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

№ 5 (травень)

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– №5 (травень) . – 137 с.

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

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

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

ЗМІСТ

«С февраля в Украине работает приложение «Дія», которое должно объединить все электронные услуги государства до 2024 года. Это воплощение обещания президента Владимира Зеленского сделать «государство в смартфоне». В «Дії» можно оплатить штрафы за нарушение правил дорожного движения или получить помощь при рождении ребенка. Сейчас «Дія» – среди лидеров самых популярных приложений в украинском Play Market и App Store – более двух миллионов загрузок. В то же время в команде разработчиков на сайте нет ни одного специалиста по кибербезопасности, а защите персональных данных посвящен только один абзац.

Автор издания «Заборона» Самуил Проскуряков разобрался, чем опасен главный цифровой проект Украины.

Как работает «Дія» и что это такое

«Государство в смартфоне», которое во время президентских выборов обещал украинцам Владимир Зеленский, стало реальностью зимой 2020 года. Публично мобильное приложение с цифровыми документами «Дія» (сокращенно от «Держава и я»), презентовали 6 февраля. Запускать главный цифровой проект страны приехал сам президент. Тогдашний премьер-министр Алексей Гончарук рассказал о планах оцифровать все государственные услуги за три года, а 50 основных – уже в 2020.

Скачать приложение можно бесплатно в App Store и Play Market. Идентификация пользователей происходит с помощью технологии BankID, а дальше «Дія» подтягивает данные из государственных реестров. ID-карта, биометрический паспорт гражданина Украины для выезда за границу, водительские права, техпаспорт и студенческий билет – все это загружается через динамический QR-код, который генерируется каждый раз, когда владелец его показывает, и действует в течение трех минут. На государственном портале «Дія» уже можно получить почти 30 публичных услуг онлайн, в частности, зарегистрироваться как физическое лицо-предприниматель, изменить деятельность и закрыть ФЛП, оформить справку о несудимости, помощь при рождении ребенка или ежемесячное возмещение стоимости услуг по уходу за ребенком до 3 лет. Также можно подать иск в суд, зарегистрировать авто или получить услуги, связанные с документами водителя, оформить ряд лицензий, разрешений или получить выписки из реестров.

Еженедельно разработчики добавляют новые функции и госуслуги. В частности, 22 апреля стали доступны цифровые паспорта, а для предпринимателей запустили онлайн-платформу «Дія.Бизнэс». Проектом занимается Министерство цифровой трансформации во главе с Михаилом Федоровым. Создавать приложения «Дія» помогали 35 специалистов-волонтеров от крупнейшей в Украине аутсорсинговой IT-компании EPAM Systems.

15 апреля Кабинет министров признал электронные загранпаспорта или ID-карты, загруженные в приложение «Дія», такими же полноценными документами, как и бумажные и пластиковые паспорта, которые они заменяют. Но в закон, который содержит перечень и вид документов, подтверждающих гражданство

Украины, соответствующие изменения так и не внесли. Это означает, что признавать документы в приложении могут только государственные учреждения, а не бизнес. То есть такой электронный паспорт могут не принять, например, в супермаркете.

Повышенная таинственность

«Поскольку приложение работает с чувствительными данными граждан, чтобы ему можно было доверять, его код должен быть открыт. Таким образом его можно просматривать и изучать, так независимые специалисты смогут проверить утверждение Минцифры о безопасности персональных данных», – объясняет Забороне политический хакер Украинского Киберальянса Шон Таунсенд.

Например, документация государственных цифровых услуг Сингапура доступна на одном из крупнейших веб-сервисов для совместной разработки программного обеспечения GitHub, там также есть украинская система электронных публичных закупок Prozorro и даже исходный код ядра Linux. Но нигде в открытом доступе нет документации и технического описания приложения «Дія».

К тому же код приложения прошел через процедуру обфускации, то есть запутывания, что затрудняет анализ и понимание алгоритма работы приложения. По словам Шона Таунсенда, запутывания кода достаточно распространенная практика, но в случае с государственным приложением следовало бы наоборот все опубликовать и объяснить, почему принятые именно такие технические решения…

Заборона не нашла информации о независимом аудите, а это базовое условие для проверки защищенности персональных данных. Есть только гарантиии самих разработчиков EPAM Systems и слова Федорова, что все под контролем. «Если аудит был, то где публичный отчет? Где техническая документация? «Мы старались» – это не результат, а хорошая эпитафия. Ее пишут на могильном камне, а не на сайте или приложении», – заключает политический хакер.

Заборона попросила предоставить Министерство цифровой трансформации Украины документацию и техническое описание, чтобы узнать, как реализована «Дія». Министерство не ответило нам в определенный законом пятидневный срок, но мы все равно ждем ответа.

У мечты президента много врагов «Украина – третья в Европе и десятая страна в мире, в которой есть электронные документы в смартфоне», – сказал министр цифровой трансформации Михаил Федоров. Но это далеко от правды. Эксперт рынка телекоммуникаций Роман Химич, председатель юридического департамента Лаборатории цифровой безопасности Вита Володовська и хактивист Шон Таунсенд рассказывают о семи подводных камнях приложения «Дія».

Хранить пароли и ключи в смартфоне ненадежно, ведь его можно легко взломать. Кроме этого, мошенники успешно похищают SIM-карты, а потом получают доступ к счетам в банке, к почте, паспорту и данным ФЛП. Это происходит так: абоненту звонят много раз, добиваются, чтобы он самостоятельно перезвонил. Затем заказывают у оператора услугу восстановления SIM-карты, когда для идентификации абонента его просят назвать несколько последних входящих или исходящих номеров.

Также иногда злоумышленники могут перечислить незначительные суммы средств на мобильный счет своей жертвы, чтобы точно знать дату последнего пополнения счета. Это глобальная проблема. Американский Bitcoin-предприниматель Майкл Терпин несколько раз терял сбережения, потому что у него украли мобильный номер. Даже после того, как он заказал у своего оператора VIP-статус с усиленной безопасностью, у него снова украли номер и сняли со счетов криптовалюту, которая стоила на тот момент 23 млн долларов.

Кражи через интернет-банкинг вообще стали обыденностью. В мессенджере Telegram появилось два бота, которые ищут персональные данные украинских пользователей, в том числе серию и номер паспорта, прописку и ИНН, по номеру телефона за деньги. Боты, скорее всего, берут данные с украденной базы пользователей «ПриватБанка».

В Украине в целом плохо с кибербезопасностью. В январе 2020 года произошла утечка персональных данных граждан, которые зарегистрировались на сайте career.gov.ua для прохождения конкурса на государственную службу. В свободном доступе оказались копии документов кандидатов, в частности паспортов.

Осенью 2019 СБУ вместе с киберполицией задержали группу «черных регистраторов». Они рассылали нотариусам электронные письма от имени государственных органов. В самых письмах были вирусы, таким образом получали удаленный доступ к компьютерам пользователей. Этот доступ мошенники использовали для того, чтобы снимать аресты по недвижимости в Государственном реестре. Группа предлагала заказчикам свои услуги, в частности через мессенджер Telegram, за сумму от 7 до 50 тысяч долларов. В то же время злоумышленники хорошо ориентировались, как снимать аресты по недвижимости, ведь некоторые из них работали в органах юстиции, на должностях государственных исполнителей. «Мы не можем доверять людям, которые регулярно лажают и призывают не делать из этого проблемы, – говорит Роман Химич. – Невозможно доверять данным, которые не защищены надлежащим образом, тем более если уже есть прецеденты успешных атак».

Пароли, подписи, ключи идентифицируют устройство, а не человека. В конце августа 2016 года в системе е-декларирования появилась поддельная декларация, заполненная неизвестным лицом от имени члена Нацагентства по предупреждению коррупции Руслана Рябошапки о том, что он якобы получил 25 миллионов гривен от фиктивной компании. Это не взлом: фальшивая электронная декларация была подписана настоящим электронным ключом, созданным госпредприятием «Украинские специальные системы». Виновные в подделке до сих пор не нашлись, а Государственная служба специальной связи и защиты информации (ГСССЗИ) и совсем не увидела необходимости в проверке центра сертификации ключей ГП «УСС».

«Двери не видят, кто вставляет ключ. Компьютер не видит, кто вводит пароль. Ваш ключ – это не вы. Если кто-то доберется до вашего телефона, то сможет получить цифровую подпись на ваше имя в «ПриватБанке» в режиме онлайн. И использовать ее с другого компьютера без вашего ведома», – объясняет Шон Таунсенд.

Слияние реестров облегчает бесконтрольный доступ к информации. В модели, когда вся информация объединена в общий банк данных, возникают новые риски. Так злоумышленники могут легче получить всю необходимую информацию, а не искать ее в разных реестрах. Таунсенд уверен, что копии паспортов, цифровых подписей и баз будут утекать как из незащищенных устройств пользователей, так и от безответственных и коррумпированных чиновников.

Государство и правоохранительные органы получают большое количество чувствительной информации – так открывается огромное пространство для злоупотреблений. В апреле 2019 диверсионная группа устроила неудачное покушение на украинского разведчика Кирилла Буданова. Машину выслеживали с помощью комплексной системы видеонаблюдения «Бэзпэчнэ мисто». В материалах суда указано, что доступ к системе предоставил сотрудник налоговой полиции Киева. За два года до этого боевик так называемой «Донецкой народной республики» Олег Шутов заложил взрывчатку под автомобиль сотрудника Главного управления разведки Минобороны Украины Максима Шаповала. Полковник погиб. По информации СБУ, машину также выслеживали с помощью «Бэзпэчного миста».

Государственные реестры работают плохо, однако их объединяют. Сам глава Минцифры Михаил Федоров признает, что техническое состояние государственных реестров ужасное. В то же время утверждает, что ведомство работает над наведением порядка.

Собеседник Забороны Роман Химич поясняет, что низкое качество реестров является следствием сложного комплекса проблем, на которые Минцифры не влияет. «О проблемах с реестрами персональных данных граждан известно как минимум лет десять. Речь идет о наличии множества ложных данных в пределах отдельно взятых реестров и, что особенно важно, несоответствия между персональными данными граждан в различных реестрах. Это делает сложным или невозможным массу, казалось бы, тривиальных задач вроде запроса данных о гражданине самими чиновниками. Поэтому в случае с приложением «Дія» мы имеем именно ситуацию цифровизации беспорядка, следствием чего будет уже цифровой беспорядок».

До сих пор нет закона для того, чтобы «Дія» легально работала. Председатель юридического департамента Лаборатории цифровой безопасности Вита Володовська говорит, что «Дія» вообще не предусмотрена ни одним законом, только постановлениями Кабмина. По закону, у каждого реестра есть отдельный администратор (чаще Минюст или Министерство внутренних дел). Информация из этих реестров передается в систему Минцифры и госпредприятия, которое обеспечивает функционирование приложения «Дія». Отсюда вопрос о законности обработки приложением и порталом персональных данных. Приложение, например, предусматривает возможность передавать данные третьим лицам, но не показывает, кому именно.

«Дія» на самоизоляции

7 апреля Минцифры презентовало «Дій дома» – приложение, которое позволяет мониторить, как граждане выполняют режим обсервации и самоизоляции. Похожие приложения есть в Китае, Сингапуре, Израиле и Польше.

Власти подчеркивают, что это приложение добровольное, но в описании на Google Play Market утверждалось, что «приложение в обязательном порядке устанавливается в смартфоны лиц, которые могут быть потенциальными носителями вируса COVID-19 и которые зарегистрированы в медучреждениях как нуждающиеся в самоизоляции или обсервации». Позже описание изменили на более нейтральное, «в обязательном порядке» исчезло.

Приложение проверяет фотографии лица и геолокации мобильного телефона в момент фотографирования. После установки «Дій дома» в случайные промежутки времени в течение дня пользователь получает push-сообщения. После этого нужно обязательно сделать фото своего лица в течение 15 минут.

В случае несоответствия геолокации или фотографии, отсутствия связи с мобильным приложением, удаление, установление ограничений по передаче информации с помощью мобильного приложения, в органы Национальной полиции направляется уведомление о случае нарушения условий самоизоляции. И уже правоохранители будут решать, надо ли приехать и проверить.

До 8 апреля пользование приложением было добровольным, после – стало обязательным для потенциально больных, вернувшихся из-за рубежа. Есть риск, что это приложение могут начать использовать для тотального контроля». ***(Об Уязвимостях Проекта «Дія» // INDEPENDENT MASSMEDIA LLP (https://job-sbu.org/ob-uyazvimostyah-proekta-diya-87566.html). 08.05.2020).***

***

«У дослідженні компанії Fabrizio Ward, проведеному для Visa, повідомляється, що у кожного восьмого українця – один пароль для входу в усі облікові записи, 54% опитаних використовують кілька різних, але не унікальних паролів, а унікальний пароль для кожного облікового запису є у 34% опитаних громадян. Враховуючи ці факти, а також чат-ботів у телеграмі, які торгують персональними даними, можна говорити, що в країні явні проблеми з цифровою безпекою.

Директор компанії RMRF, яка спеціалізується на сервісах з кібербезпеки для бізнесу, Сергій Аветісян написав для “Гетьмана” рекомендації підприємцям щодо цифрової безпеки, програмного забезпечення та навчання співробітників.

Перш за все, слід зрозуміти, що малий і середній бізнес цікавий кіберзлочинцям не менш, ніж великий. Згідно звіту Verizon, у 2019 році 43% атак було націлено саме на малий і середній бізнес. Звичайно, це не складні таргетовані кібератаки, а масові. Вони можуть бути націлені на:

- крадіжки персональних і платіжних даних користувачів
- отримання доступу до елементів інфраструктури компанії (сервери, робочі станції) для здійснення шкідливої активності.

Цей список не є вичерпним. Більш того, наслідки кібератаки для організації можуть бути критичними. Згідно того ж звіту, 60% підприємств малого й середнього бізнесу, що зазнали кібератаки, завершили діяльність протягом шести місяців після атаки.

“Безкоштовні антивіруси або VPN – це лише ілюзія захисту”

Очевидно, що підхід «встановили антивірус і можемо спати спокійно» є застарілим, недієвим і навіть шкідливим. Щодня світ дізнається про нові вразливості у ПЗ, які використовуються кіберзлочинцями для нових атак. Техніки й інструменти кіберзлочинців стають дедалі більш досконалими.

Тепер щодо практичних порад. Безкоштовні антивіруси або VPN – це лише ілюзія захисту. Перші використовують застарілий сигнатурний метод захисту, а другі створені радше для аналізу трафіка, ніж для його захисту.

Сьогодні є достатня кількість інструментів захисту, що розповсюджується за передплатою. Наприклад, для захисту сайтів і веб-застосунків можна використовувати доступний і популярний інструмент Cloudflare. Якщо потрібен більш широкий функціонал, то радимо ознайомитися з рішеннями сімейства Imperva. Обидва вендори досить гнучкі і дозволяють підібрати рішення відповідно до потреб і можливостей бізнесу.

Слід зазначити, що еволюція моделі за передплатою пішла ще далі. На Заході популярні компанії які дозволяють малому і середньому бізнесу за абонплату отримати доступ до продуктів захисту рівня enterprise, а також послуги інженерів з кібербезпеки, яких найняти в штат малий бізнес просто не може собі дозволити.

Хостинг-провайдери та мережеві провайдери

Обираючи хостинг-провайдера чи мережевого провайдера, поцікавтеся щодо захисту їхньої мережевої інфраструктури. Адже саме через них будуть проходити ваші дані і трафік.

Взагалі, при роботі із третіми сторонами треба дуже чітко продумувати обмеження доступу, а також слідкувати за тим, щоб усі цифрові активи належали компанії або її власнику. До цифрових активів належать не лише домен і хостинг веб-сайту. На жаль, трапляються випадки, коли після завершення співпраці з агенцією, компанія втрачає доступ до своїх рекламних кабінетів.

Окрім недобросовісних підрядників, доступ до онлайн-сервісів, що використовуються співробітниками компанії може бути вкрадений зловмисниками. Для захисту корпоративного доступу в онлайн-сервіси і хмари теж існує певний клас рішень. Наприклад, One Identity Starling Connect. Це SaaS-продукт, який, окрім належного рівня захисту, є достатньо простим в адмініструванні.

Навчання співробітників

Люди є одночасно головним активом і головною вразливістю бізнесу. Фішинг (вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних) на сьогодні є найпоширенішим вектором атак на бізнес. Тому тренінги персоналу з кібербезпеки є обов’язковими для будь-якої організації.

Ці тренінги можуть включати таку інформацію, про те, як розпізнати фішингові повідомленя, алгоритм поведінки у разі аномальних дій на робочій станції, правила користування пристроями за межами корпоративної мережі тощо.

В завершення, можемо сказати, що бізнес має усвідомити, що кібербезпека варта такого ж рівня уваги, як і інші процеси. Так, жоден набір інструментів не дає 100% захисту від зламу, але тут ми проводимо аналогію із захистом помешкання. Зламати можна будь-який замок, але це не привід лишати двері відкритими. Так само треба усвідомлювати, що кібератака може статися будь-ким і треба мати

«План Б» на її випадок». ***(Цифрова безпека бізнесу: як підприємцям захиститися від кібератак та витоків даних // Гетьман (http://www.getman.media/tsyfrova-bezpeka-biznesu-yak-pidpryyemtsyam-zahystytysya-vid-kiberatak-ta-vytokiv-danyh/). 12.05.2020).***

***

«В умовах карантину на кафедрі "Управління інформаційною та кібернетичною безпекою" згідно концептуально нової освітньої моделі «12 кроків до якісної освіти» триває вивчення професійної англійської мови. У процесі дистанційного навчання використовуються нові форми і методи роботи.

Так, студенти груп УБД-31 та УБД-41 під керівництвом доцента кафедри Мужанової Т.М. провели дослідження англомовних публікацій щодо загроз кібербезпеці та напрямів їх протидії в умовах коронавірусу, розміщених в мережі Інтернет.

Студенти підготували анотації статей англійською та українською мовами, в яких виклали основні тези публікацій. Загалом підготовлено понад 20 робіт, кращі з них представлені нижче.

Пропонуються висновки, до яких прийшли молоді дослідники.

Отже, науковці та практики у сфері кібербезпеки виділяють такі основні виклики, які постали перед фахівцями з кіберзахисту внаслідок пандемії коронавірусу.

Переорієнтація зусиль хакерів на працівників, які в умовах карантину працюють удома.

Зростання обсягів фішинг-атак з метою завантаження шкідливого програмного забезпечення або заволодіння чужими обліковими даними.

