те, которые в настоящее время не поддерживаются Microsoft. Уязвимость содержится в компоненте управления для пользователей и администраторов Exchange Control Panel (ECP) и вызвана неспособностью Exchange создавать уникальные криптографические ключи при установке.

Исследователь безопасности из Trend Micro Zero Day Initiative Саймон Цукербраун (Simon Zuckerbraun) описал эксплуатацию уязвимости CVE-2020-0688 в Microsoft Exchange и использования фиксированных криптографических ключей в рамках атаки на уязвимый сервер.

«Любой злоумышленник, скомпрометировавший устройство или учетные данные пользователя, сможет перейти на сервер Exchange. После этого преступник сможет разглашать или подделывать корпоративные почтовые сообщения по своему желанию», — отметил Цукербраун.

Для осуществления атаки злоумышленнику нужно лишь обнаружить уязвимые серверы в Сети, найти адреса электронной почты, которые он может добыть через URL-адрес web-клиента Outlook Web Access (OWA) или заполучить соответствующие данные из предыдущих утечек.

Как отметил ИБ-эксперт Кевин Бомон (Kevin Beaumont), злоумышленники могут использовать инструмент Mimikatz для сброса паролей всех пользователей, поскольку Exchange Server сохраняет учетные данные пользователя в памяти в виде незашифрованного открытого текста.

Администраторам уязвимых систем настоятельно рекомендуется применить последние патчи, исправляющие уязвимость». ***(Преступники сканируют Сеть на предмет уязвимых серверов Microsoft Exchange // SecurityLab.ru (https://www.securitylab.ru/news/505433.php). 27.02.2020).***

***

«Исследователи безопасности из компании ESET обнаружили опасную уязвимость (CVE-2019-15126) в широко используемых Wi-Fi-чипах от Broadcom и Cypress. Проблема затрагивает более миллиарда устройств, включая смартфоны, планшеты, ноутбуки, маршрутизаторы и IoT-устройства. Уязвимость получила название Kr00k и ее эксплуатация позволяет находящимся поблизости удаленным злоумышленникам перехватывать и дешифровать некоторые беспроводные сетевые пакеты, передаваемые уязвимым устройством.

Уязвимость затрагивает устройства, использующие протоколы WPA2-Personal или WPA2-Enterprise с алгоритмом шифрования AES-CCMP, но не устройства, использующие протокол WPA3. Для осуществления атаки не требуется подключение к беспроводной сети. По словам специалистов, риску атак подвержены продукты Amazon (Echo, Kindle), Apple (iPhone, iPad, MacBook), Google (Nexus), Samsung (Galaxy), Raspberry (Pi 3), Xiaomi (RedMi), а также точки доступа от Asus и Huawei.

Как отмечается, с помощью Kr00k злоумышленник не сможет провести MitM-атаку или узнать пароль от Wi-Fi-сети. Кроме того, уязвимость позволяет скомпрометировать шифрование на беспроводном уровне, но не имеет отношения к TLS-шифрованию, обеспечивающему безопасность сетевого трафика.

Уязвимость Kr00k в некоторой степени связана с атакой реинсталяции ключей (Key Reinstallation Attack, KRACK), позволяющей злоумышленникам взламывать пароли Wi-Fi, защищенные WPA2-протоколом.

Суть эксплуатации уязвимости Kr00k заключается в следующем: когда устройство внезапно отключается от беспроводной сети, Wi-Fi-чип очищает сессионный ключ в памяти и устанавливает его значение «0», но при этом непреднамеренно продолжает передавать все данные, оставшиеся в буфере. Таким образом, злоумышленник, находящийся в непосредственной близости от устройства, может использовать данную уязвимость для многократного инициирования разъединения, отправляя пакеты деаутентификации по беспроводной сети для перехвата большего количества данных (в том числе DNS, ARP, ICMP, HTTP, TCP и TLS-пакетов).

Исследователи ESET сообщили об обнаруженной проблеме производителям уязвимых чипов Broadcom и Cypress в прошлом году. Компании Broadcom и Cypress уже выпустили соответствующее обновление прошивки. Apple исправила уязвимость в версии iOS 13.2, iPadOS 13.2 и macOS Catalina 10.15.1. Остальные производители работают над решением проблемы». ***(Уязвимость в Wi-Fi-чипах***

затрагивает более миллиарда устройств // SecurityLab.ru (https://www.securitylab.ru/news/505401.php). 27.02.2020).

***

«Киберпреступники обнаружили уязвимость в интеграции PayPal с Google Pay и активно эксплуатируют ее для незаконных денежных переводов. Начиная с 21 февраля нынешнего года, пользователи стали замечать неизвестные транзакции в своих историях платежей PayPal, осуществленных через Google Pay. Жалобы пользователей появляются на разных платформах, в том числе на форумах PayPal (1. 2. 3. 4. 5. 6. 7), Reddit (1. 2), Twitter, (1. 2), а также на немецких и русских форумах поддержки Google Pay (1. 2. 3. 4. 5. 6. 7. 8. 9. 10).

По словам пользователей, через их учетные записи Google Pay, привязанные к PayPal, злоумышленники оплачивают товары. Судя по представленным ими скриншотам, большинство покупок совершается в магазинах США, в частности в сети Target в Нью-Йорке. Большая часть пострадавших пользователей – жители Германии. Стоимость некоторых покупок превышает 1 тыс. евро.

Какого рода уязвимость эксплуатируют киберпреступники, пока неясно. Компания PayPal проводит расследование ситуации.

По словам немецкого исследователя безопасности Маркуса Фенске (Markus Fenske), происходящее очень напоминает уязвимость, о которой он и его коллега Андреас Майер (Andreas Mayer) сообщили PayPal в феврале 2019 года. В то время компания не посчитала ее исправление приоритетной задачей.

Как пояснил Фенске, уязвимость заключается в том, что во время привязки учетной записи PayPal к учетной записи Google Pay PayPal создает виртуальную карту с собственным номером, сроком действия и CVC. Когда пользователь Google Pay решает воспользоваться функцией бесконтактных платежей PayPal, оплата производится с этой виртуальной карты.

Если бы виртуальная карта использовалась только для оплаты через PoS-терминалы, проблем бы не было. Однако виртуальная карта может использоваться и для online-платежей. Вероятно, злоумышленники нашли способ похищения данных виртуальных карт и с их помощью оплачивают покупки в американских магазинах, считает Фенске.

По словам исследователя, есть три возможных способа похищения данных виртуальных карт. Первый – подсмотреть их на экране смартфона/компьютера жертвы. Второй способ – похитить данные, заразив устройство жертвы вредоносным ПО, и третий – получить данные методом перебора. «Вполне вероятно, атакующий просто подобрал номера и даты истечения срока действия карт с помощью брутфорса, что могло занять около года. CVC не имеет значения, подойдет любое значение», – сообщил Фенске изданию ZDNet». ***(Злоумышленники обчищают кошельки PayPal через неизвестную уязвимость // SecurityLab.ru (https://www.securitylab.ru/news/505343.php). 25.02.2020).***

***

«Компания Google выпустила обновление для браузера Google Chrome 80, исправляющее три критические уязвимости. Все три уязвимости получили оценку в 8.8 по шкале CVSS 3.0.

Первая проблема (CVE-2020-6418) представляет собой уязвимость типа type confusion (несоответствие используемых типов данных). Она затрагивает JavaScript-движок V8 с открытым исходным кодом, используемый Chrome.

Две другие уязвимости связаны с целочисленным переполнением в программном обеспечении (International Components for Unicode, ICU) и доступом к памяти за пределами буфера в компоненте потоков (CVE-2020-6407)…». ***(Google исправила 0Day-уязвимость в Chrome // SecurityLab.ru (https://www.securitylab.ru/news/505344.php). 25.02.2020).***

***

«Компания Risk Based Security опубликовала отчет об обнаруженных в 2019 году уязвимостях. Из 22 316 проблем безопасности 33% получили оценку как минимум в 7,0 балла по шкале CVSS. Общее количество выявленных уязвимостей было немного меньше по сравнению с 2018 годом (23 210) и примерно таким же, как в 2017 году (22 511).

Как отметили исследователи, около тысячи уязвимостям не были присвоены идентификаторы CVE.

Среди поставщиков оборудования с наибольшим количеством обнаруженных уязвимостей эксперты отметили Oracle (1064), IBM (1054), Google (1046), Microsoft (926), Dell (701) и Cisco (615). Первое место в данном рейтинге в 2019 году занял дистрибутив Linux SUSE — 1379 уязвимостей.

Большинство уязвимостей раскрываются во «вторник обновлений», когда такие крупные поставщики, как Adobe, Microsoft, Siemens и SAP, выпускают обновления безопасности для своих продуктов. Патчи «вторника исправлений» за август 2019 года исправили 327 уязвимостей — больше, чем в любой другой день.

По словам экспертов, в электронных машинах для голосования были обнаружены 302 уязвимости, и 289 из них не были исправлены. Только для 13 уязвимостей были выпущены патчи патчи и лишь одной из них был присвоен идентификатор CVE». ***(В 2019 году обнаружено более 22 тыс. уязвимостей // SecurityLab.ru (https://www.securitylab.ru/news/505210.php). 19.02.2020).***

***

«Компания Wordfence зафиксировала атаки на сайты под управлением WordPress, на которых используется уязвимый плагин ThemeREX Addons. Этот плагин помогает пользователям продуктов ThemeREX настраивать свои новые сайты и управлять различными функциями тем. ThemeREX Addons поставляется предустановленным со всеми коммерческими темами ThemeREX. По данным Wordfence, в настоящее время плагин используется более чем на 44 тыс. сайтов.