Збільшення кількості нападів програм-вимагачів, в тому числі на лікарні та лабораторії, що працюють над коронавірусом…». ***(ЗАГРОЗИ КІБЕРБЕЗПЕЦІ В УМОВАХ КОРОНАВІРУСУ: СТУДЕНТСЬКІ ДОСЛІДЖЕННЯ ОСТАННІХ ПУБЛІКАЦІЙ В МЕРЕЖІ ІНТЕРНЕТ // Державний університет телекомунікацій (http://www.dut.edu.ua/ua/news/1/category/0/view/8386). 20.05.2020).***

***

«Дізнатися як захистити свій аккаунт від шахраїв, отримати рекомендації та повідомити про злочин в сфері кібербезпеки тепер можна в месенджері Telegram. Всі повідомлення громадян обробляються провідними фахівцями та поліцейськими.

Проєкт «Cybercentre» ініційований доцентом кафедри юридичних дисциплін к.ю.н. Ольгою Ковальовою в рамках співпраці команди курсантів та фахівців Донецького юридичного інституту МВС України з відділом протидії кіберзлочинам в Донецькій області Департаменту кіберполіції Нацполіції України та реалізується за підтримки Європейського Союзу, громадської організації "Фонд "Професійний розвиток Харкова" та UPSHIFT Україна.

Під керуванням доцента кафедри юридичних дисциплін к.ю.н. Ольги Ковальової курсанти організували команду та створили чат-бот з медіабезпеки.

Мета телеграм-каналу «Cybercentre» - інформувати населення про злочини у кіберпросторі. Окрім того, користувачі можуть безпосередньо повідомити про протиправні дії щодо особистих даних у соціальних мережах та отримати алгоритм дій, який допоможе відновити медіабезпеку.

Приєднатися до каналу можна за посиланням https://t.me/Cybercentre_bot...». ***(Курсанти ДЮІ МВС України спільно з кіберполіцейськими Донеччини презентували чат-бот з підвищення безпеки в мережі // СтопКор - антикорупційні новини України (https://stopcor.org/kursanty-dyui-mvs-ukrayiny-spilno-z-kiberpoliczejskymy-donechchyny-prezentuvaly-chat-bot-z-pidvyshhennya-bezpeky-v-merezhi/). 19.05.2020).***

***

«Штрафуют ли чиновников за «слив» персональных данных в Украине? Распространение какой информации о больных COVID-19 является нарушением медицинской тайны? Может ли судиться с государством нашедший свои персональные данные в телеграмм-боте , скандал вокруг которого вылился в уголовное дело и зацепил приложение «Дія»?..

«Сливы» года

В 2019 году количество случаев утечки данных в США выросло на 17% — до 1473, сообщает Identity Theft Resource Center — неприбыльная организация, которая фиксирует нарушения использования персональных данных.

С 2005 года центр зафиксировал около 10 000 нарушений. Наибольший скачок, по данным ITRC, состоялся в 2018-м — количество записей потребителей, подвергшихся нарушений распространение своих данных, выросло на 126%.

Самым скандальным в прошлом годду был несанкционированный доступ к 383 миллионов записей базы клиентов одной из ведущих компаний США на рынке гостиничных услуг Marriott International, включая номера паспортов, платежных карточек и тому подобное.

Средняя общая стоимость убытков, которые несет американский бизнес от утечек данных составляет около $8 200 000, согласно исследованиям IBM Security совместно с Ponemon Institute , основанных на опросе 500 компаний из 16 штатов в 2019 году. И наибольшие потери несет медицина — $6 420 000.

В странах Европейского Союза с мая 2018 вступил в силу Общий регламент защиты данных (General Data Protection Regulation — GDPR) всех лиц в пределах Европейского Союза и Европейской экономической зоны. Регламент также касается экспорта персональных данных за пределы ЕС и ЕЭЗ.

По итогам первого года функционирования GDPR , надзорные органы стран европейской экономической зоны зафиксировали более 144 тыс запросов и жалоб и более 89 тыс нарушений данных . 63% из них были закрыты, а 37%, по состоянию на май 2019-му, — продолжались, сообщала Еврокомиссия.

Рост запросов и жалоб связан, в первую очередь, с осведомленностью граждан ЕС с правами на защиту своих данных. Так, согласно опросам Еврокомиссии в 2019 году , 67% опрошенных слышали о GDPR, 36% из них знали, что влечет за собой невыполнение регламента. Такой показатель вырос на 20% по сравнению с результатами такого же опроса в 2015 году.

В результате введения GDPR, в январе этого года итальянский надзорный орган наложил два штрафа в размере 8,5 и 3 млн евро на итальянского поставщика электроэнергии и газа Eni Gas e Luce (EGL).

Первый — за то, что компания незаконно обрабатывала личные данные, осуществляя маркетинговые звонки лицам, отказавшимся от получения таких звонков. Второй — за то, что EGL заключала контракты с более 7 тыс клиентов без их уведомления. Они узнавали об этом по большей части после получения первого счета от компании.

А в начале мая шведский орган управления защиты данных (DPA) наложил штраф в размере 75 млн. шведских крон (примерно 7 млн евро) на Google как оператора поисковой системы за невыполнение требований GDPR по изъятию персональных данных за неточности или поскольку такая информация была лишней.

По сравнению с Европой и США, защита персональных данных в Украине сводится в большинстве к единичным жалобам и судебным искам.

Так, количество утечек данных фиксирует Уполномоченный по правам человека. Все могут также пожаловаться на нарушение своего права на защиту данных непосредственно в полицию или в суд.

Как отмечается в ежегодном отчете за 2019 , омбудсмен рассмотрел 1061 сообщение о нарушении права на защиту персональных данных. Составлено и направлено в суд всего 10 (!) Протоколов об административном правонарушении по части четвертой статьи 188-39 Кодекса об административных правонарушениях (нарушение законодательства в сфере защиты персональных данных).

Больше всего такие нарушения фиксировались в сферах финансовых и банковских услуг, страхования, жилищно-коммунальных услуг, здравоохранения, социальной защиты, образования, а также при обработке персональных данных при осуществлении видеонаблюдения, учете административных и уголовных правонарушений.

В комментарии изданию LB.ua представитель Уполномоченного в сфере защиты персональных данных Инна Берназюк пояснила, что небольшое количество составленных протоколов об административных правонарушениях вызвано, прежде всего, тем, что законодательством ограничены сроки привлечения к ответственности (три месяца со дня совершения), а обращение основном поступают в секретариат Уполномоченного уже после пропуска сроков.

И омбудсмен не может самостоятельно установить, кто занимается распространением или «сливом» данных. А обращается в полицию.

В свою очередь, по данным Департамента киберполиции , в течение 2018 полицейские обнаружили 6000 преступлений, совершенных в сфере использования высоких информационных технологий. 7% из них — продажа и анализ похищенных баз данных.

Омбудсман также проводит проверки распорядителей персональных данных. За прошлый год таких было 36 и 26 предписаний об устранении нарушений.

Если требования Уполномоченного не выполнены, он может составить протокол об административном правонарушении. В 98% случаев, отмечает Инна

Берназюк , предписания выполняются, или должностные лица просят Уполномоченного продлить срок их выполнения.

Юрист Назар Коршивский отмечает, что для полноценной защиты персональных данных граждан Украины средств омбудсмена недостаточно: в отделе проверок — четыре человека, в общем соответствующий департамент насчитывает 17 работников.

«Этого явно недостаточно для надлежащего контроля. В дополнение законодательная ограниченность — омбудсмен не может сам привлечь виновных к ответственности, только суд. Также относительно низкий уровень штрафов. Если в Европе это десятки, сотни, а иногда миллионы евро, у нас штраф (если не принимать во внимание уголовной ответственности) может составлять до 8500 грн. Такие штрафы отнюдь не соразмерны с расходами, которые должна понести компания для внедрения необходимых технических и организационных мер по защите данных», — отмечает он.

По мнению юриста, в Украине еще не сформирована культура защиты и ответственного отношения к персональным данным.

«В Европе отношение компании к персональным данным — одно из определяющих конкурентных преимуществ. Утечка данных может нанести удар по репутации, которые не сравнится ни с одним штрафом (даже учитывая размер штрафа в ЕС). Компании в США и ЕС идут на «мировые» соглашения с потребителями и готовы возмещать им убытки только, чтобы не получить огласку по делу. В Украине же компании часто совсем не занимаются вопросами защиты персональных данных», — отмечает Коршивский.

Чувствительность данных

И украинским, и европейским законодательством «персональные данные» определены как сведения или их совокупность о физическом лице, по которым оно идентифицировано или может быть идентифицировано (Закон «О защите персональных данных»).

Так называемые «нечувствительные» персональные данные — фамилия, имя, отчество, адрес, телефоны, паспортные данные, национальность, образование, семейное положение, религиозные и мировоззренческие убеждения, состояние здоровья, материальное положение, дата и место рождения, место жительства и пребывания и т.д., данные о личных имущественных и неимущественных отношениях этого лица с другими лицами.

К «чувствительным» данных относят персональные данные , которые раскрывают расовое или этническое происхождение, политические, религиозные или иные убеждения; сведения касающиеся здоровья или половой жизни; данные об уголовном осуждении.

Заметим, что украинским законодательством четко не определен перечень персональных данных. Европейское — содержит следующий перечень данных , которые считаются персональными:

- имя и фамилия;
- домашний адрес;
- электронный адрес,
- номер удостоверения личности;

- данные о местоположении (в том числе, функция данных о местонахождении на мобильном телефоне) адрес интернет-протокола (IP) идентификатор файла cookie;
- рекламный идентификатор телефона;
- данные больницы или врача, которые могут быть такими, которые однозначно идентифицирует человека.

Для получения разрешения на обработку персональных данных:

— человек не должен испытывать давления;

— должен быть надлежащим образом информирован о цели и последствия предоставления согласия;

— границы распространения его согласия должны быть конкретными и разумными.

То есть данные лица можно обрабатывать только в случае, если оно само дало на это согласие, или в соответствии с законодательством (в основном речь идет об оперативно-розыскной деятельности, хотя и это — с разрешения суда).

«Проблема в том, что для разработки любой базы данных привлекают в основном связанных с руководством этой структуры лиц, иногда еще и не очень профессиональных. Соответственно — плохое качество продукта. То есть человеческий фактор срабатывает дважды: первый раз — при разработке, второй раз — когда возникает соблазн скачать эту базу, поскольку в основном работники, имеющие к ней доступ, получают три копейки зарплаты», — отмечает в комментарии LB.ua Павел Белоусов , эксперт Школы цифровой безопасности .

Адвокат Оксана Кочкодан добавляет:

«Данные сливают, потому что за них можно получить хорошую оплату, а за их безопасность на практике отвечают все и никто. Должным оразом защищать данные должен и владелец, он же контроллер (кто определил цель обработки), и распорядитель, он же процессор (тот, кто обрабатывает данные с разрешения контроллера). В государственных органах должны быть целые подразделения или ответственные лица, отвечающие за безопасность персональных данных (ст.24 ЗУ О защите персональных данных). Государственные органы также обязаны иметь сертификаты КСЗИ (комплексной системы защиты информации — LB.ua), это что-то похожее на сертификаты безопасности ISO, но не так пафосно, потому отечественно. Но все время где-то что-то кто-то сливает. И прежде всего потому, что защитить данные в Украине эффективно невозможно».

Законом «О защите персональных данных», как и европейским законодательством определено, что обработка персональных данных осуществляется для конкретных и законных целей, а также открыто и прозрачно.

Объем и содержание данных, которые собираются, должны быть не чрезмерными относительно цели их обработки. И храниться они могут не дольше, чем это необходимо для законных целей, для которых их собирали.

«И в украинском, и в европейском законодательстве содержится гарантия — персональные данные, которые собираются, не могут быть чрезмерными относительно цели их сбора. Если ее можно достичь с помощью меньшего количества данных, то такие действия являются чрезмерными. То есть контролирующие органы должны провести проверку, наложить штраф и

предписание в таком случае, а затем проконтролировать, как было выполнено предписание. Если нет, то — штраф в двойном размере. Так работают в Европе. В Украине — нет. Именно поэтому у нас появляются телеграмм-боты с персональными данными», — отмечает Ирина Кушнир , эксперт по защите персональных данных.

Следовательно, отмечает она, любой, кто зафиксировал распространение своих персональных данных в телеграмм-боте «UA База» , скандал вокруг которого задел и приложение «Дія», может подавать в суд. Сначала украинский, а затем и Европейский суд по правам человека.

«Для такого иска необходимо в национальных судах доказать, что определенная персональная информация была открыта, а ее хранения относится к ответственности конкретной государственной структуры. И вам все равно, какое должностное лицо за это несет ответственность. Государство должно было обеспечить сохранность ваших данных. А поскольку нарушило, то имеете право требовать компенсацию», — отметила Кушнир.

«Баги» реестров

Довольно часто, отмечают эксперты, такие «нечувствительные» сведения, как имена пользователей и пароли, становятся целями для хакеров, поскольку люди используют их для защиты «чувствительных» — например, финансовых счетов. Немало лиц повторно используют одни и те же учетные данные или подобные для удобства запоминания.

Почему данные настолько уязвимы? Обычно, из-за плохих мер безопасности. Несмотря на общий рост расходов на кибербезопасность, многие компании (а украинские госструктуры и подавно) пренебрегают необходимостью регулярно обновлять и совершенствовать свои базы данных, менять устаревшую технику, нанимать квалифицированных специалистов.

«Продают все: номера телефонов, имейлы, паспортные данные … Это было и раньше, просто сейчас информацию можно купить в большем количестве и не только одного региона, как было раньше, а нескольких или по всей Украине, — говорит хакер Алексей (имя изменено), с которым удалось пообщаться LB.ua. — На самом деле это стоит довольно дешево. Но работники определенных структур, имеющих эти базы, соблазняются на эти деньги, потому что зарплаты у них — мизерные».

Он, говорит, часто писал государственным структурам о «дырах» в их реестрах, через которые профессиональные хакеры могут получить доступ, но там не реагировали.

«В Украине не привыкли нормально оплачивать работу, а нанимают студентов, платят им минималку и хотят при этом создать защищенную базу. Или вообще использовать открытые платформы. Понятно, что этот код — несовершенный и всем доступен. Сломать его — вообще не проблема», — отметил он.

Чтобы замести следы, говорит Алексей, достаточно часто создают телеграмм-боты с открытыми данными, «связывая его с «облачными» сервисами где-нибудь в Индии или любой другой стране».

«Делают переадресацию, чтобы данные переходили с одного сервиса на другой, с защитой связей между ними … Есть также немало обменников, чтобы спрятать следы транзакций. Оплата может быть в биткоинах, Perfect Money (электронная платежная система, зарегистрированная в Панаме — LB.ua) можно перевести их в «эфиры» (Ethereum, — LB.ua) или «паеры» (Payeer, — LB.ua) и так далее . А «концы» спрятать где-то в России. Кто будет сейчас выезжать из Украины туда, чтобы разбираться?», — предполагает он.

Программист Тарас (имя изменено) отмечает, что в основном на разработку программного обеспечения или баз данных для государственных структур соглашаются специалисты низшего уровня — «Джуниор». «Мидл» или «Синиоры» — имеют немало высокооплачиваемых предложений от коммерческих компаний.

Обычно, работник компании, работающей над созданием определенного программного обеспечения, имеет доступ и к персональным данным лиц. Впрочем, в частных компаниях они подписывают NDA (Non-disclosure Agreement) — соглашение о неразглашении — с четкими и, как правило, жесткими условиями выполнения заказа. А значит, несут ответственность в случае их нарушения.

Коронавирусная правда

Пандемия коронавируса поставила под угрозу защиту персональных данных, связанных со здоровьем. Они могут подлежать обработке в случаях, когда ставят под угрозу, в частности, интересы общества по охране здоровья, предотвращение распространения коронавирусной инфекции и тому подобное. В частности, GDPR позволяет это делать для научных исследований. Хотя только после согласия человека. По возможности такие данные должны быть анонимизированы и храниться определенное время под контролем и ответственностью тех, кто имеет к ним доступ.

В свою очередь, в Украине парламент принял изменения в Закон «О защите населения от инфекционных болезней» в середине апреля этого года, которым временно (на период карантина и до 30 дней после его отмены) разрешается обработка персональных данных граждан, заболевших COVID-19 без их согласия.

В частности, разрешается обработка данных, касающихся состояния здоровья, места госпитализации или самоизоляции, фамилии, имени, отчества, даты рождения, места жительства, работы (учебы) … «при условии использования таких данных исключительно в целях осуществления противоэпидемических мероприятий ».

В течение 30 дней после окончания карантина такие данные подлежат обезличиванию, а в случае невозможности — уничтожению.

Эти нормы применяются и для использования мобильного приложения «Дій вдома» для мониторинга соблюдения самоизоляции или обсервации гражданами, прибывших из-за рубежа, с подтверждением или подозрением на COVID-19.

По состоянию на начало мая этого года, этим приложением воспользовались более 32 000 физических лиц, сообщает Министерство цифровой трансформации.

По словам эксперта Олега Заярна , министерство должно было утвердить отдельный порядок обработки персональных данных в приложении «Дій вдома», предварительно согласовав его с Уполномоченным. Кроме того, остается открытым вопрос, что будет с персональными данными тех, кто пользовался приложением,

после обнародования официального решения об отмене карантина. Поскольку в вышеупомянутом законе говорится, что данные могут быть либо уничтожены, либо обезличенны.

По мнению Ирины Кушнир, даже в условиях противодействия распространению коронавируса важно, чтобы обнародованые данные больных в совокупности не приводили к возможности их идентификации.

«Есть отдельные данные, обнародовав которые по крайней мере узкий круг лиц идентифицирует человека. Если сообщают, к примеру, что в Дарницком районе заболело столько-то людей, то идентификации не произошло. В этом районе проживает много людей. Впрочем, если говорят о маленьком городке, где называют конкретный адрес и еще и дату рождения или профессию, то его жители узнают, о ком идет речь», — объясняет она, отмечая, что в таком случае речь идет о распространении персональных данных.

По ее мнению, чтобы соблюдалось по крайней мере действующее законодательство по защите персональных данных, нужно привлекать к ответственности тех, кто его нарушает.

«Иначе не будет обеспечено сдерживающего эффекта. Все будут знать, что данные могут разгласить или продать, и никто не понесет ответственности за это», — добавляет она.