Как пояснили специалисты, плагин работает путем настройки конечной точки WordPress REST-API. Проблема заключается в том, что он не проверяет источник команды, отправляемой его REST-API. Любой посетитель сайта (будь то

его владелец или злоумышленник) может удаленно выполнить код, получить привилегии администратора и захватить полный контроль над сайтом.

В настоящее время уязвимость остается неисправленной. Во избежание атак пользователям версий ThemeREX Addons после 1.6.50 рекомендуется временно удалить плагин до тех пор, пока не будет выпущен патч.

Помимо атак через ThemeREX Addons, зафиксирована еще одна волна атак на сайты под управлением WordPress – через плагин ThemeGrill Demo Importer (установлен на 200 тыс. сайтов). Однако в данном случае злоумышленники не включают взломанные ресурсы в ботнет, а преследуют деструктивные цели. С помощью уязвимости они стирают базы данных сайтов и сбрасывают их настройки. Для предотвращения атак администраторам рекомендуется установить обновленную версию ThemeGrill Demo Importer». ***(Зафиксированы две волны атак на сайты под управлением WordPress // SecurityLab.ru (https://www.securitylab.ru/news/505220.php). 20.02.2020).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Решения Eset помогли выявить атаку киберпреступников Winnti Group на университеты Гонконга. Winnti Group известна резонансными кибератаками на цепочки поставок в индустрии видеоигр и различного ПО, а также вмешательством в сферы здравоохранения и образования.

В настоящее время цель злоумышленников – хищение данных с атакуемых компьютеров. Преступная кампания проходила на фоне массовых протестов, затронувших в том числе и университеты.

По данным актуальных исследований, группировка по-прежнему использует флагманский бэкдор ShadowPad. Но в рамках данной кампании загрузчик ShadowPad заменен на упрощенную версию.

«ShadowPad – мультимодульный бэкдор, в частности с помощью модуля-кейлоггера записывается каждое нажатие клавиши на клавиатуре. Использование этого модуля по умолчанию указывает на то, что злоумышленники заинтересованы в краже информации с компьютеров жертв», – говорит Матье Тартар, исследователь Eset.» ***(Хакерская группировка Winnti Group воспользовалась протестами в Гонконге // Компьютерное Обозрение (https://ko.com.ua/hakerskaya_gruppirovka_winnti_group_vospolzovalas_protestami_v_gonkonge_131793). 12.02.2020).***

***

«Браузеры все агрессивнее конкурируют в сфере конфиденциальности, предлагая принципиально разные подходы для защиты пользователей. Лили Хэй Ньюман из Wired разобралась, чем именно различаются позиции ведущих игроков.

В 1990-х годах такие браузеры, как Netscape Navigator и Microsoft Internet Explorer, соревновались в запуске удивительных функций и привлечении

пользователей. Сегодня браузерный ландшафт выглядит совершенно иначе. С одной стороны, доминирует Chrome, который контролирует около двух третей рынка как настольных, так и мобильных устройств. С другой стороны, еще более жесткой стала борьба, касающаяся защиты пользовательских данных. Это хорошие новости для всех, кого пугает небрежное обращение с конфиденциальной информацией, но браузеры все больше расходятся в своих методах, и становится ясно, что не все средства защиты данных равны.

На конференции по безопасности USENIX Enigma, которая состоялась в Сан-Франциско на прошлой неделе, разработчики и исследователи озвучили различные мнения о том, как браузеры должны защищать пользователей от злоупотребления их данными. На панельной дискуссии, в которой приняли участие представители Mozilla Firefox, Google Chrome, Microsoft Edge и Brave, все согласились с тем, что сотрудничество в этой сфере стимулирует инновации. Но одни браузеры выбирают радикальные изменения, а другие предпочитают усиливать защиту данных, сохраняя статус-кво.

«Думаю, конкуренция подталкивает всех нас к усилению защиты по умолчанию. Например, когда мы видим, что Safari разворачивает новое решение в этой области, то думаем: ″О, мы должны хотя бы попытаться соответствовать″. Как у браузера, прежде всего ориентированного на конфиденциальность, это одно из наших главных коммерческих преимуществ», — рассказал Ян Чжу, директор по информационной безопасности Brave.

Браузеры могут предпринять ряд шагов, чтобы помешать сайтам и рекламным сетям отслеживать действия пользователей в интернете. Они могут затруднить сопоставление истории посещений с личностью, которое базируется на сочетании уникальных характеристик — «отпечатков пальцев» — браузера и устройства, на котором он установлен. Они могут блокировать встроенные в сайты трекеры. Браузеры также могут ввести дополнительное шифрование информации о посещениях сайтов и поддержать сторонние расширения, которые позволяют самостоятельно настраивать защиту данных.

Еще одна давняя тема споров — как обрабатывать куки-файлы сторонних сайтов, которые браузеры хранят для персонализации пользовательского опыта, но которые также часто используются для отслеживания действий. Safari, Firefox и Brave решили блокировать сторонние куки по умолчанию — к большому огорчению рекламодателей. Google объявил, что планирует сделать то же самое, но не сейчас, а в течение двух лет. Как крупнейший рекламодатель он также выигрывает от блокировки сторонних трекеров, чего не скажешь о других браузерах.

Почти все основные браузеры принимают меры по защите персональных данных, но концептуально их подходы различаются. Многие споры касаются вопросов о том, как далеко продвинутся эти методы и не будет ли у них побочного эффекта. Иногда защита конфиденциальности может нарушать законную функциональность сайта. Например, комментарии, загружаемые со стороннего хостинга, могут быть ошибочно приняты за модуль таргетированной рекламы. Таким образом, каждый браузер должен решить, что для него приоритетнее: защита конфиденциальности или простота использования.

«Firefox, Edge, Brave и Safari по умолчанию предлагают системы защиты от отслеживания, но все они немного различаются, все идут на разные компромиссы. Но, в конце концов, все мы пытаемся улучшить защиту и учимся этому друг у друга. Думаю, мы [Firefox] отличаемся от Chrome тем, что не пытаемся сохранить существующую модель. Для нас главным приоритетом является конфиденциальность, поэтому, когда мы выбираем между существующей моделью и конфиденциальностью, мы всегда отдаем предпочтение конфиденциальности», — сказал Танви Вьяс, главный инженер Mozilla.

Существующая модель предоставляет компаниям и рекламодателям доступ к некоторым маркетинговым данным. Один из аргументов в пользу сохранения этого подхода звучит так: если браузеры станут слишком строгими, рекламодатели начнут извлекать контент из открытого веб-пространства и перемещать его в закрытые мобильные приложения.

«Веб не существует в вакууме. Люди, которые создают сайты и сервисы, могут выбирать платформы для таргетинга. Они могут создать мобильное приложение и убрать свой контент из открытой сети, чтобы поместить его в огороженный сад. Если мы внесем изменения во благо конфиденциальности, которые нанесут ущерб открытому веб-пространству, мы можем подтолкнуть людей к использованию менее защищенных экосистем», — считает Эрик Лоуренс, руководитель Edge.

Джастин Шу, директор по разработке Chrome, говорит, что Google уже видит эту миграцию в сторону приложений и других закрытых платформ. По его словам, хоть теоретически в этой эволюции и нет ничего плохого, она не должна происходить за счет веб-пространства. Именно по этой причине Chrome работает над набором открытых стандартов, известных как Privacy Sandbox, цель которых — найти золотую середину в защите конфиденциальности.

«Вообще говоря, рекламодатели нуждаются не в ваших данных. Все, чего они действительно хотят, — это эффективная монетизация. Мы можем дать им инструменты, чтобы они добивались ее, не создавая профили пользователей и не отслеживая их», — сказал Шу на конференции. В Privacy Sandbox Google планирует предложить стандарты, которые позволят анонимно агрегировать рекламные данные для маркетологов.

Chrome твердо стоит на том, что это предложение укрепит открытую сеть. Если контент переместится в закрытые приложения, пользователи не получат выгоды от усиления прозрачности и защиты в веб-пространстве. Но трудно игнорировать тот факт, что Google, управляющий одной из крупнейших в мире рекламных интернет-сетей, также явно заинтересован в защите этой отрасли.

Критики такого подхода утверждают, что он не решает фундаментальных проблем, которые делают цифровой маркетинг настолько агрессивным. Это достаточно сложная проблема, поскольку усилия по сокращению отслеживания могут иметь противоположный эффект. Например, Apple сейчас устраняет уязвимости в Safari Intelligent Tracking Prevention, из-за которых пользователя можно идентифицировать по заблокированным сигналам. Исследователи продолжают находить недостатки в исправлениях компании.

«Общественное внимание к ежедневному отслеживанию и усилия, предпринимаемые в нескольких регионах мира, по-видимому, оказывают все большее давление на браузеры и заставляют их двигаться навстречу пользователям и защищать конфиденциальность по умолчанию. Но они не идут одинаковыми путями и не получают одинакового эффекта. Некоторые заставляют всех поверить, что многое делают для своих пользователей, но на самом деле это не так. В некоторых случаях они только ухудшают ситуацию: это относится к стандартизации других способов отслеживания, удалению пользовательского контроля и настройке отслеживания по умолчанию», — говорит Андрес Арриета, директор по проектированию потребительских систем безопасности в Electronic Frontier Foundation.