Скупая судебная практика

Украинским законодательством предусмотрена разная ответственность за нарушение прав человека на защиту персональных данных. В частности:

— административная (если произошел незаконный доступ к данным, возможен штраф в размере от 1700 до 8500 грн, а если это произошло по вине должностного лица — штраф от 5100 до 17000 грн)

— дисциплинарная (выговор или увольнение работника, допустившего такое нарушение)

— гражданско-правовая (лицо, чьи права на защиту персональных данных были нарушены, может обратиться с требованием или иском в суд о возмещении ему имущественного и/или морального вреда, причиненного нарушением)

— уголовная (ст. 182 Уголовного кодекса (нарушение неприкосновенности частной жизни), но речь идет только о умышленных действиях):

- штраф от 8500 грн до 17000 грн, или
- исправительные работы на срок до 2 лет, или
- арест на срок до 6 месяцев, или
- ограничение свободы на срок до 3 лет (в отдельных случаях на срок от 3 до 5 лет), или
- в отдельных случаях лишения свободы от 3 до 5 лет.

Хотя журналистам LB.ua не удалось найти судебные решения, где кого-то оштрафовали бы на значительную сумму или арестовали за нарушение права на защиту персональных данных. В основном речь идет об устранении нарушения.

Так, в феврале прошлого года Верховный Суд увидел нарушения прав чиновницы Чопского горсовета по защите ее персональных данных. В марте 2015 года ее фото было опубликовано в одной из местных газет «с лицом мужского пола» без ее разрешения. Суд подтвердил решение первой инстанции, которым

признал, что публикация этого фото касается личной жизни чиновницы и не несет никакой роли для общества, а следовательно, не могла быть опубликована без его согласия.

В марте этого года Верховный Суд отменил решения предыдущих инстанций и отправил на новое рассмотрение дело в отношении видеонаблюдения. В частности, истец жаловался на то, что его сосед достроил пристройку к своему дому и установил четыре камеры, две из которых направлены в сторону его участка, что является нарушением права на частную жизнь. Нижестоящие инстанции приняли решение, указав, что истец не предоставил достаточных доказательств. Впрочем, кассация увидела нарушения при рассмотрении этого дела и отправила его на новое рассмотрение.

Львовский окружной админсуд в январе прошлого года признал нарушением прав истца и обязал Министерство внутренних дел удалить из баз данных информацию о сообщении ему три года назад о подозрении в уголовном правонарушении, поскольку другой суд закрыл это производство.

Суд признал, что после закрытия дела хранения этой информации является вмешательством в его право на уважение частной жизни, и не соответствует критерию «по закону».

Единый реестр судебных решений содержит также немало жалоб к омбудсмену на ненадлежащее рассмотрение заявления о нарушении прав человека. Так, одно из них касалась публикации Анатолием Матиосом на его странице в Facebook запроса на доступ к публичной информации, содержащий персональные данные истца. Суд оставил заявление без движения, давая истцу возможность исправить допущенные ошибки в жалобе.

По итогам прошлого года Офис омбудсмена сообщил о передаче Высшей школой адвокатуры Национальной ассоциации адвокатов Украины персональных данных (фамилии, имена, номера телефонов, адреса электронной почты, IP-адреса, регион, дата и время входа, а также при наличии должности, названия компаний, профили facebook и фото) адвокатов, помощников адвокатов, стажеров адвокатов, а также других лиц без их ведома и однозначного согласия.

Во время проверки было установлено, что Высшая школа адвокатуры НААУ фактически осуществляет обработку персональных данных онлайн-курсов в электронном виде с помощью онлайн-платформы www.antitreningi.ru, хостинг которой физически находится на территории Российской Федерации, а непосредственная регистрация пользователей и оплата услуг осуществляется через онлайн-форму, хостинг которой находится на территории Германии.

В феврале этого года Подольский райсуд Киева закрыл это производство , не увидев в действиях Высшей школы адвокатуры состава административного правонарушения. В частности, ссылаясь на позицию ответчика, представители омбудсмена не анализировали программный код сайта, а потому не доказали самого факта передачи данных или российской, или немецкой компании.

И снова — Конституция

По словам Ирины Кушнир , в парламенте создана рабочая группа по наработке изменений в Конституцию и Закон «О защите персональных данных» для создания отдельного органа по защите данных.

«Чтобы этот орган действовал независимо, его надо вывести из-под контроля исполнительной ветви власти, чтобы он мог проверять, давать предписания, штрафовать и тому подобное. А это требует внесения изменений в Конституцию», — отметила она.

Эту информацию подтвердил LB.ua и сопредседатель рабочей группы, депутат фракции «Слуга народа» Тарас Тарасенко.

«Сейчас юридическое сообщество дискутирует, нужны ли изменения в Конституцию, достаточно ли внести изменения подзаконными актами … Впрочем, большинство склоняется к мысли, что для создания отдельного органа для полноценной защиты персональных данных, все же нужны изменения в Конституцию. Чтобы этот орган мог проводить расследование, налагать штрафы и т.д.», — отметил Тарасенко.

По его словам, параллельно рабочая группа нарабатывает новую редакцию Закона «О защите персональных данных», учитывая европейский GDPR. И планирует через полторы-две недели представить проект изменений.

Его коллега по этой группе, депутат от «Слуги народа» Егор Чернев, отмечает, что пока неизвестно, в Украине будет работать такой персональный или коллегиальный орган. «Рассматриваются различные варианты: возможно, это будет Информационный комиссар или комиссия, или комитет … Есть разная практика Европейского Союза», — добавил он.

А тем временем эксперты советуют:

- не передавать свои данные без соответствующего запроса;
- не давать доступ к данным непроверенным источникам;
- читать политику конфиденциальности сайта или компании перед тем как передавать данные;
- создавать надежные пароли и менять их время от времени.

И самое главное — интересоваться своими правами для защиты персональных данных и в случае необходимости защищать их. ***(Виктория Матола. «Утечки» из государственных реестров, или как защитить персональные данные // Антикор (https://antikor.com.ua/articles/381760-utechki_iz_gosudarstvennyh_reestrov_ili_kak_zashchititj_personaljnye_dannye). 20.05.2020).***

***

ГП «Отраслевой центр цифровизации и кибербезопасности» Министерства инфраструктуры заказало ООО «Софтлист» программное обеспечение «облачных» услуг на 28,3 млн гривен…

К июлю поставят и внедрят программный комплекс по созданию отраслевой системы комплексного контроля и мониторинга кибербезопасности на транспорте «I-Cyber». Срок действия лицензий на использование софта и срок пользования мощностями обработки и хранения данных в сфере информатизации облачного центра обработки данных «De Novo» составляют год.

Столичным дата-центром «De Novo» владеет одноименное ООО «Де Ново» кипрской компании «ДеНово Оверсиз Холдингз Лимитед» бизнесмена Евгения Уткина.

По спецификации, подсистема обнаружения и реагирования на киберугрозы (уровень конечных точек) MVISION EDR 1: 1 BZ 30 Day Storage стоит 845 гривен за штуку. В США такой софт с различными номерами производителя MV4ECE-AA — ** продается по 26-34 доллара, или 689-924 гривен. Ценовое предложение победителя «Софтлист» на 5,5% ниже ожидаемой стоимости закупки.

ООО «Октава киберзащиты» не допустили к торгам за отсутствие писем от производителей, представительств или дистрибьюторов софта с подтверждением статуса официального партнера и срока поставки. Также фирма не предоставила аттестат облачного ЦОД и / или экспертное заключение Госспецсвязи об обеспечении защиты информации, а также экспертное заключение Госспецсвязи о соответствии софта требованиям нормативных документов. При этом фирма жаловалась в АМКУ на дискриминацию и соперников. Конкурентами были ООО «Оптидата», ООО «Гартен-Консалтинг» и ООО «Кубит».

Компания «Софтлист» принадлежит Дмитрию Прокопенко, Максиму Ролику и Дмитрию Козяревичу, которые также владеют ООО «Идеалсофт». Прокопенко и Козяревич владеют ООО «Тлумево». Кроме того, Козяревич еще и руководит ООО «Украинский национальный антивирус» Валентины Ждановой, Сергея Невдала и Оксаны Щегловой.+

Отмечается, что «Софтлист» вместе с ООО «Телекарт» фигурируют в уголовном производстве прокуратуры по покупке КП «Информатика» комплекса «Единый диспетчерский центр мониторинга работы транспорта и сбора информации» по цене, которая могла быть завышенной». **(Ирина Жменова. Предприятие Мининфраструктуры купило систему кибербезопасности на транспорте за 28 млн гривен // 368.media (https://368.media/2020/05/13/predpriyatie-mininfrastruktury-kupilo-sistemu-kiberbezopasnosti-na-transporte-za-28-mln-griven/). 13.05.2020).**

***

«Україна потребує нових підходів і концепції в сфері національної безпеки, оскільки в майбутньому можливі біологічні війни і конфлікти в космосі.

Таку думку висловив секретар Ради національної безпеки і оборони Олексій Данілов під час зустрічі з тимчасовим повіреним у справах США в Україні Крістіною Квін, передає прес-служба РНБО.

Сторони обговорили стан співробітництва в секторі оборони і розширення партнерства в області кібербезпеки.

"У цьому напрямі ми рухатися максимально швидко. Наступні війни – це війни кібернетичні, біологічні та протистояння в космосі, що вимагає від держави принципово нових підходів і концепцій у сфері національної безпеки", – заявив Данілов». ***(У РНБО побоюються "біологічних воєн і протистоянь в космосі" // Рубрика (https://rubryka.com/2020/05/30/u-rnbo-poboyuyutsya-biologichnyh-voyen-i-protystoyan-v-kosmosi/).***

***

«26 травня 2020 року Міністерство цифрової трансформації разом із НКЦК при РНБО, компанією з кібербезпеки 10Guards, компанії Cyberlab і компанією Moneyveo презентували новий освітній серіал «Кіберняні».

Освітній серіал складається з 10 серій тривалістю 4-11 хвилин і дозволить дізнатися, як мінімізувати ризики втрати вашої приватної важливої інформації. Також у ньому розповідається, як попередити кібератаку або кібершахрайство та як швидко відновитися після них у випадку, якщо вони все ж таки сталися.

Участь у серіалі взяв Костя Клепка, креативний продюсер і режисер YouTube-каналу «Чоткий Паца». У якості експертів виступили Віталій Якушев, директор компанії з кібербезпеки 10Guards; Юрій Мелащенко, партнер компанії з кібербезпеки Cyberlab, радник секретаря РНБО на громадських засадах з питань кібербезпеки; Альона Андронікова, директор Moneyveo; Тарас Кучерявий, керівник відділу Brand Management Moneyveo.

Під час презентації серіалу заступник Міністра цифрової трансформації з питань євроінтеграції Валерія Іонан зауважила, що злочинці та шахраї є не тільки у реальному світі, але й у цифровому середовищі. «Всі ми колись чули історії про те, як хакери зламують сторінки у соцмережах і пошті, отримують персональні дані та займаються фішингом, крадуть кошти з банківських і вчиняють інші злочини. Мінцифра дбає про безпеку українців, тому за підтримки партнерів створило освітній серіал про кібербезпеку», — підкреслила Валерія Іонан.

«Ми займаємося просвітницькою діяльністю з кібербезпеки вже декілька років. Те, що ми розповідали в освітньому серіалі, ми розповідаємо на корпоративних навчальних тренінгах», — сказав під час презентації директор компанії з кібербезпеки 10Guards Віталій Якушев.

«На просторах Інтернету існує дуже багато контенту по темі кібербезпеки, але він дуже складний і незрозумілий для звичайного громадянина. Ми побачили, що через портал Дія.Цифрова освіта можна донести рекомендації з кібербезпеки для пересічного українця. Ми намагалися всі 10 серій зробити трошки з гумором, щоб це були не якісь сухі тренінги, а люди запам’ятовували інформацію та проходили тести», — наголосив Юрій Мелащенко, партнер компанії Cyberlab, радник секретаря РНБО на громадських засадах з питань кібербезпеки…». ***(Мінцифра презентувало освітній серіал про кібербезпеку // Освіта.ua (http://osvita.ua/vnz/73903/). 28.05.2020).***

***

«Система державних електронних закупівель Prozorro запустила програму пошуку вразливостей та запрошує до співпраці "білих" хакерів

Про це повідомила пресслужба Prozorro.

Зазначається, що пошук вразливостей в електронній системі закупівель діятиме на постійній основі.

“Як адміністратори Prozorro ми завжди приділяємо дуже багато уваги кібербезпеці. І тому вирішили на постійній основі залучати незалежних аудиторів, так званих "білих" хакерів, до пошуку вразливостей у нашій системі”, - заявив директор ДП Прозорро Василь Задворний.

До проекту можуть приєднатися як окремі фахівці, так і цілі команди. Для пошуку вразливостей учасникам доступне тестове середовище та інформація для роботи з нею: копія центральної бази даних, офіційний портал, кабінет Антимонопольного комітету України, кабінет Державної аудиторської служби, майданчики, залучені в програму BugBounty, а також необмежена кількість часу на дослідження.

У Prozorro наголосили, що всі дії будуть проходити на pre-production environment (тестове середовище). Усім учасникам гарантують правову безпеку, зазначають на сайті програми». ***(Prozorro запросила "білих" хакерів спробувати зламати систему // Espreso.tv (https://espreso.tv/news/2020/05/26/prozorro_zaprosyla_quotbilykhquot_khakeriv_sprobuvaty_zlamaty_systemu). 26.05.2020).***

***

«Про це сказав Секретар Ради національної безпеки і оборони України Олексій Данілов під час 14-го засідання Національного координаційного центру кібербезпеки.

Як зазначає пресслужба РНБО, у засіданні 22 травня взяли участь представники Міністерства оборони України, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, Національної поліції України, Національного банку України, Генерального штабу Збройних Сил України та розвідувальних органів.

«В умовах активізації проти нашої держави діяльності іноземних спецслужб, зокрема, розвідувальних органів Російської Федерації, посилення кіберзахисту державних інформаційних ресурсів та захист персональних даних громадян України від витоків стали пріоритетом державної політики у сфері кібербезпеки. Ситуацію ускладнює необхідність роботи державних органів в умовах віддаленого доступу у період протистояння усього світу загрозі, пов'язаній із поширенням коронавірусу», - зазначив Олександр Данілов.

Він звернув увагу представників органів влади на незадовільний стан захищеності державних електронних інформаційних ресурсів, реєстрів, баз даних та інших інформаційних масивів та наголосив на удосконаленні практичної взаємодії між суб'єктами забезпечення кібербезпеки.

«Важливим у цьому процесі є невідкладне інформування НКЦК про виявлені факти кібератак та кіберінцидентів на інформаційні системи державних органів, об'єктів критичної інфраструктури для здійснення координації з оперативного реагування, адже наслідки від кібератак можуть створити суттєву загрозу життєво важливим інтересам держави і суспільства», - підкреслив секретар РНБО.

За результатами засідання розробили комплекс заходів, спрямованих на покращення стану захищеності національних електронних інформаційних ресурсів та удосконалення нормативно-правової бази у сфері кібербезпеки». ***(У РНБО заявили про незадовільний стан кібербезпеки державних ресурсів // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/24733/2020-05-24-u-rnbo-zayavili-pro-nezadovilnii-stan-kiberbezpeki-derzhavnikh-resursiv/). 24.05.2020).***

***

«Фахівці Служби безпеки України нейтралізували 103 кібератаки на інформаційні ресурси державних органів влади протягом першого кварталу 2020 року. Починаючи з березня, значна кількість атак відбувається проти відомств, які забезпечують боротьбу з COVID-19 – протидії таким атакам приділяється особлива увага. З початку карантину хакерські угруповання, зокрема, масово направляють на поштові скриньки державних установ електронні листи на тематику коронавірусу. До е-мейлів насправді прикріплені файли зі шкідливим програмним кодом, який активізується при відкриванні листа. Більшість хакерських атак скеровані російськими спецслужбами, які намагаються отримати віддалений доступ до комп'ютерів українських держорганів. Потім вони планують спотворювати чи знищувати дані, поширювати фейки нібито від імені держструктур, а також дискредитувати дії української влади. Загалом у січні-березні СБУ припинила роботу майже 2 тисяч веб-ресурсів, які хакери використовували для здійснення кібератак. За зібраними матеріалами відкрито 117 кримінальних проваджень, у тому числі 42 за фактами несанкціонованого втручання у роботу комп'ютерів, автоматизованих систем і комп'ютерних мереж (статті 361, 362 ККУ). Крім того Служба безпеки України направила в органи державної влади методичні рекомендації: як дотримуватися кібернетичної та інформаційної безпеки. СБУ закликає користувачів не відкривати листи з додатками від невідомих адресатів, обов'язково перевіряти їх за допомогою антивірусних програм і дотримуватись правил кібергігієни…». ***(СБУ нейтралізувала 103 кібератаки і завадила російським хакерам отримати дані держустанов // Служба безпеки України (https://www.ssu.gov.ua/ua/news/1/category/2/view/7559#.ZjY7iHzm.dpbs). 06.05.2020).***

***

«В Україні протягом тижня система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури зафіксувала 15 718 підозрілих подій та заблокувала 10 DDoS-атак, переважну більшість - на сайти Офісу Президента України…

«Протягом 28 квітня - 5 травня система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури зафіксувала 15 718 підозрілих подій. Переважна більшість з них - виявлення нестандартних протоколів або подій (9759 подій), спроб мережевого сканування (2861 подія), виявлення мережевого трояна (1528 подій) та спроб отримання прав адміністратора (1210 подій)»…

Зазначається, що система захищеного доступу державних органів до мережі Інтернет заблокувала 7932 різних видів атак, з яких 7838 - це мережеві атаки прикладного рівня.

"Також заблоковано 10 DDoS-атак (переважна більшість - на сайти Офісу Президента України)"…

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєстровано та опрацьовано 1671 кіберінцидентів.

Більшість інцидентів належить доменній зоні UACOM (1617 інцидентів). Основна кількість інцидентів стосується розповсюдженню шкідливого програмного забезпечення (більше 90%) та фішингу (до 2%).

В разі будь-яких кіберінцидентів, кібератак або підозрілих дій щодо інформаційно-телекомунікаційних систем просимо інформувати урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA…». ***(Валерія Гуржий. В Україні протягом тижня зафіксовано 10 атак на сайти Офісу Президента // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1867579-v-ukrayini-protyagom-tizhnya-zafiksovano-10-atak-na-sayti-ofisu-prezidenta). 05.05.2020).***

***

«Протягом 6-12 травня системою захищеного доступу державних органів до мережі Інтернет було заблоковано 7908 різних видів атак, більшість з них – мережеві атаки прикладного рівня. Також було заблоковано 18 DDoS-атак (переважна більшість – на сайти Офісу президента України), повідомляє Державна служба спеціального зв'язку та захисту інформації.