Разногласия по поводу лучшего подхода к вопросам конфиденциальности в сети стали настолько сильными, что некоторые игроки решили остаться в тени. Например, Microsoft Edge хочет избавиться от багажа плохих выборов, сделанных Internet Explorer в начале 2000-х годов, и после ребрендинга предстать как надежный, но нейтральный браузер.

«Одна из вещей, которые мы до сих пор пытаемся делать в Edge, — это быть немного спокойнее. Мы не хвалимся защитой конфиденциальности на верхнем уровне, не так много говорим: ″Эй, мы защищаем вас так или эдак″», — отмечает Лоуренс из Edge.

Edge теперь работает на программном обеспечении Chromium с открытым исходным кодом Google, но он все еще использует решения Microsoft, а не третьих сторон. Таким образом, пользователям Edge не нужно доверять второму вездесущему технологическому гиганту и рисковать своими данными перед лицом множества рекламных сетей. Например, Edge использует функцию под названием Microsoft Defender SmartScreen вместо Google Safe Browsing. Edge также предлагает функцию Tracking Prevention, которую Microsoft использует для блокировки трекеров и которую пользователи могут настроить более или менее строго в зависимости от их отношения к ложным срабатываниям.

Очевидно, что противостояние только начинается. Но, по крайней мере, радует, что браузеры наконец обсуждают защиту пользователей и конкурируют, предлагая лучшие варианты. Но актуальным остается вопрос о том, удастся ли им найти правильное решение». ***(Анна Полякова. Почему браузеры спорят о том, как нужно защищать данные пользователей // Rusbase (https://rb.ru/story/browser-privacy/). 04.02.2020).***

***

«По результатам двухмесячного анализа, проведенного независимым экспертом Джамилией Кайя (Jamila Kaya) и специалистами из компании Cisco Duo Security, из Chrome Web Store было удалено более 500 вредоносных расширений, жертвами которых стало несколько миллионов пользователей.

Злоумышленники были активны в течение по крайней мере восьми месяцев, начиная с января 2019 года, а в период с марта по июнь 2019 года выпустили десятки новых вариантов расширений. Вполне возможно, что преступники начали

действовать намного раньше, так как некоторые вредоносные программы и связанные домены были зарегистрированы в 2018 и 2017 годах.

С помощью сервиса для анализа расширений CRXcavator специалистам удалось выявить 70 рекламных расширений с общим числом загрузок более 1,7 млн. Плагины были объединены почти идентичной кодовой базой и использовали неприметельные названия. Вредоносный код внедрял рекламу в браузеры пользователей, а также перенаправлял жертв на фишинговые сайты. Исследователи проинформировали Google о своих находках, и компания провела собственное расследование, в ходе которого обнаружила еще более 420 подобных программ.

Во всех расширениях применялась схожая техника для маскировки вредоносной активности и избежания механизмов верификации программ в Chrome Web Store. Код практически не отличался на уровне исходных текстов, за исключением имен функций, которые в каждом расширении были уникальны. Передача вредоносных команд осуществлялась с C&C-серверов.

В числе выполняемых расширениями действий упоминается загрузка на C&C-сервер конфиденциальных данных пользователей, перенаправление на вредоносные сайты и установка вредоносных приложений под видом антивирусного ПО или обновления браузера». ***(Более 500 вредоносных расширений для Chrome собирали данные пользователей // SecurityLab.ru (https://www.securitylab.ru/news/505103.php). 17.02.2020).***

***

«Ученые из Университета Глазго (Великобритания) научились использовать кристаллы как генератор случайных чисел для шифрования.

Исследователи смогли использовать кристаллизацию для получения настоящих случайных чисел, что позволило достичь более высокого уровня шифрования. Ранее для защиты от злоумышленников, которые могли так или иначе получить ключ для взлома, использовали «природные» источники случайных чисел — например, датчики движения или шума.

Химики разработали роботизированную систему, которая использует процесс кристаллизации для создания случайных цепочек чисел и шифрования информации. При правильных условиях химические вещества в жидком растворе могут перейти из неупорядоченного состояния в чрезвычайно организованное — кристалл. Процесс наполнен случайностью — от времени, которое требуется для формирования кристалла, до геометрии структур.

Как сообщил профессор химии Ли Кронин (Lee Cronin), они разработали простого робота, который следил через web-камеру за процессами кристаллизации и преобразовывал разные обнаруженные реакции в последовательность единиц и нулей. Исследователи рассмотрели три различные химические реакции и сравнили их закодированные строки с одной, созданной с помощью генератора псевдослучайных чисел общего назначения Mersenne Twister. Обратная расшифровка такой информации заняла куда больше времени, чем в случае с ранее известными методами, что доказывает эффективность выбранного метода.

По словам специалистов, данный метод предлагает хорошую альтернативу существующим генераторам истинных случайных чисел. Форму их робота можно

уменьшить и встроить в обычный компьютер, «предоставляя доступ к мощному и удобному генератору случайных чисел, работающему на химических процессах». Как отметил Кронин, новый метод будет дешевле, чем квантовые вычисления, которые считаются золотым стандартом для генерации случайных чисел». ***(Ученые научились шифровать данные с помощью кристаллов // SecurityLab.ru (https://www.securitylab.ru/news/505044.php). 13.02.2020).***

***

«Ученые из Техасского университета в Далласе (США) разработали новый подход к обеспечению киберзащиты. Метод, получивший название DEEP-Dig (DEcEPtion DIGging), заманивает злоумышленников на сайт-приманку с целью узнать больше информации об их тактике. Собранная информация используется для обучения искусственного интеллекта распознавать и предотвращать будущие атаки.

DEEP-Dig развивает область кибербезопасности, известную как технология обмана, которая подразумевает установку ловушек для киберпреступников. Как отметили исследователи, новый подход может быть особенно полезен для оборонных организаций.

«Мы чаще всего рассматриваем преступников, постоянно пытающихся атаковать наши сети, как негативное явление. Вместо их блокировки, возможно, мы могли бы использовать их в качестве источника бесплатной рабочей силы. Они будут предоставлять нам ценные данные о том, как выглядят вредоносные атаки», — профессор компьютерных наук Кевин Хэмлен (Kevin Hamlen).

Новый метод направлен на решение основной проблемы использования искусственного интеллекта для обеспечения кибербезопасности — нехватки данных, необходимых для разработки моделей по выявлению вредоносных атак, пояснили исследователи». ***(Новая разработка позволит изучать методы киберпреступников // SecurityLab.ru (https://www.securitylab.ru/news/505436.php). 27.02.2020).***

***

«В Техасском университете создали систему киберзащиты, которая учится у хакеров.

Метод борьбы со злоумышленниками получил название DEEP-Dig (с англ. DEcEPtion DIGging — "обнаружение вторжений"). Он основан на том, что компьютер обучается на тактике хакеров, которых специально заманивают на сайт-ловушку. Полученная информация используется для распознавания и прекращения будущих атак. Об этом пишут на сайте Техасского университета.

Исследователи из Техасского университета представили доклад о своей работе "Улучшение детекторов вторжений с помощью Crook-Sourcing" на ежегодной конференции по прикладной компьютерной безопасности в декабре в Пуэрто-Рико. В январе на Гавайской международной конференции по системным наукам они представили еще одну статью "Автоматизация оценки кибердетекции с помощью глубокого обучения".

DEEP-Dig стал частью быстро растущей области кибербезопасности, известной как технология обмана и включающей в себя установку ловушек для хакеров. Исследователи надеются, что такой подход может быть особенно полезен для оборонных организаций.

"Есть преступники, пытающиеся постоянно атаковать наши сети, и обычно мы рассматриваем это с негативной точки зрения, — рассказал доктор Кевин Хэмлен. — Вместо того, чтобы блокировать их, мы могли бы рассматривать этих злоумышленников как источник бесплатной рабочей силы. Они предоставляют нам данные о том, как выглядят вредоносные атаки. Это бесплатный источник высоко ценимых данных".

Подход направлен на решение основной проблемы использования искусственного интеллекта для обеспечения кибербезопасности: нехватка данных, необходимых для обучения компьютеров обнаружению злоумышленников. Отсутствие данных связано с проблемами конфиденциальности. Более качественные данные будут означать лучшую способность обнаруживать атаки.

По словам Хэмлена, хакеры обычно начинают с самых простых трюков, а затем используют все более изощренную тактику. Но большинство программ киберзащиты пытаются разрушить приемы злоумышленников, прежде чем кто-либо сможет их контролировать. DEEP-Dig даст представление о методах хакеров, когда они заходят на сайт-приманку с дезинформацией». ***(Бесплатная "рабочая сила": ИИ будет учиться у хакеров // Телеграф (https://telegraf.com.ua/tehnologii/5369748-besplatnaya-rabochaya-sila-ii-budet-uchitsya-u-hakerov.html). 27.02.2020).***

***

«Для сучасного етапу розвитку систем забезпечення кібербезпеки корпоративних інформаційних систем є характерним застосування інформаційних систем класу SIEM (Security information and event management), які лежать в основі сучасного SOC (Security operations center).

В нашому Університеті під час підготовки фахівців за спеціальністю 125 Кібербезпека вивчаються технології кібербезпеки, які базуються на рішенні IBM QRadar SIEM. Унікальні можливості IBM QRadar Security Intelligence Platform дозволяють розгортати та застосовувати будь-які найсучасніші технології забезпечення кібербезпеки корпоративних інформаційних систем.

Це сталося завдяки прийняття участі Кафедри інформаційної та кібернетичної безпеки у програмі IBM Academic Initiative, а також кропіткої праці доцента кафедри Гахова Сергія Олександровича.