За 6 днів система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала 10964 підозрілих подій. З них 45% стосується виявлення нестандартних протоколів або подій, 23% – спроб мережевого сканування, 16% – виявлення мережевого трояна, 10% – спроб отримання прав адміністратора». ***(Державна служба спецзв'язку повідомляє про близько 8 тис. кібератак на сайти держорганів // UA.NEWS (https://ua.news/ua/derzhavna-sluzhba-spetszv-yazku-povidomlyaye-pro-blyzko-8-tys-kiberatak-na-sajty-derzhorganiv/). 14.05.2020).***

***

«Протягом останніх двох діб на низку критичних до чинної влади сайтів було здійснено кілька DDoS-атак. Про це, зокрема, заявили редакції порталів Obozrevatel та "Високий Замок Online".

Причиною кібератак, на думку журналістів, можуть бути викривальні публікації щодо можливих спекулятивних оборудок оточення президента Володимира Зеленського. А саме – щодо привезення в Україну літаками "гуманітарного" медичного обладнання, захисних костюмів і масок, санітайзерів та тестів на коронавірус.

За словами редакції Obozrevatel, до атаки можуть бути причетні заступник голови Офісу президента Кирило Тимошенко та російський бізнесмен Борис Баум, які і фігурують у відповідних журналістських розвідуваннях.

"Уже в розпал атаки новоспечений власник українського паспорту Баум написав повідомлення та передав "привіт" голові редакційної ради Obozrevatel

Михайлу Бродському. Це можна сприйняти, як його розправу за публікацію викривальних матеріалів", – йдеться у повідомленні видання.

Про технічні проблеми повідомило і видання "Високий Замок онлайн".» ***(НИЗКА УКРАЇНСЬКИХ САЙТІВ ЗАЗНАЛА DDOS-АТАК – ЗАМОВНИКАМИ НАЗИВАЮТЬ ОТОЧЕННЯ ЗЕЛЕНСЬКОГО // 5 канал (https://www.5.ua/polityka/nyzka-ukrainskykh-saitiv-zaznala-ddos-atak-zamovnykamy-nazyvaiut-otochennia-zelenskoho-214029.html). 02.05.2020).***

***

«Специалисты Совета национальной безопасности и обороны Украины отреагировали на массированную кибератаку на систему информационной безопасности ГК «Укроборонпром», зафиксированную в апреле 2020 г., и присоединились к соответствующей рабочей группе реагирования на киберугрозы, созданную на базе концерна. Об этом сообщает пресс-служба «Укроборонпрома».

Вместе со специалистами аппарата СНБО Украины в рабочую группу реагирования на кибератаки вошли эксперты других профильных органов государственной власти - Департамента киберполиции, Госслужбы спецсвязи и защиты информации, Ситуационного центра обеспечения кибернетической безопасности СБУ.

«Мы убеждены, что недавний успешных опыт «Укроборонпрома» в сдерживании мощной кибератаки типа brute-force может помочь обезопасить от подобных угроз другие государственные предприятия и объекты критической инфраструктуры Украины. Поэтому мы наладили обмен данными о киберугрозе, совместно разрабатываем методы эффективного противодействия подобным атакам», - сообщил заместитель генерального директора «Укроборонпрома» по безопасности Константин Бушуев.

Он рассказал, что в «Укроборонпроме» обновилась команда специалистов, которые занимаются вопросами киберзащиты и информационной безопасности оборонных предприятий концерна, которые ввели новые протоколы реагирования на внешние атаки…». ***(В СНБО отреагировали на кибератаку «Укроборонпрома» // Транспортный бизнес (http://tbu.com.ua/news/v_snbo_otreagirovali_na_kiberataku_ukroboronproma_.html). 05.05.2020).***

***

«Фигурантка сообщала о минировании объектов на территории Украины с помощью электронной почты с использованием средств анонимизации. За это ей грозит уголовная ответственность…

Сотрудники Департамента киберполиции совместно с Главным следственным управлением Национальной полиции Украины под процессуальным руководством Офиса Генерального прокурора разоблачили киевлянку в рассылке сообщений о минировании.

Киберполиция установила, что женщина осуществляла рассылку ложных сообщений о минировании объектов на территории Украины. Такие сообщения присылались по электронной почте с использованием средств анонимизации.

Правоохранители провели обыск по месту жительства подозреваемой. По результатам обыска изъяты мобильные телефоны и компьютерная техника, с помощью которой отправлялись заведомо ложные сообщения о заминировании.

Сейчас решается вопрос об объявлении фигурантке о подозрении по ст. 259 (Заведомо ложное сообщение об угрозе безопасности граждан, уничтожения или повреждения объектов собственности) Уголовного кодекса Украины. Досудебное расследование продолжается». ***(Артем Сереженок. Киберполиция разоблачила жительницу столицы в рассылке ложных сообщений о минировании // Internetua (https://internetua.com/kiberpoliciya-razoblacsila-jitelnicu-stolicy-v-rassylke-lojnyh-soobsxenii-o-minirovanii). 08.05.2020).***

***

«Кіберфахівці Служби безпеки України задокументували несанкціоноване втручання у роботу інформаційно-телекомунікаційних систем Державної податкової служби.

Про це повідомляє прессслужба СБУ.

«У межах розпочатого кримінального провадження співробітники спецслужби встановили, що група зловмисників, серед яких посадовці податкової, здійснювала несанкціоноване втручання у роботу інформаційно-телекомунікаційних систем ДПС. Вони робили маніпуляції з інформацією, яка в них зберігається і обробляється, що призвело до витоку, підробки, блокування даних, спотворення процесу обробки інформації та порушення встановленого порядку її маршрутизації", - йдеться у повідомленні.

Задокументовано, що зловмисники проводили незаконні дії, зокрема, у базах ІТС «Податковий блок», ІТС «Електронний кабінет», ІТС «Єдине вікно подання електронної звітності», «Єдиного реєстру податкових накладних», системі моніторингу відповідності податкових накладних розрахунків коригування критеріям оцінки ступеня ризиків «СМКОР». Зловмисники цим сприяли підприємствам, які обслуговуються конвертаційно-транзитними групами, ухилятись від сплати податків…

Наразі одному з учасників протиправного механізму повідомлено про підозру у вчиненні злочину, передбаченого ч. 2 ст. 361 Кримінального кодексу України, вирішується питання про обрання міри запобіжного заходу.

Також приймається рішення про притягнення до відповідальності службових осіб ДПС України, причетних до організації та функціонування оборудки». ***(СБУ виявила втручання у роботу інформаційних систем Податкової // Укрінформ (https://www.ukrinform.ua/rubric-economy/3021844-sbu-viavila-vtrucanna-u-robotu-informacijnih-sistem-podatkovoi.html). 08.05.2020).***

***

«Правоохоронні органи вже більше місяця не можуть розслідувати гучну справу, пов`язану з кібератаками на комп'ютерні ресурси Київської міської держадміністрації.

Хто організував DDoS-атаку?

Ще в квітні-2020 представники столичної влади поскаржились правоохоронцям на незаконні дії кіберзлочинців, які намагались вивести з ладу е-сервіси на Хрещатику, 36. Проте й досі невідомо: хто ж організував масовану DDoS-атаку?

Згідно з офіційними даними, хакерські атаки тривали декілька днів – із 11 до 15 квітня 2020 року. За першу годину кібернападів було зафіксовано близько 1,5 мільйона оригінальних IP-адрес (через які здійснювалися спроби дестабілізувати роботу е-сервісів). Зважаючи на величезну кількість атакуючих ботів, подібних викликів у нашій країні ще не було. Про це повідомили у департаменті інформаційно-комунікаційних технологій КМДА.

– Внаслідок атаки, зокрема на її піку, інформаційні ресурси були недоступні поза межами периметру мережевої інфраструктури Київради, структурних підрозділів КМДА, що належать до комунальної власності територіальної громади міста Києва. При цьому всередині периметру мережі все обладнання та інформаційні сервіси були у працездатному стані, функціонування здійснювалось у повному обсязі, – розповів виконувач обов’язків директора департаменту Вячеслав Новохацький.

За словами Новохацького, матеріали «про масовану DDoS-атаку передано до Державної служби спеціального зв'язку та захисту інформації і Служби безпеки України для подальшого з’ясування обставин та розслідування інциденту».

Завдячуючи надійній системі кіберзахисту, вдалося відхилити мільярди атакуючих запитів, мінімізувати хакерські загрози та розблокувати трафіки для міських е-сервісів.

Сьогодні всі інформаційні сервіси КМДА працюють у штатному режимі (відкриті для зовнішніх доступів).

Кіберзлочинці є, а кіберзлочинів – немає!

У профільному департаменті КМДА лише фіксували DDoS-атаки. А відстежувати антизаконну діяльність хакерів повинні правоохоронні органи.

Проте в СБУ ще й досі нічого не кажуть про результати розслідування квітневих атак на комп`ютерні ресурси столичної влади.

– У Департаменті інформаційно-комунікаційних технологій відсутня будь-яка інформація щодо притягнення осіб та їх покарання за здійснення кіберзлочинів, – стверджує Вячеслав Новохацький.

Сумна практика показує: якщо злочини не розкриті по гарячих слідах, то такі справи перетворюються на «глухарів». Більше того, сьогодні у правоохоронній сфері спостерігається парадокс: де-факто кіберзлочинці є, а де-юре кіберзлочинів – немає! Така ситуація викликає більше запитань, аніж відповідей.

Ще в 2005 році Україна ратифікувала Конвенцію про кіберзлочинність – імплементувала положення міжнародного акта у вітчизняне законодавство. А в червні-2015 Парламентська Асамблея Ради Європи ухвалила резолюцію 2070: «Зміцнення співпраці у протидії кібертероризму та іншим масштабним атакам в

Інтернеті» (із закликами до країн-членів Ради Європи запровадити визначення кібертероризму та відповідальності за нього).

Як показує аналіз, у сфері кібербезпеки вітчизняні правоохоронці майже не використовують міжнародні правові норми. А Кримінальний кодекс узагалі не містить такі поняття, як «кіберзлочинність» і «кібертероризм». Статті КК вказують лише на інші види покарання: починаючи від порушення авторських прав і закінчуючи перешкоджанням роботі комп'ютерних мереж.

Щоб заповнити цю законодавчу прогалину, у Верховній Раді ще в 2015 році зареєстрували проєкт закону про встановлення кримінальної відповідальності за кібертероризм. Проте, зважаючи на парламентські перевибори-2019, цей документ «наказав довго жити»…

Небезпечний інтелект

За даними правоохоронців, кіберзлочинці – творчі особистості, здатні йти на технічні виклики і ризики. Серед них можуть бути високопосадовці, які користуються доступом до широкого кола інформації і дають вказівки, але при цьому не несуть відповідальності за роботу комп'ютерної техніки.

Переважна кількість хакерів (близько 54%) – особи віком 22-40 років із високим інтелектом і дипломами про вищу освіту.

– Найчисельнішими є хакери-аматори. На їхню частку припадає до 80% всіх комп'ютерних атак. Цю категорію цікавить не якась мета, а лише сам процес атаки. Вони відчувають задоволення від подолання систем захисту. Їх дії вдається легко припинити, оскільки хакери-аматори воліють не ризикувати і не вступати в конфлікт з законом. Найбільш небезпечну групу складають професійні кіберзлочинці, які не тільки прекрасно знають тонкощі інтернет-технологій, а й володіють декількома мовами програмування. Під час «злому» системи захисту навіть не залишають слідів, – пояснив експерт із дослідження комп'ютерної злочинності, кандидат юридичних наук Олександр Голубєв.

Для боротьби з хакерами у правоохоронних органах уже давно створені спеціальні підрозділи, але чи можна говорити про надійну кібербезпеку держави загалом та її органів зокрема?

«Лотереї», «аукціони», «фішинг»

Сьогодні кіберзлочинність розвивається разом із комп`ютерними технологіями, залишаючись при цьому не лише небезпечним, а й маловивченим явищем у нашому суспільстві.

Найпоширеніші види кіберзлочинів – інтернет-шахрайства, які пов`язані з так званими «лотереями». Організатор цих акцій завалює поштові скриньки користувачів своїми «захопленими» враженнями про так звані «виграші» ноутбуків (путівок, авто тощо) в яких вони ніколи не брали участь. Попадаючи на такі приманки, довірливі люди заходять на «потрібні» сайти, вводять номери своїх рахунків та ПІН-коди карток (які нібито необхідні для оплати послуг доставки).

В інтернет-просторі також можна зустріти «аукціони», на які припадає майже 75% усіх скарг ошуканих споживачів (зареєстрованих в мережі Internet Fraud Complaint Center). Такі приманки розраховані на любителів «халяви»: для них створюють віртуальні інтернет-магазини, в яких постійно проходить «розпродажа». Розплачуватися треба не готівкою, а лише за пластиковою карткою.

Перераховуючи гроші за обіцяний товар, клієнт нічого не отримує, а шахрай відразу зникає.

Відносно новим видом обману є фішинг (від англ. fishing – рибалка): людям розсилають масу листів, замаскованих під «офіційні бланки» фінансових установ з посиланнями на сайти-пастки, які візуально копіюють сайти банків, казино і магазинів. Зловмисники використовують схожі домени та web-дизайни. Головна мета – виманювати кредитні дані і паролі банківських рахунків…» ***(Валентин КОВАЛЬСЬКИЙ. Чому київські хакери не по «зубах» СБУ // Хрещатик (http://kreschatic.kiev.ua/ua/5313/news/1589721983.html). 17.05.2020).***

***

«…Паспорти українців разом з відбитками пальців злили в мережу. В інтернет потрапили дані, якими володіли лише демографічні реєстри та ДП "Документ".

Дані з біометричного паспорта, водійського посвідчення, інформація, що була лише в банку – все це Володимиру Фльонцу видав у соцмережі анонімний бот.

"Перевірив максимально далеко від себе інформацію, номер телефону не контрактний, не прив'язаний до мого прізвища, база чудово змогла зв'язати його зі мною, знайти не тільки всі мої паспортні дані. Бот показав мої фотографії з паспорта, які були, очевидно, тільки в державному демографічному реєстрі. Причому, як ви знаєте, у вас на паспорті буде чорно-біле фото, а бот зміг показати це ж фото в кольорі", – каже голова громадської організації "Електронна демократія" Володимир Фльонц.

Володимир каже: таке фото надавав лише міграційній службі, коли зо три роки тому робив новий паспорт. Тому впевнений – інформація з шахрайської бази – достовірна.

Скандал із витоком даних вибухнув у вівторок. Автори цього телеграм-каналу заявили, що об'єднали дані українців з різних баз. За номером телефону можна дізнатися максимум інформації про його власника. За гроші. Ціна стартує від 50 доларів. Деякі водії пов'язали такий "злив" з додатком "Дія". У ньому з лютого можна тримати в електронному вигляді водійське посвідчення, а віднедавна – ще й внутрішній паспорт. У Мінцифри такий зв'язок назвали фейком.

Експерти з кібербезпеки погоджуються: мобільний застосунок "Дія" не збирає дані про українців. А лише бере їх із держреєстрів. Тож оновлену базу біометричних паспортів, відбитки пальців, фото та водійські посвідчення – злили ті, хто мав доступ до цих реєстрів. Такий доступ має, зокрема, і ДП "Документ", яке за законом лише надає послуги. Але не має права зберігати дані.

Хто злив дані – заходилася розслідувати кіберполіція. Згодом з'ясувалося: до витоку даних можуть бути причетні посадовці МВС та міграційної служби. Тож справу скерували до ДБР…». ***(Ганна Рибалка, Віктор Сніжко. ВІД ФОТО ДО ВІДБИТКІВ ПАЛЬЦІВ: ХТО "ЗЛИВ" ПЕРСОНАЛЬНІ ДАНІ УКРАЇНЦІВ У МЕРЕЖУ – ПОДРОБИЦІ СКАНДАЛУ // 5 канал (https://www.5.ua/suspilstvo/vid-foto-do-vidbytkiv-paltsiv-khto-zlyv-personalni-dani-ukraintsiv-u-merezhu-podrobytsi-skandalu-214877.html). 19.05.2020).***

***

«Через постійні сторонні атаки не може бути відновлена робота сайту уповноваженого ВРУ з прав людини, за інформацією можна слідкувати на офіційних сторінках у соціальних мережах. Про це у Facebook написала омбудсмен Людмила Денісова…

"Робота сайту уповноваженого ВРУ з прав людини не може бути відновлена через постійні сторонні атаки на ресурс. Тому всю актуальну інформацію читайте на публічних сторінках у Facebook та Telegram", - написала Денісова.

Так, слідкувати за інформацією можна на сторінках Facebook та Telegram Офісу омбудсмена України, а також на сторінках Facebook та Telegram Денісової…». ***(Антоніна Карташева. Через постійні кібератаки заблоковано роботу сайту Омбудсмена // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1869871-cherez-postiyni-kiberataki-zablokovano-robotu-saytu-ombudsmena). 18.05.2020).***

***

«Україна, яка фактично є полігоном для використання кіберінструментів Росією, за роки набралась унікального досвіду з протистояння ним.

Про це заявив міністр закордонних справ України Дмитро Кулеба у зверненні до Ради Безпеки ООН під час неформального відкритого засідання РБ ООН за формулою Арріа на тему “Кіберстабільність, запобігання конфліктам та зміцнення спроможностей”…

“Як ви всі знаєте, з 2014 року Україна стикається з гібридною агресією Російської Федерації, яка використовує інформаційно-комунікаційні технології як один із її методів гібридної війни. Ми — країна, де Росія випробовує нові кібер-війни проти нас, і колись одна гібридна війна змусила нашу країну переосмислити нашу стратегію кібербезпеки”, — сказав Кулеба.

Він заявив, що протягом 2019 року відповідні органи України виявили та негайно відреагували на понад 1 500 кібер-інцидентів на критично важливих інфраструктурних об’єктах.

Крім того,сказав міністр, інші західні країни також зіткнулися з ворожою кібер-поведінкою Росії і вважають Кремль відповідальним за руйнівні кібератаки.

“Ми усвідомлюємо, що використовуючи інформаційні комунікаційні технології як політичний інструмент, Росія бере участь у ряді кібер-операцій, спрямованих на дезінформаційну кампанію, втручання у суверенні виборчі процеси, кібер-шпигунство та кібер-атаки на критичні інфраструктурні об’єкти у ряді країн Європи і за її межами. Я хотів би підкреслити, що Україна, яка фактично є полігоном для використання кіберінструментів для цілей військових формувань, має унікальний практичний досвід нейтралізації кібератак, який може бути корисним для країн-партнерів. Ми пропонуємо вам свій досвід та знання”, — сказав міністр». ***(Україна є полігоном для використання кіберінструментів РФ, - Кулеба // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/220520-ukrayina-ye-poligonom-dlya-vykorystannya-kiberinstrumentiv-rf-kuleba). 22.05.2020).***

***

«В Україні істотно збільшилася кількість кібератак на сайти органів влади. У період з 20 по 26 травня зафіксовано збільшення підозрілих подій майже в 12 разів, передає 1NEWS з посиланням на прес-центр Державної служби спеціального зв'язку та захисту інформації України.

Було виявлено 107 566 підозрілих подій.

«Переважна більшість зафіксованих підозрілих подій стосується виявлення нестандартних протоколів або подій (59%), спроб мережевого сканування (35%), виявлення мережевого трояна (2%) і спроб отримання прав адміністратора (2%)», – повідомили в Держспецзв'язку.

При цьому система захисту заблокувала 4705 різних атак, що на 24% менше, ніж на попередньому тижні. Більшість (98%) – це атаки прикладного рівня. Крім цього було виявлено 13 DDoS-атак, більшість з яких на сайти Офісу президента.

«Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA в цей період зареєструвала і обробила 3377 кіберінцидентів, що на 10% більше, ніж на попередньому тижні. Переважна більшість оброблених інцидентів належить доменній зоні UACOM (близько 99%). Основна кількість інцидентів стосується поширення ШПЗ (93% від загальної кількості) і фішингу (4%)», – йдеться в повідомленні.

У Держспецзв'язку закликали у разі кібератак або підозрілих дій відразу звертатися в урядову команду реагування CERT-UA». ***(Суттєво збільшилася кількість кібератак на сайти українських органів влади // Інформаційне агентство «1NEWS» (https://1news.com.ua/ipol/suttyevo-zbilshylasya-kilkist-kiberatak-na-sajty-ukrayinskyh-organiv-vlady.html). 27.05.2020).***

***

«В украинской прессе не так давно прошла информация о том, что сервис электронной почты Мета может быть связан с российскими спецслужбами. Якобы он согласился предоставить свои данные в реестр Роскомнадзора организованный в 2014 году. Для того, чтобы войти в этот реестр нужно согласие владельцев на сбор, сохранность и предоставление информации по требованию ФСБ России. В качестве аргумента приведем вытяжку из реестра Роскомнадзора.

Об этом пишет "pingvin.pro".

Согласно информации электронная почта Мета может передавать данные пользователей российским спецслужбам. Он может быть первым ресурсом в Украине, который обнаружили в реестре Роскомнадзора.

Для этого нужно чтобы сервиз согласился расшифровывать данные пользователей, а также сохранять, собирать и предоставлять информацию уполномоченным специальным органам. Отмечается также возможность запроса от ФСБ на все контакты пользователя из адресной книги и электронной почты. Сюда же может входить и личная переписка, авторизация на посторонних сервисах, количество и объем сообщений.

По так называемому закону Ирины Яровой, который вступил в силу 1 июля от 2018 года, все участники реестра обязаны предоставлять и сберегать данные пользователей, телефонные разговоры, текстовые сообщения, изображения, аудио, видео и другую информацию от 30 дней до полугода.

Все будет зависеть от типа информации, и передаваться по требованию российских спецслужб. Также от участников реестра, которые поддерживают шифровку данных, требуется расшифровка информации по требованию ФСБ…» ***(Алена Лесная. Срочно проверьте ваши данные: украинский сервис META сливает данные российским спецслужбам // akcenty.com.ua (https://glavnoe.akcenty.com.ua/52167-srochno-proverte-vashi-dannye-ukrainskiy-servis-meta-slivaet-dannye-rossiyskim-specsluzhbam). 27.05.2020).***

***

Боротьба з кіберзлочинністю в Україні

«Служба безпеки України встановила та затримала хакера, відомого під ніком Sanix, який минулого року виклав на одному з форумів оголошення про продаж бази з 773 мільйонами адрес електронної пошти та 21 мільйоном унікальних паролів.

Джерело: пресслужба СБУ

Деталі: Правоохоронці нагадують, що у січні 2019 року про нього писали The Guardian, Forbes та Newsweek, йому присвятив сюжет телеканал Italia 1, адже база даних, яку він виставив на продаж, була "найбільшим за всю історію масивом викрадених даних".

Спеціалісти встановили, що виставлена хакером на продаж база обсягом 87 гігабайтів становить лише маленьку частину із загальної кількості даних, якими він заволодів. Подібних баз викрадених і зламаних паролів у хакера було щонайменше сім, загальний обсяг яких сягав майже терабайт. До них входили персональні, в тому числі фінансові, дані жителів Євросоюзу та Північної Америки.

Служба безпеки України отримала інформацію, що хакером на псевдонім Sanix є, ймовірно, українець, мешканець Івано-Франківської області.

Кіберфахівці СБУ зафіксували продаж ним баз даних з логінами і паролями до скриньок електронної пошти, пін-кодами до банківських карток, електронних гаманців криптовалют, рахунків PayPal, відомостями про комп'ютери, зламані для подальшого використання у бот-мережах та для організації DDoS-атак…». ***(СБУ заявила про затримання відомого на весь світ хакера // Економічна правда (https://www.epravda.com.ua/news/2020/05/20/660717/). 20.05.2020).***

***

«…Співробітники Департаменту кіберполіції спільно із Головним слідчим управлінням НПУ, під процесуальним керівництвом Офісу генерального прокурора, викрили мешканця Київської області у розповсюджені персональних даних громадян України.

Кіберполіція встановила, що фігурант організував діяльність вебресурсу, через який здійснював розповсюдження персональних даних громадян України. Для доступу до зазначеної інформації користувачу необхідно було зареєструватись на вебресурсі з використанням мессенджера.

Задля наповнення бази зловмисник створив відповідну форму, яку заповнювали користувачі вебресурсу. Після чого він несанкціоновано отримував доступ до персональних даних користувачів…

За даним фактом триває розслідування кримінального провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Санкція статті передбачає позбавлення волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років». ***(Кіберполіція викрила чоловіка у розповсюдженні конфіденційної інформації громадян // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-cholovika-u-rozpovsyudzheni-konfidenczijnoyi-informacziyi-gromadyan-2300/). 21.05.2020).***

***

«…Кіберполіцейські Чернівецької області спільно зі слідчими, під процесуальним керівництвом місцевої прокуратури, викрили двох братів, які за допомогою шкідливого програмного забезпечення втручалися в роботу автоматизованих систем.

Встановлено, що програма підбирала логіни та паролі до облікових записів популярних у всьому світі Інтернет-ресурсів. Далі отримані файли з конфіденційною інформацією зловмисники збували на закритих хакерських форумах, а також у месенджерах. Крім цього, з акаунтів, що мали активний грошовий баланс, частково виводили кошти на підконтрольні банківські рахунки.

Правоохоронці провели обшуки. Попереднім оглядом вилученої комп’ютерної техніки виявлено 55 тисяч файлів, на яких знаходиться більше 1,5 мільйона облікових записів громадян різних країн світу.

За попередній рік від злочинної діяльності фігуранти «заробили» близько мільйона гривень.

Наразі триває досудове розслідування кримінального провадження за ч.2 ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Санкція статті передбачає позбавлення волі на строк до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років…». ***(Кіберполіцейські викрили двох братів у зламі облікових записів // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpoliczejski-vykryly-dvox-brativ-u-zlami-oblikovyx-zapysiv-4988/). 14.05.2020).***

***

«…Співробітники кіберполіції в Полтавській області спільно зі слідчими Полтавщини, із залученням підрозділу особливого призначення КОРД, під процесуальним керівництвом місцевої прокуратури, викрили 32-річного жителя м. Горішні Плавні у копіюванні персональних даних користувачів мережі.

Кіберполіція встановила, що для протиправної діяльності хакер використовував вебфоруми «тіньової» тематики, де розповсюджував шкідливе програмне забезпечення, замасковане під іншу програму.

Вказаний вірус призначений для крадіжки персональних даних користувачів мережі. Після завантаження на комп'ютер програма шукала необхідну зловмиснику інформацію: паролі до аккаунтів соціальних мереж, доступ до конфіденційної інформації про електронні платіжні системи, паролі від електронних поштових скриньок, а також ключі від електронних гаманців різних криптовалют.

Для приховання своєї злочинної діяльності, зловмисник використовував низку анонімайзерів та проксі-серверів.

Правоохоронці провели обшук за місцем мешкання фігуранта. За результатами вилучено комп'ютерну техніку, мобільні телефони, жорсткі диски, флеш-накопичувачі, банківські картки, сім-карти та стартові пакети. Вилучене обладнання направлено на експертизу.

За даним фактом відкрито кримінальне провадження за ч.1 ст.361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України. Після отримання результатів експертизи буде вирішено питання щодо оголошення підозрюваному про підозру. Йому загрожує до 2 років ув'язнення». ***(Кіберполіція викрила хакера у крадіжці персональних даних громадян // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-xakera-u-kradizhczi-personalnix-danix-gromadyan/). 29.05.2020).***

***

«…Співробітники кіберполіції у Волинській області спільно зі слідчими поліції області, під процесуальним керівництвом місцевої прокуратури, викрили хакера у розповсюдженні шкідливого програмного забезпечення.

Кіберполіція встановила, що до такої діяльності причетний 20-річний місцевий мешканець Горохівського району. Чоловік розповсюджував вірусне програмне забезпечення за допомогою месенджеру.

Програма працювала наступним чином: коли потерпілий натискав на файл або посилання, хакер отримував віддалений доступ до персональних комп'ютерів потерпілих…

Наразі порушнику повідомлено про підозру ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України. Санкція статті передбачає позбавлення волі на строк до п'яти років. Слідчі дії тривають, встановлюється повне коло потерпілих осіб». ***(На Волині кіберполіція викрила хакера у розповсюдження шкідливого програмного забезпечення //***

Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/na-volini-kiberpolicziya-vikrila-xakera-u-rozpovsyudzhennya-shkidlivogo-programnogo-zabezpechennya/). 28.05.2020).

***

«…Співробітники відділу протидії кіберзлочинам у Луганській області спільно зі слідчими Луганщини та Службою безпеки України, під процесуальним керівництвом місцевої прокуратури, викрили чоловіка у створенні шкідливого програмного забезпечення.

Встановлено, що мешканець Старобільська створив та розповсюджував шкідливе програмне забезпечення з викрадення даних громадян: логінів та паролів від електронної пошти, платіжних систем тощо. Програму продавав через закриті хакерські форуми.

Правоохоронцями за місцем мешкання фігуранта проведено обшук. Вилучено речові докази: комп'ютерну техніку зі зразками шкідливого програмного забезпечення. Вирішується питання щодо оголошення підозри за ст. 361-1 (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України». ***(На Луганщині викрито чоловіка, який продавав програму з викрадення даних громадян // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/na-luganshhini-vikrito-cholovika-yakij-prodavav-programu-z-vikradennya-danix-gromadyan/). 28.05.2020).***

***

«…Співробітники кіберполіції в Одеській області спільно зі слідчими, під процесуальним керівництвом місцевої прокуратури, викрили хакера, який розповсюджував логіни та паролі до облікових записів різних поштових ресурсів.

Кіберполіція встановила, що фігурант розробив та запустив вебресурс, на якому протягом двох років розміщував оголошення щодо продажу облікових даних користувачів поштових сервісів та криптовалютних бірж. Крім цього, використовуючи шкідливе програмне забезпечення, чоловік несанкціоновано збирав вхідні дані до електронних поштових скриньок. Таким чином він формував та поповнював бази даних. За продаж такої інформації хакер отримував гроші на свій електронний гаманець…

Наразі фігуранту оголошено про підозру за ч. 1 ст. 361-2 (несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України. Зазначеному громадянину загрожує позбавлення волі на строк до двох років». ***(Кіберполіція викрила чоловіка у продажі баз даних з логінами та паролями до електронних поштових скриньок // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-cholovika-u-prodazhi-baz-danix-z-loginami-ta-parolyami-do-elektronnix-poshtovix-skrinok/). 28.05.2020).***

***

«…Співробітники кіберполіції у Тернопільській області спільно із слідчими поліції Тернопільщини, під процесуальним керівництвом місцевої прокуратури, із залученням працівників роти поліції особливого призначення, викрили місцевого мешканця у продажі баз даних, що містять інформацію з обмеженим доступом.

Кіберполіція встановила, що мешканець Тернополя, 2001 року народження, використовуючи месенджер, у різних тематичних групах розміщував оголошення щодо продажу електронних баз даних підприємств та установ, що містять ознаки інформації з обмеженим доступом. Купівля баз даних здійснювалась шляхом перерахування грошей покупцями через платіжну систему QIWI або на банківську картку.

Вартість бази даних становила до півтори тисячі гривень…

За даним фактом розслідується кримінальне провадження за ч. 2 ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в комп'ютерах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України. Санкція статті передбачає позбавлення волі на строк від двох до п'яти років. Досудове розслідування триває». ***(На Тернопільщині кіберполіція викрила чоловіка у продажі інформації з обмеженим доступом // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/na-ternopilshhini-kiberpolicziya-vikrila-cholovika-u-prodazhi-informacziji-z-obmezhenim-dostupom/). 25.05.2020).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Російські хакери здійснили напад на університети Сполученого Королівства, які займаються розробкою вакцини та обладнанням для боротьби з коронавірусом…

Британський національний центр кібернетичної безпеки (NCSC) заявив, що університети Сполученого Королівства і дослідницькі центри стають ціллю цілої хвилі нападів хакерів із "ворожих держав".

Вони хочуть заволодіти інформацією про дослідження про створення вакцини проти коронавірусу. Вважається, що кіберзлочинців спонсорують уряди Росії, Китаю та Ірану. Але наразі жодна зі спроб нападу на британські установи не була успішною.

Популярний у Великій Британії часопис Express, із посиланням на джерела у колах британських служб безпеки, зокрема, у відділі боротьби з кіберзлочинністю, наводить слова неназваного фахівця, який вважає, що у випадку кібернападів на британські університети та дослідницькі лабораторії йдеться про спроби викрадення інтелектуальної власності. За цих обставин вже зникає межа між

державою, яка все це замовляє, і серйозними злочинами. Відтак, уряди, які скеровують напади кіберзлочинців, самі є співучасниками цих злочинів.

Це видання також наводить слова Тобаяса Елвуда, голови Оборонного комітету британського парламенту, який каже, що Британія не мусить зволікати у наданні відповідного удару у помсту за подібні ворожі кроки.

"Глобальне розпорошення уваги, пов'язане з Covid-19, створює ідеальну «димову завісу» для здійснення кібернападів. Надто, коли ціна антивірусної вакцини є величезною. Британія не мусить зволікати щодо відповіді на подібну ворожу діяльність", – сказав Тобаяс Елву.» ***(РОСІЙСЬКІ ХАКЕРИ НАМАГАЮТЬСЯ ВИКРАСТИ ІНФОРМАЦІЮ ЩОДО ПРОТИДІЇ COVID-19, - СПЕЦСЛУЖБИ БРИТАНІЇ // ESPRESO.TV (https://espreso.tv/news/2020/05/05/rosiyski_khakery_namagayutsya_vykrasty_informaciyu_schodo_protydiyi_covid_19_specsluzhby_brytaniyi). 05.05.2020).***

***

«Исследователь безопасности Боб Дяченко (Bob Diachenko) обнаружил в открытом доступе незащищенный сервер компании NSO Group, поставляющей спецслужбам по всему миру инструменты для взлома.

В марте 2020 года NSO Group начала работу над системой Fleming, предназначенной для отслеживания контактов с зараженными COVID-19. Если разрабатываемые в других странах системы отслеживания распространения коронавируса используют Bluetooth, то Fleming полагается на геолокационные данные мобильных устройств.

С помощью подтвержденных данных тестирований на COVID-19 от органов здравоохранения и данных о местоположении мобильных устройств система выявляет людей, которые могли заразиться коронавирусом. Каждому, кто приблизится к человеку с подтвержденным диагнозом, Fleming отобразит соответствующее уведомление.

По уверению NSO Group, обнаруженный Дяченко сервер предназначался исключительно для демонстрации технологии, и никакой утечки не произошло. Исследователь подтверждает, что система содержала данные-«пустышки». В настоящее время производитель только ожидает одобрения от правительства Израиля на использование в своей системе реальных данных мобильных устройств. Несмотря на это, эксперты уверены, что база данных ни при каких обстоятельствах не должна быть открытой, да и само существование централизованной БД о перемещениях граждан ставит их конфиденциальность под угрозу.

Как пишет TechCrunch, незащищенная БД содержалась на сервере Amazon Web Services во Франкфурте (Германия), где законодательство по защите данных является одним из самых строгих в мире. В ней хранились геолокационные данные за шесть недель (с 10 марта по 23 апреля), даты, время и местоположения «целей» (так NSO Group называет отслеживаемых людей), которые потенциально могли контактировать с зараженными.

Обнаружив незащищенный сервер, Дяченко сообщил об этом NSO Group, и компания отключила его от интернета». ***(В Сети обнаружен незащищенный***

сервер компании NSO Group // SecurityLab.ru (https://www.securitylab.ru/news/508150.php). 08.05.2020).

***

«Приложения для отслеживания людей с COVID-19 должны использоваться только во время пандемии и должны быть автоматически деактивированы по ее окончании, передает Reuters слова комиссара по вопросам юстиции ЕС Дидье Рейндерса (Didier Reynders). Также эти сервисы не могут быть использованы для массового наблюдения. «Частные лица будут контролировать свои данные», — сказал Рейндерс законодателям ЕС на пленарном заседании.

В середине апреля Еврокомиссия заявила, что страны Европейского союза, использующие мобильные приложения для сдерживания распространения коронавируса, должны обеспечить соответствие этих приложений правилам конфиденциальности. В частности, им следует избегать использования персонализированных данных о местоположении людей. Подобные рекомендации – часть единого европейского подхода к использованию технологий для борьбы с COVID-19. Они появились после того, как несколько стран ЕС выпустили различные приложения, вызвав критику со стороны активистов защиты конфиденциальности данных.

Ранее «Роскомсвобода» запустила карту нарушений гражданских прав в цифровой среде Pandemic Big Brother. Проект ставит целью не только зафиксировать все факты усиления государственного вмешательства в права граждан во время режимов чрезвычайных ситуаций и карантина по всему миру, но и выявить случаи злоупотреблений после окончания эпидемии». ***(ЕС: отслеживающие приложения после пандемии нужно деактивировать // РосКомСвобода (https://roskomsvoboda.org/58580/). 15.05.2020).***

***

«Компания Group-IB сообщает, что в 2019 г. в целом заблокировала свыше 14 тыс. фишинговых ресурсов – почти втрое больше, чем годом ранее. Среди ключевых тенденций эксперты центра реагирования на инциденты кибербезопасности CERT-GIB отмечают смещение фокуса атак на пользователей облачных хранилищ как в B2C, так и B2B сегментах, а также переход фишеров с создания единичных мошеннических страниц на целые «сетки» сайтов под определенные бренды, что обеспечивает непрерывность их функционирования и устойчивость к блокировкам.