18 лютого 2020 року авторитетніша дослідницька і консалтингова компанія Gartner, що спеціалізується на ринках інформаційних технологій, опублікувала Magic Quadrant for Security Information and Event Management.

За результатами останнього проведеного дослідження Gartner назвала IBM лідером серед виробників SIEM систем. Даний момент говорить про те, що в нашому Університеті вивчаються найсучасніші технології забезпечення кібербезпеки. Це є результатом втіленої інноваційної моделі навчання та буде запорукою професійного успіху майбутніх фахівців із кібербезпеки». ***(Найкращі***

технології кібербезпеки в начальному процесі: IBM лідер Magic Quadrant for Security Information and Event Management // Державний університет телекомунікацій (http://www.dut.edu.ua/ua/news/1/category/0/view/8023). 25.02.2020).

***

Нові надходження до Національної бібліотеки України імені В.І. Вернадського

Веселова Л. Ю. Особливості взаємодії спеціальних органів, служб та підрозділів у сфері забезпечення кібербезпеки / Веселова Л. Ю. // Актуальні проблеми вітчизняної юриспруденції. - 2019. - Вип. 5. - С. 51-55.

Проаналізовано особливості взаємодії спеціальних органів, служб та підрозділів у сфері забезпечення кібернетичної безпеки. Виокремлено специфіку інформаційних ресурсів у кібернетичному просторі, яка проявляється у стрімкому розвитку інформаційних та інформаційно-комунікаційних технологій. Запропоновано прийняття Державної цільової програми забезпечення кібернетичної безпеки України. Охарактеризовано особливості проекту Державної цільової програми забезпечення кібернетичної безпеки України.

Шифр зберігання НБУВ: Ж74269

***

Веселова Л. Ю. Особливості державної політики України у сфері забезпечення кібербезпеки в умовах гібридної війни / Веселова Лілія Юріївна // Науковий вісник Херсонського державного університету. Сер. : Юридичні науки. - 2019. - Вип. 2. – С. 23-27.

Проаналізовано дослідження провідних учених у галузі адміністративного, конституційного та інших суміжних галузей права щодо проблематики кібернетичної безпеки та державної політики констатовано, що державна політика

у сфері забезпечення національної безпеки (кібернетичної безпеки) відноситься до вищого інтегрованого елемента внутрішньої та зовнішньої політики України, а також сукупність принципів, норм, напрямків та форм діяльності органів державної влади у сфері забезпечення національної безпеки (кібернетичної безпеки) та стійкого соціально-економічного розвитку країни. Охарактеризовано Стратегію національної безпеки України. Доведено, що окремі недоліки та рамковий характер Доктрини інформаційної безпеки України знижують ефективність і обмежують сферу її застосування, визначають хибний напрямок розвитку законодавства в кібернетичної сфері та вносять плутанину в процесі його застосування.

Шифр зберігання НБУВ: Ж73149/юр

***

Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія / С. Ф. Гончар. - Київ, 2019. - 175 с.

Обгрунтовано поняття комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури. Здійснено його змістову інтерпретацію. Розроблено структурні рішення обчислювальних систем для розрахунку сумарного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури з використанням запропонованих методів, а також алготирмічне та програмне забезпечення обчислювальних систем для розрахунку зазначених ризиків.

Шифр зберігання НБУВ: ВА839524

***

Дяковський О. С. Правове забезпечення захисту персональних даних : автореф. дис. ... канд. юрид. наук : 12.00.07 / Дяковський Олександр Сергійович ; Ун-т мит. справи та фінансів. - Дніпро, 2019. - 17 с.

Проаналізовано такі нові поняття для юридичної науки, як «персональні дані», «обіг персональних даних», «база даних», «спадкування права на базу персональних даних» та ін. Встановлено етапи та порядок відшкодування моральної шкоди за порушення законодавства у сфері захисту персональних даних, виходячи із повноважень Уповноваженого Верховної Ради України з прав людини та суду, з ураху ванням матеріального та процесуального законодавства. Досліджено міру відповідальності за порушення законодавства у сфері захисту персональних даних в національному законодавстві, на підставі чого сформульовановідповідні рекомендації, спрямованіна підвищ ення ефективностізахисту персональних даних. Визначено систему суб'єктів захисту персональних даних. Розкрито процесуальні особливості обігу інформації та баз даних, що містять персональні дані. На основі вивчення міжнародного та зарубіжного досвіду в сфері правового забезпечення захисту персональних даних запропоновано внесення змін до законодавства, які є необхідними для підвищення якісної складової національного законодавства.

Шифр зберігання НБУВ: РА444288

***

Економіко-правові та управлінські аспекти розвитку суспільства: молодіжний погляд : матеріали міжнар. наук.-практ. конф., 01 листоп. 2019 р. - Дніпро, 2019. - Ч. 2. - 377 с.