Во второй половине 2019 г. в ходе работ по обнаружению и нейтрализации угроз, распространяющихся в сети Интернет, CERT-GIB заблокировал 8506 фишинговых ресурсов, в то время как годом ранее этот показатель составлял 2567.

Резкий рост числа блокировок объясняется не только эффективностью обнаружения и детектирования преступных схем, но также изменением тактики фишеров, в результате чего увеличилась продолжительность фишинговых атак: в предыдущие годы злоумышленники по большей части прекращали свои кампании после блокировки мошеннических веб-ресурсов и быстро переключались на другие

бренды. Сегодня они продолжают работу, создавая все новые страницы на смену заблокированным. Как следствие, еще одним трендом прошлого года стало усложнение и расширение инфраструктуры для реализации фишинговой атаки.

В прошлом году наибольшее число фишинговых страниц было нацелено на онлайн-сервисы (29,3%), облачные хранилища (25,4%) и финансовые организации (17,6%). Данные CERT-GIB говорят о том, что в прошлом году злоумышленники пересмотрели «пул» своих жертв. Так, число фишинга под облачные хранилища практически удвоилось, а количество мошеннических страниц, нацеленных на пользователей интернет-провайдеров, возросло втрое. Ценность доступа к облачному хранилищу пользователя или его личному кабинету на сайте интернет-провайдера понятна: «охота», как всегда, идет за персональными или платежными данными, которые могут там храниться. Рост интереса к атакам на облачные хранилища и интернет-провайдеров сопровождался снижением объема фишинга под почтовые сервисы – их доля в общем количестве фишинговых ресурсов упала с 19,9% до 5,9% – и криптовалютные проекты.

Второе полугодие 2019 г. не внесло изменений в тренд последних нескольких лет: электронная почта осталась основным каналом доставки ВПО – шифровальщиков, банковских троянов, бэкдоров – и использовалась злоумышленниками в 94% изученных кейсов. В большинстве случаев (98%) ВПО пряталось во вложениях, лишь 2% фишинговых писем содержали ссылки, ведущие на загрузку вредоносных объектов. Для сравнения: в первом полугодии 2019-го 23% фишинговых писем содержали ссылки. Такая статистика может говорить о том, что письма с вложениями имеют для атакующих большую эффективность.

Для обхода корпоративных средств защиты, злоумышленники продолжили архивировать вредоносные вложения. Во второй половине 2019 г. в архивах доставлялось около 70% всех вредоносных объектов, в основном, для этого использовались форматы .rar (29%) и .zip (16%). Сам пароль для расшифровки содержимого злоумышленники указывали в письме с вредоносным вложением, в теме письма или в названии архива, либо, в ходе дальнейшей переписки с жертвой.

Шифровальщики остались самой распространенной «начинкой» фишинговых писем во второй половине прошлого года – они составили 47% от общего числа вредоносных вложений. Банковские трояны продолжили терять популярность и были обнаружены лишь в 9% вредоносных кампаний, уступив место шпионскому ПО и бэкдорам (35%). Такая перемена может быть обусловлена растущим функционалом бэкдоров, которые также могут быть использованы для похищения финансовой информации.

В Топ-10 инструментов, использовавшихся злоумышленниками в атаках, зафиксированных CERT-GIB во второй половине 2019, вошли шифровальщик Troldesh (55%); бэкдоры Pony (11%), Formbook (5%), Nanocore (4%) и Netwire (1%); банкеры RTM (6%) и Emotet (5%); и шпионское ПО AgentTesla (3%), Hawkeye (2%), и Azorult (1%). AgentTesla, Netwire и Azorult стали новыми угрозами наблюдаемого периода.

Компания Check Point Software Technologies зафиксировала более 192 тыс. случаев атак в неделю, связанных с коронавирусом в течении последних 14 дней. Это на 30% выше по сравнению с прошлыми неделями. Все атаки были связаны с

темой коронавируса и осуществлялись с фальшивых доменов, которые имитировали сайты международных организаций, а также сайт платформы Zoom.

Хакеры часто прибегают к использованию имени «Всемирной организации здравоохранения» (ВОЗ) для осуществления своих атак. Так, недавно киберпреступники осуществили фишинговую рассылку от лица ВОЗ (англ. World Health Organization, WHO) с использованием домена «who.int». Чтобы привлечь внимание жертвы, в теме письма мошенники указывали: «Срочное письмо от ВОЗ: результаты теста первой вакцины от COVID-19». К письму был прикреплен файл с именем «Xerox_scan_covid-19_urgent информационное письмо.xlxs.exe». При его загрузке автоматически устанавливался вредонос Agent Tesla, который используя кейлоггер похищал пароли с устройств пользователей.

Также исследователи Check Point обнаружили фишинговые письма, в которых от лица ООН и ВОЗ злоумышленники просят отправить деньги на биткоин-кошельки.

За последние три недели было зарегистрировано около 2449 новых доменов Zoom, 1,5% из которых – вредоносные (32), а 13% – подозрительные (320). С января во всем мире было зарегистрировано в общей сложности 6576 доменов, имитирующих платформу Zoom, среди них 37% пришлось на последние три недели после объявления пандемии коронавируса.

Злоумышленники также часто используют названия популярным сервисов Microsoft Teams и Google Meet для обмана людей. В последнее время пользователи получали фишинговые письма с темой: «You have been added to a team in Microsoft Teams» («Вы были добавлены в команду Microsoft Teams»). Нажимая на иконку «Открыть Microsoft Teams» жертвы переходили по зараженной ссылке (http://login\.microsoftonline.com-common-oauth2-eezylnrb\.medyacam\.com/common/oauth2/), загружая на свое устройство вредоносное ПО. Официальная ссылка Microsoft Teams выглядит совсем иначе: https://teams.microsoft.com/l/team.

Кроме того, исследователи Check Point обнаружили поддельные домены Google Meets. Например, «Googelmeets\.com», который был зарегистрирован 27 апреля.

За последние три недели было зарегистрировано 19749 новых доменов, связанных с темой коронавируса, из которых 2% являются вредоносными (354) и еще 15% – подозрительными (2961). С начала вспышки эпидемии во всем мире было зарегистрировано в общей сложности 90284 новых домена, связанных с COVID-19.

Исследователи Check Point вывили зависимость между возникновением фейковых доменов и этапами вспышек эпидемии.

1. В начале пандемии часто встречались домены, содержащие живые карты, которые позволяли отслеживать распространение вируса по разным регионам. Также популярны были сайты, описывающие симптомы коронавируса.

2. К концу марта внимание было сосредоточено на различных видах помощи и выплатах, которые осуществлялись в нескольких странах.

3. Затем широкое распространение получили домены, связанные с жизнью после коронавируса, а также домены, информирующие о второй волне эпидемии.

4. На протяжении всего периода пандемии домены, связанные с тестами и вакцинами, остаются неугасающим трендом для злоумышленников. Их общее число продолжает расти.

Меры предосторожности:

1. Остерегайтесь доменов, схожих с различными популярными сайтами. Обращайте внимание на орфографические ошибки в электронных письмах или на веб-сайтах;

2. Не доверяйте неизвестным отправителям. Будьте осторожны с файлами, полученными по электронной почте от неизвестных отправителей, особенно если при их открытии необходимо выполнить какие-либо действия (перейти по ссылке или открыть вложение к письму);

3. Используйте подлинные источники. Убедитесь, что при оформлении заказа вы используете официальный сайт. Не стоит переходить по ссылкам в электронных письмах. Вместо этого найдите нужный вам сайт самостоятельно с помощью поисковой системы, которой вы пользуетесь;

4. Остерегайтесь «специальных предложений». Предложение скажем «эксклюзивного лекарства от коронавируса» по почте или в интернете должно вызвать сомнение;

5. Убедитесь, что вы используете разные пароли для каждого приложения и каждой учетной записи». ***(Еженедельно свыше 190 тыс. кибератак эксплуатируют тему коронавируса // Компьютерное Обозрение (https://ko.com.ua/ezhenedelno_svyshe_190_tys_kiberatak_jekspluatiruyut_temu_koronavirusa_133082). 21.05.2020).***

***

«Компания Check Point Software Technologies зафиксировала 192 000 случаев атак в неделю, связанных с коронавирусом в течении последних двух недель. Это на 30% выше по сравнению с прошлыми неделями. Все атаки были связаны с темой коронавируса и осуществлялись с фальшивых доменов, которые имитировали сайты международных организаций, а также сайт платформы Zoom.

Атаки от лица ВОЗ и ООН

Хакеры часто прибегают к использованию имени Всемирной организации здравоохранения (ВОЗ) для осуществления своих атак. Так, недавно киберпреступники осуществили фишинговую рассылку от лица ВОЗ (англ. World Health Organization, WHO) с использованием домена «who.int». Чтобы привлечь внимание жертвы, в теме письма мошенники указывали: «Срочное письмо от ВОЗ: результаты теста первой вакцины от COVID-19». К письму был прикреплен файл с именем «Xerox_scan_covid-19_urgent информационное письмо.xlxs.exe». При его загрузке автоматически устанавливался вредонос Agent Tesla, который используя кейлоггер похищал пароли с устройств пользователей.

Также исследователи Check Point обнаружили фишинговые письма, в которых от лица ООН и ВОЗ злоумышленники просят отправить деньги на биткоин-кошельки.

Рост числа поддельных доменов Zoom

За последние три недели было зарегистрировано около 2449 новых доменов Zoom, 1,5% из которых — вредоносные (32), 13% — подозрительные (320). С января 2020 года во всем мире было зарегистрировано в общей сложности 6576 доменов, имитирующих платформу Zoom, среди них 37% пришлось на последние три недели после объявления пандемии коронавируса.

Атаки с использованием Microsoft Teams и Google Meets

Злоумышленники также часто используют названия популярным сервисов Microsoft Teams и Google Meet для обмана людей. В последнее время пользователи получали фишинговые письма с темой: “You have been added to a team in Microsoft Teams“ («Вы были добавлены в команду Microsoft Teams»). Нажимая на иконку «Открыть Microsoft Teams» жертвы переходили по зараженной ссылке (http://login\.microsoftonline.com-common-oauth2-eezylnrb\.medyacam\.com/common/oauth2/), загружая на свое устройство вредоносное ПО. Официальная ссылка Microsoft Teams выглядит совсем иначе: https://teams.microsoft.com/l/team.

Кроме того, исследователи Check Point обнаружили поддельные домены Google Meets. Например, «Googelmeets\.com», который был зарегистрирован 27 апреля 2020 года.

Рост доменов, связанных с темой COVID-19

За последние три недели было зарегистрировано 19 749 новых доменов, связанных с темой коронавируса, из которых 2% являются вредоносными (354) и еще 15% — подозрительными (2961). С начала вспышки эпидемии во всем мире было зарегистрировано в общей сложности 90 284 новых домена, связанных с COVID-19.

Темы и тенденции регистрации доменов, связанных с коронавирусом

Исследователи Check Point вывили зависимость между возникновением фейковых доменов и этапами вспышек эпидемии.

В начале пандемии часто встречались домены, содержащие живые карты, которые позволяли отслеживать распространение вируса по разным регионам. Также популярны были сайты, описывающие симптомы коронавируса.

К концу марта внимание было сосредоточено на различных видах помощи и выплатах, которые осуществлялись в нескольких странах.

Затем широкое распространение получили домены, связанные с жизнью после коронавируса, а также домены, информирующие о второй волне эпидемии.

На протяжении всего периода пандемии домены, связанные с тестами и вакцинами, остаются неугасающим трендом для злоумышленников. Их общее число продолжает расти.

«За последние три недели мы заметили изменения в тенденциях распространения поддельных доменов. Чтобы выжать максимум из сложившейся ситуации, хакеры прибегают к рисковым методам. — рассказывает Василий Дягилев, глава представительства Check Point Software Technologies в России и СНГ. — Если проанализировать последние кибератаки, очевидна тенденция имитирования доменов авторитетных организаций или популярных приложений. Например, в последнее время активно ведутся атаки от лица ВОЗ, ООН или Zoom. Сегодня особенно важно проявлять бдительность и остерегаться подозрительных

доменов и отправителей, если речь идет о рассылках по email». ***(Количество атак, связанных с коронавирусом, выросло на 30% // IKSMEDIA.RU (http://www.iksmedia.ru/news/5665013-Kolichestvoatak-svyazannyx-s-korona.html).21.05.2020).***

***

«Компания Microsoft опубликовала информацию об киберугрозах, собранных в ходе вредоносных кампаний, которые связаны с коронавирусной инфекцией (COVID-19). Таким образом техногигант намерен повысить осведомленность других организаций и предприятий об изменениях техник злоумышленников во время пандемии.

Как отметил президент и главный исполнительный директор некоммерческой организации Cyber Threat Alliance Майкл Дэниел (Michael Daniel), киберпреступники во время пандемии нацелены на людей, впервые использующих новые платформы. По его словам, злоумышленники переключили свое внимание на темы, связанные с COVID-19, пытаясь извлечь выгоду из страхов людей, общего недостатка информации и увеличения числа новых пользователей многих online-платформ.

Опубликованная компанией Microsoft информация включает 283 индикатора компрометации, которые использовались во вредоносных вложениях в кампаниях по электронной почте, связанных с пандемией. Многие вредоносные электронные письма были отправлены якобы от имени Всемирной организации здравоохранения или Красного Креста, в то время как в других письмах якобы предоставлялась информация о COVID-19». ***(Microsoft опубликовала идентификаторы киберугроз, связанных с COVID-19 // SecurityLab.ru (https://www.securitylab.ru/news/508351.php). 15.05.2020).***

***

«Пов'язані з пандемією COVID-19 обмеження влади на переміщення робочої сили по всьому світу змусили компанії адаптуватися до нових умов. Негайним відповіддю стало впровадження та інтеграція хмарних сервісів. Особливо хмарних інструментів для спільної роботи, таких як Microsoft Office 365, Slack і платформи для відеоконференцій. У новій доповіді компанії McAfee, що спеціалізується на кібербезпеки пристроїв і хмари, відзначено, що хакери зараз зосередилися на порушеннях, пов'язаних з використанням хмарних облікових записів.

Проаналізувавши дані про використання хмарних обчислень за січень-квітень 2020 року більш ніж 30 млн корпоративних користувачів своєї платформи моніторингу безпеки MVISION Cloud, компанія оцінює зростання використання хмарних сервісів у всіх галузях в 50%. Разом з тим в деяких галузях спостерігався набагато більше зростання, наприклад, в обробній промисловості – на 144%, в сфері освіти – на 114%.

Особливо високим було зростання застосування деяких інструментів для спільної роботи і відеоконференцій. Використання Cisco Webex зросла на 600%, Zoom – на 350%, Microsoft Teams – на 300% і Slack – на 200%. Знову ж таки, тут

теж лідирують виробництво і сфера освіти. Зростання поширення хмарних сервісів створює разом з тим підвищені ризики для безпеки.

Згідно з даними McAfee, трафік від некерованих пристроїв до корпоративних хмарним облікових записів подвоївся. За цей же період число зовнішніх загроз, націлених на хмарні сервіси, збільшилася на 630%, причому найбільше число атак було направлено на платформи для спільної роботи.

У своєму звіті McAfee розділила підозрілі спроби входу в систему і отримання доступу на дві категорії: «надмірно велика використання з аномального розташування» і «підозріло надприродне». В обох категоріях спостерігався схожий зростання за аналізований період. Перша категорія призначена для обліку успішних входів з місць розташування, які не зовсім звичайні з урахуванням профілю організації, після чого користувач отримує доступ до великих обсягів даних або виконує велику кількість привілейованих завдань.

До другої категорії відносяться входи одним і тим же користувачем з двох географічно віддалених місць протягом короткого періоду часу. Наприклад, якщо один і той же користувач входить в сервіс з однієї країни, а потім через кілька хвилин отримує доступ до сервісу, використовуючи IP-адреса в іншій країні.

Найбільше зростання загроз спостерігався в транспортній індустрії і логістики, досягнувши 1350%. За ними слід сфера освіти з ростом загроз в розмірі 1114%, урядові організації – 773%, виробництво – 679%, фінансові послуги – 571% і енергетика – 472%. В першу десятку джерел зовнішніх атак на корпоративні хмарні облікові записи по розташуванню IP-адрес увійшли Таїланд, США, Китай, Індія, Бразилія, Росія, Лаос, Мексика, Нова Каледонія і В'єтнам.

Також відзначено, що за останні роки значно зросла кількість атак, коли злочинці використовують списки «утёкшіх» або викрадених комбінацій імені користувача і пароля для отримання доступу до облікових записів. У доповіді, опублікованій в цьому році, компанія Akamai, що займається питаннями безпеки і доставки контенту, повідомила, що за період з грудня 2017 року по листопад 2019 року нею було зафіксовано 85,4 млрд атак проти організацій по всьому світу, які використовують неправильне поводження з обліковими даними. З них 473 млн атак було направлено на фінансовий сектор.

Щоб краще захистити хмарні облікові записи своїх співробітників і запобігти несанкціонованому доступу, McAfee рекомендує компаніям впровадити хмарні шлюзи безпеки». ***(Зростання хакерських атак на хмарні сервіси перевищив 1000% // Український телекомунікаційний канал (https://portaltele.com.ua/news/internet/zrostannya-hakerskih-atak-na-hmarni-servisi-perevishhiv-1000.html). 28.05.2020).***

***

«Хакери здійснили кібератаку на ізраїльські лабораторії в яких працюють над створенням вакцини проти кронавирусу SARS-CoV-2, повідомляє Jerusalem Post.

"Через кібератаки на минулому тижні було закрито сотні ізраїльських веб-сайтів. Дослідницькі центри, що працюють над створенням вакцини проти коронавірусу також стали жертвами кібератаки", – йдеться в повідомленні.

Наголошується, що атаки намагалися, але не змогли завдати шкоди процесу розробки вакцини. Також повідомляється, що з допомогою кібератак не намагалися вкрасти інформацію.

Крім того, зазначено, що про кібератаки повідомлялося і в інших дослідницьких центрах по вакцинам по всьому світу, в тому числі в США і Англії. У деяких нападах звинувачували Росію і Китай…» ***(Хакери атакували ізраїльські лабораторії де розробляється вакцина проти COVID-19 // Дзеркало тижня. Україна (https://dt.ua/WORLD/hakeri-atakuvali-izrayilski-laboratoriyi-de-rozroblyayetsya-vakcina-proti-covid-19-348953_.html). 26.05.2020).***

***

«Международный комитет Красного Креста призывает прекратить кибератаки в секторе здравоохранения на фоне COVID-19…

Красный Крест опубликовал во вторник обращение, в котором организация призвала прекратить кибератаки в медицинских и медицинских исследовательских учреждениях во время пандемии коронавируса.

В обращении сказано, что такие атаки ставят под угрозу человеческие жизни, и правительства должны принять «немедленные и решительные меры», чтобы остановить их.

«Мы надеемся, что правительства мира сделают все возможное, чтобы подтвердить свои обязательства по международным правилам, запрещающим такие действия», – сказал в письме президент Международного комитета Красного Креста Питер Маурер.

Это требование появилось после того, как в Чехии заявили о том, что сектор здравоохранения подвергся цифровой атаке.

Госсекретарь США Майка Помпео назвал кибератаку «безответственной и опасной».

Отмечается, что за последние несколько месяцев участились кибератаки на информационные системы больниц и исследовательских центров…» ***(Красный Крест призвал защитить сектор здравоохранения от кібератак // Журналист (https://journalist.today/krasnyj-krest-prizval-zashhitit-sektor-zdravoohranenija-ot-kiberatak/). 26.05.2020).***

***

«В апреле Google отправил более 1700 предупреждений пользователям, чьи учетные записи стали объектами хакерских атак, поддерживаемых правительством, после возобновления попыток взлома и фишинга.

Кибератаки в основном были связаны с коронавирусом, при этом многие хакеры «одели маски» Всемирной организации здравоохранения (ВОЗ).

Лидеры бизнеса в сфере финансовых услуг, консалтинга и здравоохранения в ряде стран, были охвачены кампаниями хакерских атак, поддерживаемыми государством.

Одним из примеров стал случай, когда хакеры выдавали себя за ВОЗ, побуждая людей подписаться на самую свежую информацию о пандемии.

«Сами приманки побуждают людей подписываться на прямые уведомления от ВОЗ, чтобы они всегда были в курсе объявлений, связанных с COVID-19, и размещают ссылки на сайты, созданные киберпреступниками, которые очень похожи на официальный сайт ВОЗ», - говорится в официальном заявлении Google.

«На сайтах, как правило, есть поддельные страницы входа, которые подталкивают потенциальных жертв отказаться от учетных данных аккаунта в Google, а иногда побуждают пользователей предоставлять другую личную информацию, такую как номера телефонов».

ВОЗ и другие организации, находящиеся в центре глобальной борьбы с распространением коронавируса, постоянно подвергаются кибератакам со стороны хакеров, которые ищут информацию о вспышке.

«С марта мы удалили более тысячи каналов YouTube, которые, по нашему мнению, являются частью большой кампании и ведут себя согласованно», - говорится в сообщении в блоге Google.

В прошлом месяце GCHQ (Центр правительственной связи Великобритании) предупредил, что киберпреступники пользуются страхами и тревогой по поводу вспышки коронавируса и «охотятся за легкой наживой» на теме COVID-19.

Национальный центр кибербезопасности Великобритании (NCSC), публичное подразделение разведывательного и охранного агентства, заявил, что он обнаружил определенную тактику хакеров, включая отправку поддельных электронных писем, предположительно от популярных служб видеоконференций, таких как Zoom и Microsoft Teams.

Наибольшую долю новых обнаруженных мошенников составили лица, выдававшие себя за государственные ведомства и/или организации здравоохранения. GCHQ заявил, что киберпреступники также пытаются использовать растущее число людей, работающих из дома, проверяя кибер-уязвимости в программном обеспечении для удаленной работы.» ***(Романов Роман. Google обнаружил всплеск хакерских атак при поддержке государства // InternetUA (https://internetua.com/google-obnarujil-vsplesk-hakerskih-atak-pri-podderjke-gosudarstva). 29.05.2020).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Представник України при ЄС Микола Точицький розповів, чому Україні варто брати участь в ініціативі Східного партнерства, і що вона планує в ній робити.

За словами дипломата, Україна планує посилити співпрацю з Євросоюзом у сферах кібербезпеки та боротьби з дезінформацією.

"Україна вже не перший рік чинить опір дезінформаційним атакам. Нині цей напрям набув особливої актуальності, враховуючи зусилля РФ з дестабілізації ЄС зсередини через дезінформацій кампанії, які руйнують довіру до європейських інституцій", - наголошує він у своїй статті для ZN.UA.

Україна планує продовжити започатковану міністром закордонних справ Дмитром Кулебою практику проведення засідань Україна-ЄС з питань стратегічних комунікацій для обговорення скоординованих дій щодо боротьби зі шкідливою дезінформацією в контексті COVID-19.

Ще одним пріоритетом є кібербезпека. Україна пропонує розглянути можливість залучення зацікавлених партнерів до роботи Агенції Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA).

"Ми б хотіли у майбутньому побачити діалоги ЄС-Східне партнерство з питань кібербезпеки. Масовані кібератаки на українську інфраструктуру навчили нас бути сильнішими і професійнішими, і ми готові ділитися нашим досвідом у форматі майбутніх кібердіалогів", - додає Точицький». ***(Дипломат назвав пріоритети співпраці України та ЄС у межах Східного партнерства // Чорноморські новини (https://www.blackseanews.net/read/163870). 20.05.2020).***

***

«Заместитель министра энергетики и защиты окружающей среды Алексей Рябчин обсудил с представителями USAID и команды проекта «Энергетическая безопасность» текущие и перспективные направления сотрудничества. Обсужден был и вопрос кибернетической безопасности, что может стать еще одним направлением сотрудничества. Об этом сообщает пресс-служба Минекоенерго, передает УНН.

Сообщается, что во время встречи Рябчин рассказал о мерах, которые принимает министерство и правительство для стабилизации энергетического сектора Украины. Он отметил, что кроме вопросов энергетической безопасности, в последнее время все более важной становится кибернетическая безопасность.

Исполняющая обязанности директора миссии USAID в Украине Сюзан Кутор отметила, что правительство США уделяет значительное внимание вопросам кибербезопасности, что может стать еще одним направлением сотрудничества Минекоенерго и USAID.

Заместитель министра также заверил, что вопрос экологизации и декарбонизации энергетики и в дальнейшем будут в фокусе Минекоенерго. Участники встречи договорились и в дальнейшем поддерживать диалог с существующих и перспективных программ сотрудничества…». ***(Евгений Радченко. Украина и USAID обсудили реализацию проекта «Энергетическая безопасность» // Независимый Регион (https://nr2.com.ua/politika/2020/05/15/ykraina-i-usaid-obsydili-realizaciu-proekta-energeticheskaia-bezopasnost/). 15.05.2020).***

***

Світові тенденції в галузі кібербезпеки

«Сьогодні вже існують процедури забезпечення кібербезпеки окремої інформаційно-телекомунікаційної системи організації (установи, фірми тощо), які достатньо задокументовані різними стандартами та нормативами. Однак, їх, навіть 100- відсоткова, практична реалізація не дозволяє гарантувати

повну безпеку організації. Свідченням цьому є відсутність позитивних тенденцій щодо зменшення результативності кібератак, втрат та негативних наслідків від їх реалізації.

Невирішеними залишаються дві основні проблеми:

- відсутність дієвих механізмів мотивації та контролю персоналу організації щодо безумовного виконання правил кібербезпеки;
- реактивність процедур аудиту кібербезпеки (тобто, аудит здійснюється шляхом аналізу подій, які вже відбулися).

Оцінка ризиків та прогнозування майбутніх загроз часто залишаються незрозумілими для керівництва організацій і не мотивують керівництво на вкладення коштів в інновації та розвиток в них кібербезпекової складової.

Цікавий аналіз внутрішньоорганізаційних загроз кібербезпеці проведений міжнародною компанією Ernst & Young Global Limited.

В результаті проведення цього аналізу встановлено:

Крім організованих хакерських угрупувань, які є основним джерелом кіберзагроз (23% кібератак), зростає кількість кібератак - 21% проводяться «Хактивістами», вони переслідують політичні чи соціальні цілі. Причому, часто ці «Хактивісти» є співробітниками тих же організацій, проти яких проводяться атаки;

Тільки 26% флагманів світової економіки розглядають питання забезпечення кібербезпеки вже на етапі планування нових бізнес-ініціатив;

Інвестиції в кібербезпеку, в першу чергу, орієнтовані на захист, а не на інновацію та трансформацію (лише 5% від загального бюджету спрямовується на кібербезпеку, і з них 77% ресурсів витрачається на управління ризиками та виконання нормативних вимог);

59% організацій відмічають, що у службі кібербезпеки «натягнуті» чи, в кращому випадку, нейтральні відносини з іншими підрозділами. Часто різні підрозділи орагнізації взагалі не взаємодіють (з питань кібербезпеки) між собою;

Лише близько 50% організацій, які досліджувались, виносять питання кібербезпеки на наради керівництва; менше половини керівників взагалі розуміють актуальність і необхідність забезпечення кібербезпеки;

Лише 7% організацій вважають, що служба кібербезпеки сприяє розвитку, 93% впевнені, що дотримання безпекових процедур та виконання нормативних вимог тільки стримує розвиток.

Очевидно, що вирішення зазначених проблем стосується докорінно нових підходів в організації менеджменту кібербезпеки.

Одним з таких підходів є впровадження в діяльність організації принципів інтегрованої безпеки (SbD - Secure by Design), розроблених компанією Amazon.

Ці принципи полягають в:

- перетворенні кібербезпеки в ключовий елемент цифрової трансформації (урахування аспектів кібербезпеки на етапі планування всіх нових проектів та грамотного використання механізмів забезпечення кібербезпеки для управління всіма ризиками організації, а також своєчасної розробки необхідних продуктів чи послуг);
- розвитку довірливих відносин служби кібербезпеки з кожним підрозділом організації шляхом спільного аналізу ключових бізнес-процесів,

визначення кіберизиків і розуміння того, як служба кібербезпеки може підвищити ефективність роботи кожного підрозділу організації;

- розробці комплексних показників ефективності роботи організації з урахування кіберризиків, які дозволять керівництву організації чітко зрозуміти важливість заходів забезпечення кібербезпеки.

Практична реалізація принципів інтегрованої безпеки полягає в розробці гнучких механізмів забезпечення кібербезпеки, розробці відповідної політики безпеки, налаштуванні та використанні відповідних програмно-апаратних засобів відповідно до функцій підрозділів організації (тобто виробничі процедури різних підрозділів формують завдання для служби кібербезпеки, а не навпаки).

Виходячи з цього стає можливим:

- створення сервісів, недоступних для зміни коростувачами, які не мають відповідного дозволу;
- організація надійної експлуатації системи контролю процесів організації;
- безперервний аудит в режимі реального часу;
- технічна реалізація управління підрозділами організації в формі безпечних

програмних скриптів…». ***(НАВЧАННЯ ПРИНЦИПАМ ІНТЕГРОВАНОЇ БЕЗПЕКИ (SBD) – ВИМОГА ЧАСУ ТА НОВІ МОЖЛИВОСТІ ДЛЯ УПРАВЛІНЦІВ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ // Державний університет телекомунікацій (http://www.dut.edu.ua/ua/news/1/category/0/view/8311). 06.05.2020).***

***

Сполучені Штати Америки

«Американские центры занятости заспамили поддельными заявлениями. Неизвестные мошенники из Нигерии используют украденную базу данных с личной информацией граждан США, чтобы от их имени получать пособия по безработице.

Время подобрано идеально

За расследование взялась Секретная служба США. По их данным, организаторы преступной схемы воспользовались уязвимостью в системах безопасности центров занятости во многих штатах. Основной целью мошенников был Вашингтон, однако есть доказательства кибератак во Флориде, Массачусетсе, Северной Каролине, Оклахоме, Род-Айленде и Вайоминге. Также сообщается о существовании обширной базы данных с украденной личной информацией, в основном, сотрудников экстренных служб, госслужащих и школьных работников…». ***(Антон Янковский. Как нигерийские хакеры обворовывают безработных в США // gagadget.com (https://gagadget.com/63123-kak-nigerijskie-hakeryi-obvorovyivayut-bezrabotnyih-v-ssha/). 18.05.2020).***

***

«Национальное криминальное агентство (National Crime Agency, NCA) Великобритании запустило рекламную кампанию, направленную на отвлечение детей от поиска незаконных услуг и вредоносных инструментов в сфере киберпреступности.

Как сообщил ИБ-эксперт Брайан Кребс (Brian Krebs), используя британский IP-адрес при поиске в Google определенных терминов, связанных с киберпреступностью, например, DDoS-как-услуга, бустеры, стрессеры или трояны для удаленного доступа (RAT), пользователь может увидеть рекламу, оплаченную ведомством.

NCA выбрала рекламу, указывающую на незаконность использования сервисов DDoS-как-услуга или RAT. Однако вместо того, чтобы просто отговаривать пользователей от незаконных действий, ведомство также использует рекламную кампанию для привлечения молодых людей в сферу кибербезопасности.

Например, некоторые рекламные объявления ссылаются на инициативу Cybersecurity Challenge в Великобритании, приглашающую «молодых талантливых людей» принять участие в играх, соревнованиях и семинарах по кибербезопасности.

По словам старшего менеджера NCA Дэвида Кокса (David Cox), реклама основывается на результатах отчета NCA 2017 года «Pathways into cybercrime» и ориентирована на мужчин в возрасте от 13 до 22 лет. Согласно результатам отчета, главными мотиваторами вступления в сообщество киберпреступников являются «достижения, испытания и самообучение», а не финансовая выгода.

Как отметил Кокс, рекламная кампания оказалась очень успешной и позволила получить более 5,3 млн показов и более 57 тыс. кликов за последние 30 дней. В настоящее время NCA ищет дополнительные источники финансирования для расширения рекламной кампании…». ***(Британская полиция отвлечет подростков от поиска вредоносных инструментов с помощью рекламы // SecurityLab.ru (https://www.securitylab.ru/news/508742.php). 30.05.2020).***

***

Протидія зовнішній кібернетичній агресії

«Федеральна прокуратура Німеччини видала міжнародний ордер на арешт росіянина, якого підозрюють у зламі комп'ютерних систем німецького парламенту у 2015 році на замовлення Головного розвідувального управління РФ…

Підозрюваним є 29-річний Дмітрій Бадін, якого також розшукують Сполучені Штати за хакерські атаки, включаючи крадіжку електронних листів Гілларі Клінтон та Демократичної партії напередодні президентських виборів 2016 року.

Кібератака на Бундестаг розпочалася 30 квітня 2015 року. У цей день кілька членів парламенту майже одночасно отримали електронний лист, адреса відправника якого закінчилася на "@un.org". Це виглядало як справжній електронний лист від Організації Об'єднаних Націй з темою: "Конфлікт України з Росією залишає економіку в руїнах".

Електронний лист містив посилання нібито на сайт ООН. Насправді сайт містив шкідливе програмне забезпечення, яке непомітно встановлювалося на комп'ютері людини, яка переходила за посиланням.

Докази про причетність Бадіна були отримані завдяки співпраці із нідерландськими колегами. У квітні 2018 року контррозвідувальне агентство Нідерландів розкрило групу росіян, які, як вважали, належать до підрозділу ГРУ "26165", також відомим як хакерська група "Fancy Bear".

Четверо чоловіків приїхали до Амстердама з дипломатичними паспортами, а потім їхали до Гааги на орендованому автомобілі. Вважалося, що вони планували зламати систему у штаб-квартирі Організації із заборони хімічної зброї (ОЗХЗ).

Кількома тижнями раніше колишній російський шпигун Сергій Скрипаль та його дочка отруїлися "новічком" у Британії - британський уряд звинуватив Москву в нападі.

До розслідування була залучена ОЗХЗ, лабораторії досліджували використану отруту. Голландські органи безпеки припускають, що російській команді хакерів було доручено зламати комп'ютери OPCW та викрасти інформацію.

13 квітня 2018 року голландські органи безпеки зупинили росіян і негайно вислали їх з країни - через їх дипломатичний статус вони не могли бути заарештовані. Її багаж - включаючи ноутбуки, мобільні телефони - було конфісковано.

Знайдена у них інформація стала знахідкою для слідчих у Німеччині, які після детального вивчення прийшли до висновків, що мають достатньо доказів проти Бадіна.

Видання відзначає, що хакер навряд чи виїде за межі країни, і навіть якби його спіймали в будь-якій точці світу, спочатку його мали б видати США. Втім, встановлення особи хакера є рідкісним випадком і само по собі вважається великим успіхом». ***(Німеччина видала ордер на арешт російського хакера, який зламав мережу Бундестагу // Українська правда (https://www.pravda.com.ua/news/2020/05/5/7250496/). 05.05.2020).***

***

«Російські хакери в 2015 році викрали листування канцлера Німеччини Ангели Меркель, отримавши доступ до комп'ютерів в її офісі в Бундестазі

…хакер під псевдонімом Scaramouche проник на комп'ютер Меркель п'ять років тому - 8 травня 2015 року.

Поки невідомо, які саме відомості йому і його поплічникам вдалося викрасти під час кібератаки. Загальний об'єм даних, до яких отримав доступ зловмисник, сягає не менше 16 гігабайт.

За даними слідства, за кібератакою стоїть російська військова розвідка…». ***(Російські хакери зламали електронну пошту Меркель, - Spiegel // ESPRESO.TV (https://espreso.tv/news/2020/05/08/rosiyski_khakery_zlamaly_elektronnu_poshtu_merkel_spiegel). 08.05.2020).***

***

«Рада ЄС продовжила до 18 травня 2021 року дію режиму санкцій у відповідь на злочинну кібердіяльність.

Про це… йдеться у повідомленні Ради ЄС.

Витік даних, крадіжка інтелектуальної власності, атаки на ІТ-інфраструктуру та викрадення секретної інформації можуть у майбутньому призвести до того, що ЄС накладе санкції на відповідальних за такі дії іноземних юридичних та фізичних осіб.

Санкції можуть бути спрямовані на тих, хто вчиняє ці види кібердіяльності в будь-якому місці, незалежно від їхньої національності та місцеперебування.

"Основною метою залишається стримування і реагування на кібератаки, спрямовані проти ЄС або його держав-членів. Обмежувальні заходи включають заборону на в'їзд осіб до ЄС і заморожування активів фізичних і юридичних осіб. Крім того, фізичним і юридичним особам ЄС заборонено надавати кошти тим, хто включений до переліку" - пояснили у Раді ЄС.