Зі змісту:

- Солошенко М.О. Нові проблеми, що стоять перед реалізацією безпеки персональних даних в Інтернеті;
- Олєйніков А.В. Оцінка функціональної та кібернетичної безпеки інфраструктури Інтернета речей системи SCADA.

Шифр зберігання НБУВ: В358088/2

***

Заболотна Ю. В. Проблеми взаємодії під час розслідування кіберзлочинів / Заболотна Ю. В., Іванко Є. Б. // Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція. - 2019. - Вип. 39. - С. 120-122.

Розглянуто особливості міжнародного співробітництва при розслідуванні кіберзлочинів. Зосереджено увагу на аналізі 5 груп злочинів: злочини, що спрямовані проти конфіденційності, цілісності та доступності комп'ютер-них даних, злочини, пов'язані з контентом (змістом), злочини, пов'язані з порушенням авторських прав, злочини, пов'язані із застосуванням комп'ютерних засобів та комп'ютерних систем, акти расизму і ксенофобії, що здійснюються за допомогою комп'ютерних мереж. Виділено ряд проблем, що виникають при боротьбі з кіберзлочинністю та запропоновано шляхи їх подолання.

Шифр зберігання НБУВ: Ж74042/юр.

***

Захист систем електронних комунікацій : навч. посіб. - Київ, 2019. - 163 с.

Розглянуто основи організації та порядок виконання робіт із захисту інформації в систем електронних комунікацій, порядок прийняття рішень щодо складу комплексної системи захисту інформації в залежності від умов функціонування систем електронних комунікацій і видів оброблювальної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

Шифр зберігання НБУВ: ВА839204

***

Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці : матеріали міжнар. «круглого столу» (Харків, 12 груд. 2019 р.). - Харків : Право, 2019. - 162 с.

Зі змісту:

- Неділько Я.В. Проблемні питання підслідності кіберзлочинів.

Шифр зберігання НБУВ: ВА839834

***

Інформаційна безпека: сучасний стан, проблеми та перспективи : матеріали І міжнар. наук.-практ. конф., 20 верес. 2019 р. - Київ : КПІ ім. І. Сікорського, 2019. - 123 с.

Зі змісту:

- Петров С.Г. До питання про класифікацію кіберзагроз;
- Янчук Ю.В. До питання загроз інформаційної безпеки у зв'язку з використанням технологій Інтернет речей;
- Дубняк М.В. Технологія DEEPFAKE: загроза інтелектуальній власності чи інформаційній безпеці?
- Каздовіна Ю.К. Питання державного регулювання контенту в Інтернеті;
- Цифра Г.О. Розвиток кіберстрахування:питання кібербезпеки.

Шифр зберігання НБУВ: ВА839476

***

Інформація, аналіз, прогноз - стратегічні важелі ефективного державного управління : матеріали XII Міжнар. наук.-практ. конф., 7 листоп. 2019 р. - Київ, 2019. - 267 с.

Зі змісту:

- Кравчук Т.А. Адміністративно-правові засади забезпечення кібербезпеки України.

Шифр зберігання НБУВ: ВА838474

***

Економіко-правові та управлінські аспекти розвитку суспільства: молодіжний погляд : матеріали міжнар. наук.-практ. конф., 01 листоп. 2019 р. - Дніпро, 2019. - Ч. 2. - 377 с.

Зі змісту:

- Солошенко М.О. Нові проблеми, що стоять перед реалізацією безпеки персональних даних в Інтернеті;
- Олєйніков А.В. Оцінка функціональної та кібернетичної безпеки інфраструктури Інтернета речей системи SCADA.

Шифр зберігання НБУВ: В358088/2

***

Теорія та практика публічного управління та адміністрування у XXI сторіччі : матеріали II Всеукр. наук.-практ. конф. за міжнар. участю здобувачів вищ. освіти та молод. вчених (Київ, 22 листоп. 2019 р.). - Київ, 2019. - 344 с.

Зі змісту:

- Арсенович Л. Організація підготовки фахівців у сфері кібербезпеки органів публічної влади;
- Грановський М. Державна політика у сфері забезпечення кібербезпеки – досвід Республіки Польща.

Шифр зберігання НБУВ: СО37009

***

Шемчук В.В. Захист інтернет-середовища як складник інформаційної безпеки держави: досвід Франції / Шемчук В.В. // Науковий вісник Ужгородського національного університету. Серія : Право. - 2019. - Вип. 57(2). - С. 49-52.

Розглянуто програмні документи щодо аналізу загроз і вироблення стратегій захисту кіберпростору. Окрему увагу приділено Стратегічному огляду оборони та національної безпеки 2017 р.

Шифр зберігання НБУВ: Ж68850/пр

***