Це рішення було прийнято всього через кілька днів після заяви Європейського Союзу та його держав-членів про умисні кібератаки, що використовують пандемію коронавірусу. В заяві була відзначена рішучість ЄС запобігати, стримувати і реагувати на зловмисні кібератаки, в тому числі в рамках його більш широкого реагування на кризу COVID-19». ***(ЄС продовжив на рік дію санкційного режиму за кібератаки // Європейська правда (https://www.eurointegration.com.ua/news/2020/05/14/7109914/). 14.05.2020).***

***

«Міністерство внутрішньої безпеки США і ФБР попередили про 8 можливих сценаріїв втручання Росії у майбутні президентські вибори. Рівень їх загрози оцінили як "високий" і "помірний". Про це повідомляє Associated Press із посиланням на меморандум, підготовлений американськими спецслужбами…

"Міністерство внутрішньої безпеки і ФБР на початку цього року попередили, що Росія може втрутитися у вибори в США у 2020 році, таємно консультуючи політичних кандидатів і проводячи відповідні кампанії", - пишуть у виданні.

Так, у меморандумі передбачається 8 сценаріїв російського втручання. Серед загроз "високого" рівня виділили можливу хакерську атаку і витік інформації, так як подібне вже відбувалося під час президентської компанії у 2016 році при зломі серверів Національного комітету Демократичної партії США. Американські спецслужби вважають, що кібератаки провели хакери із РФ.

Передбачається, що російська сторона може також застосувати економічні і ділові важелі, просувати свої інтереси за допомогою фейкових акаунтів у

соцмережах, а також використовувати контрольовані державою ЗМІ, щоб поширювати серед цільової аудиторії теми, пов'язані з виборами.

Також Росія може маніпулювати з базами даних виборців та системами підрахунку голосів, а також може здійснити фінансову підтримку кандидатів у президенти і провести таємні консультації із представниками їхніх кампаній. Це спецслужби відносять до погроз "помірного рівня".

Імена конкретних "консультантів" не називаються, проте повідомляється, що раніше російські радники вели подібну кампанію у 20 африканських країнах.

Також у документі згадується, що до роботи в Африці мають відношення співробітники "ділового магната", близького до президента Росії Володимира Путіна. Зі всього видно, що цією людиною є російський бізнесмен Євгеній Пригожин, якого також називають "кухарем Путіна".

В агентстві підкреслюють, що документ був складений до пандемії коронавірусу. Її вплив на можливе російське втручання в вибори не оцінюється…». ***(Наталія Рябцева. Спецслужби США попередили про можливе втручання Росії у вибори президента – АР // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1867595-spetssluzhbi-ssha-poperedili-pro-mozhlive-vtruchannya-rosiyi-u-vibori-prezidenta-ar). 05.05.2020).***

***

«Дональд Трамп своим указом разрешил ограничивать закупку импортного оборудования для системы электроснабжения США – чтобы снизить риск кибератак из-за границы.

Указ обнародован на сайте Белого дома.

"Иностранные противники все чаще используют уязвимые места в системе электроснабжения США, которая поддерживает нашу национальную оборону, жизненно важные службы по чрезвычайным ситуациям, критически важную инфраструктуру, экономику и наш образ жизни. Эта система является целью для тех, кто стремится совершить злонамеренные действия против Соединенных Штатов и американского народа", - отмечается в документе.

Как указывается, угроза исходит прежде всего от потенциальных кибератак, которые могут создать значительные риски для национальной экономики, здоровья и безопасности людей, а также обороноспособности государства.

Своим указом Трамп наделил министра энергетики полномочиями запрещать приобретение, ввоз, передачу или установку энергетического оборудования от государств-противников, чтобы предотвратить возможные диверсии против системы электроснабжения США…». ***(США планируют снизить риск кибератак усиливая безопасность энергосистем // Телеграф (https://telegraf.com.ua/mir/usa/5453499-ssha-usilivayut-kiberbezopasnost-svoey-energosistemyi.html). 02.05.2020).***

***

«В апреле нынешнего года Иран осуществил кибератаку на несколько объектов водоснабжения и очистки Израиля. Как сообщил телеканал Fox News, в ходе кибератаки Иран использовал американские сервера.

Иностранный корреспондент Fox News Трей Йингст (Trey Yingst) сообщил в социальной сети Twitter, что «по словам высокопоставленного чиновника в министерстве энергетики США, администрация президента США Дональда Трампа делает все возможное, чтобы защитить своих союзников от кибернападений». Министерство энергетики США отказалось комментировать данную ситуацию, однако заверило, что расследование инцидента продолжается…». ***(Иран использовал серверы в США в кибератаке на израильские водные объекты // SecurityLab.ru (https://www.securitylab.ru/news/508158.php). 08.05.2020).***

***

«Можна було легко помітити, наскільки неприємно було канцлеру Ангелі Меркель виступати на пленарному засіданні Бундестагу й розповідати про кібератаки проти німецького парламенту, які відбулися навесні 2015 року. Ці ж напади стосувалися і її електронної пошти. "Мені від цього боляче", - сказала канцлер щиро. Вона завжди намагалася покращити відносини з Росією. Але тепер з'явилися "тверді докази, що "російські сили" відповідальні за хакерські атаки. І хоч Меркель говорила про "обурливі події", реакції на вчинки Росії досі немає. Про це пише Sueddeutsche Zeitung. Російський міністр закордонних справ Сергій Лавров відкидає всі звинувачення, озвучені Меркель. За його словами, конкретних доказів немає. Але через п'ять років після кібератак Генеральна прокурора Німеччини отрмала ордер на арешт Дмитра Бадіна.

29-річний росіянин працює на російську військову розвідку - ГРУ, а саме в кіберпідрозділі 26165, який також відомий як "Fancy Bear" чи APT28. Бадін заразив мережу Бундестага вірусом, який також виявили на комп'ютерах в офісі канцлера. Німецька система юстиції ще не мала справу з такими випадками. Іноземний шпигун, член іноземної військової розвідки, здійснив атаку проти парламенту Німеччини. Саме так злочин кваліфікувала Федеральна кримінальна поліція(BKA), яка за п'ять років провела ретельну роботу й зібрала велику кількість доказів. І суддя Федерального суду, який підписав ордер на арешт, вочевидь, згоден з висновками слідства. Ордер на арешт налічує більше 50 сторінок. І він надзвичайно чіткий. В ньому перелічені докази проти російського хакера, а також факти, які доводять його приналежність до ГРУ. У висновках йдеться про масштаби справи і її правова оцінка. Це "особливо тяжкий випадок" шпигунства, - написав суддя. Це була атака проти парламенту Німеччини, а отже проти захисника суверенітету ФРН, її народу і центрального елементу демократії. І скоїла цю атаку військова служба Росії. Це "безпрецедентний" випадок. Також суддя вважає, що ГРУ викрало дані для "дезінформації". І що далі? Видання пише, що федеральний уряд Німеччини здається розгубленим і не знає, як реагувати на результати розслідування. Меркель принаймні задала напрямок для реакції в Бундестазі. Вона сказала, що уряд обурений і жорстка дипломатична відповідь не виключена. Але досі конкретних рішень немає. Є певні сумніви. Ордер на арешт вже можна розглядати як сильний натяк для Москви. А відносини з Росією й без того напружені, - кажуть в Берліні. З іншого боку, уряд хоче дати Москві чітко зрозуміти, що така поведінка не прийнятна. В урядових колах в Берліні говорять, що йдеться не лише про хакерську атаку проти Бундестагу, яка сама має

"величезне" значення. Йдеться також про те, що російські спецслужби вже давно порушують усі правила гри. Вони скоюють не лише кібератаки, а й вбивства на німецькій території. 23 серпня 2019 року найманий вбивця застрелив посеред Берліна чеченця, який воював проти армії Росії. Вбивство сталося за лічені метри від офісу федеральної канцелярії ФРН. Виконавця схопили на місці. Німецькі слідчі вважають, що його в Німеччину прислали спецслужби Росії. У найближчі тижні генеральний прокурор прийме рішення, чи будуть державні органи РФ вказані в обвинувачувальному висновку як замовник. Якщо так, тоді справа буде розглядатися не просто як вбивство, а як акт державного тероризму. В німецькому уряді розуміють, що не можна кожен з випадків розглядати окремо. Потрібно, в першу чергу, бачити дедалі більшу агресивність Москви, яка стоїть за ними. Меркель під час виступу в Бундестазі нагадала, що Росія дотримується "стратегії гібридної війни". Sueddeutsche Zeitung пише, що у федеральній канцелярії, МЗС і федеральній службі розвідки (BND) не можуть вирішити, як краще відреагувати на поведінку Кремля. Зазвичай в таких випадках прийнято висилати співробітників спецслужб, які діють на німецькій території як дипломати. Але є загроза, що Кремль зробить те ж саме з німецькими дипломатами. І так Німеччина нашкодить сама собі. "Атака проти Бундестага була атакою проти нашої країни. Тому від міністра закордонних справ Гайко Мааса я чекаю щонайменше того, що він викличе російського посла", - вимагає політик від "Вільної демократичної партії" Мануель Хеферлін. "З часів Гійома жоден іноземний шпигун не підбирався так близько до німецького канцлера. Тому відповідь на цей інцидент повинна включати всі наслідки: правові і політичні", - додав політик. Видання нагадує, що Гюнтер Гійом був агентом НДР, який в 1970-ті роки став особистим референтом канцлера ФРН Віллі Брандта. Його викриття стало причиною для відставки канцлера». ***(Süddeutsche Zeitung: Німеччина не наважується покарати РФ за атаки на її суверенітет // Информационный портал "ua.today" (http://ua.today/news/world/s_ddeutsche_zeitung_nimechchina_ne_navazhuyetsya_pokarati_rf_za_ataki_na_yiyi_suverenitet). 19.05.2020).***

***

«Специализирующаяся на изучении вредоносного ПО исследовательская группа IssueMakersLab сообщила о кибероперации, проводимой Разведывательным управлением КНДР против турецкого производителя военной техники Otokar. Как пишет IssueMakersLab на своей странице в Twitter, с помощью целенаправленного фишинга служащие Пятого департамента (так называемой «35-й комнаты») атаковали сотрудников предприятия.

По словам исследователей, злоумышленники создали поддельную страницу авторизации в почтовом сервисе Outlook, которым пользуются сотрудники компании, как две капли воды похожую на настоящую. Никаких других подробностей о кибероперации IssueMakersLab не представила. Была ли попытка кибератаки успешной, также неизвестно.

Как ранее сообщал SecurityLab, северокорейская киберпреступная группировка Lazarus (другое название Hidden Cobra) вооружилась тремя новыми

вариантами вредоносного ПО – COPPERHEDGE, TAINTEDSCRIBE и PEBBLEDASH.

«35-я комната» – Департамент внешних расследований и разведки КНДР. Самая маленькая, но самая влиятельная спецслужба, занимающаяся Южной Кореей, Японией, международным сектором, США и Юго-Восточной Азией». ***(Северокорейские хакеры атаковали производителя военной техники // SecurityLab.ru (https://www.securitylab.ru/news/508343.php). 15.05.2020).***

***

«У Польщі повідомили про масову інформаційну атаку з боку Росії, спрямовану на дестабілізацію у стосунках між Варшавою і Вашингтоном

Про це йдеться в заяві польського уряду.

Йдеться про злам і розміщення на польських та іноземних ресурсах неправдивої і маніпулятивної інформації щодо навчань НАТО Defender Europe-2020.

«Польща знову стала метою інформаційних атак, що збігаються з діями Кремля проти Заходу, особливо проти країн НАТО. Організатори таких дій використали відомі методи: хакерську атаку, підміну контенту на інтернет-сторінках, а також підроблене інтерв'ю з американським генералом», — повідомив речник міністра-координатора в уряді Польщі з питань спецслужб Станіслав Жарин.

Внаслідок хакерських атак на кількох польських сайтах було розміщено матеріали про навчання Defender Europe-2020, які тривають у Східній Європі, зокрема в Польщі. На низці польських інтернет-ресурсів була розміщена стаття, в якій висміюється Польща та її армія.

За словами Жарина, це мало завдати удару по єдності НАТО і можливості спільних дій військ США та Польщі». ***(Польський уряд звинуватив Росію у кібератаках // Високий Замок Online. (https://wz.lviv.ua/news/413542-polskyi-uriad-zvynuvatyv-rosiiu-u-kiberatakakh). 29.05.2020).***

***

«Агенство національної безпеки США оголосило про те, що підрозділ ГРУ РФ, яке зламав пошту демократів у 2016 році, бере участь у триваючій кампанії щодо злому електронної пошти.

Хакери ГРУ Росії регулярно атакують поштові облікові записи. Але це перший випадок, коли АНБ випустило пряме публічне попередження, в якому назвали агентство і попередили про триваючу хакерську кампанію, пише NBC News.

У попередженні описується, як ГРУ РФ атакує непатентованою систему Unix, яка є альтернативою операційних систем Microsoft і Apple.

Наголошується, що це робота підрозділу 74455 ГРУ, яке було пов'язане іншими кібератаками.

"Вони, ймовірно, сама нахабна та успішна організація кібератак Росії", - сказав Джон Халквіст, директор служби аналізу кіберзагроз.

Велика Британії звинуватила підрозділ ГРУ РФ створенні вірусу NotPetya, який завдав шкоди на мільярди доларів.

У лютому Державний департамент звинуватив підрозділ 74455 у проведенні багаторівневої кампанії переслідування проти народу Грузії.

Раніше повідомлялося про те, що Федеральна прокуратура Німеччини видала ордер на арешт російського хакера, підозрюваного у зломі комп'ютерних систем парламенту Німеччини в 2015 році». ***(Агентство Нацбезпеки США попереджає: хакери ГРУ Росії як і раніше активні // Дзеркало тижня. Україна (https://dt.ua/WORLD/agentstvo-nacbezpeki-ssha-poperedzhaye-hakeri-gru-rosiyi-yak-i-ranishe-aktivni-349318_.html). 29.05.2020).***

***

«Глава израильского управления кибербезопасности заявил, что совершенное в прошлом месяце кибернападение на израильские системы водоснабжения было "синхронизированной и организованной атакой", направленной на подрыв жизненно важной национальной инфраструктуры. Считается, что за этой атакой стоял Иран.

Игаль Унна (Yigal Unna), возглавляющий Национальное управление по кибербезопасности, напрямую не стал упоминать Иран, как и комментировать предполагаемый ответный шаг Израиля, в результате которого на две недели закрылся ключевой иранский порт. Однако, он заявил, что недавние события открыли новую эру тайной войны, которую он угрожающие назвал "кибер-зимой".

Хотя Израиль и Иран много лет ведут тайные битвы, включающие хакерские взломы и кибератаки, по словам господина Унна попытка взлома израильских систем водоснабжения впервые в современной истории ознаменовала то, что объектами нападений становятся инфраструктурные объекты, то есть "ущерб наносится в реальной жизни, а не в сфере информационных технологий или области управления данными".» ***(В кибер-войне наблюдается "переломный момент" // ISRAland Online (http://www.isra.com/news/245846). 28.05.2020).***

***

«В четверг Агентство национальной безопасности США (АНБ) публично обвинило известную российскую хакерскую группу в использовании уязвимости в программном обеспечении, часто встречающемся в компьютерах Linux.

АНБ заявило, что наблюдало за тем, как хакеры из подразделения российской разведывательной службы ГРУ используют уязвимость для получения доступа к компьютерам.

Недостаток существует в программном обеспечении под названием «Exim», мессенджер, который, по мнению агентства, помогает упростить отправку электронной почты. АНБ сообщает, что хакерская группа, известная как Sandworm, эксплуатирует эту уязвимость с августа 2019 года.

Раскрывая, как работает эта уязвимость, АНБ стремится эффективно противостоять использованию этого инструмента российскими хакерами.

Это публичное обвинение ознаменовало тонкую эскалацию между двумя спецслужбами, оно было сделано вслед за указом президента Трампа, изданным в 2018 году, которым тот дал Министерству обороны, в состав которого входит АНБ, новые полномочия по поиску иностранных хакерских кампаний по кибератакам и более самостоятельному проведению своих собственных операций.

«Удаленный киберпреступник, не прошедший проверку подлинности, может отправить специально созданное электронное письмо для выполнения команд с привилегиями root, позволяющими хакеру устанавливать программы, изменять данные и создавать новые учетные записи», - говорится в пресс-релизе АНБ. Агентство призывает пользователей и администраторов систем применить уже выпущенное исправление для уязвимости exim. Агентство пока не сообщает какие именно компьютерные системы российские хакеры уже взломали, используя эту уязвимость.

Sandworm был связан с разрушительными кибератаками в Украине, в результате которых дважды отключалась энергосистема в стране и другие важные службы. США также обвиняют эту группу в том, что она стоит за печально известным вирусом NotPetya, который уничтожил компьютерные сети в крупных компаниях, включая Merck&Co, и поразил системы на зимних Олимпийских играх 2018 года.

В феврале Государственный департамент США связал Sandworm с атаками на правительственные сайты и телеканалы Грузии.

До недавнего времени правительство США связывало хакерские операции со спецслужбами иностранных правительств крайне редко. Когда это происходило, то часто делалось с помощью официальных документов, сопровождаемых обширными доказательствами, такими как обвинения Министерства юстиции в отношении пяти китайских военных хакеров в 2014 году.

Но поскольку агрессивность подобных хакерских атак возросла, то это стало основной причиной для публичных обвинений стоящих за ними спецслужб и даже конкретных спецподразделений.

В случае с Россией операции ГРУ, в том числе хакерское вмешательство в президентские выборы 2016 года в США, сделали их обьектом пристального внимания для АНБ за последние четыре года.» ***(Романов Роман. АНБ раскрыло уязвимость в Linux, которую использовали российские хакеры для кибератак // InternetUA (https://internetua.com/anb-raskrylo-uyazvimost-v-linux-kotoruua-ispolzovali-rossiiskie-hakery-dlya-kiberatak). 28.05.2020).***

***

Створення та функціонування кібервійськ

«Фахівці з Ізраїлю, по всій видимості, 9 травня зламали комп'ютерні системи іранського порту Шахід-Раджан, термінал якого розташовується в місті Бендер-Аббас на березі Перської затоки. Про кібератаку проти Ірану повідомила американська газета The Washington Post з посиланням на урядові джерела в США та інших країнах.

Одне з джерел газети в службах безпеки назвав кібератаку "високоточною". Він додав, що вона заподіяла більш значний, ніж це визнали в Ірані, коли повідомляли, що хакери змогли порушити роботу лише приватних комп'ютерних систем, не торкнувшись мережі Організації портів та судноплавства Ірану.

The Post пише, що в її розпорядженні є супутникові знімки Шахід-Раджан. На цих фотографіях розтягнулися на кілометри черзі судів на вході в порт, а 12 травня - десятки контейнеровозів в зоні очікування біля порту.

Така кібератака імовірно стала відповіддю на спроби киберзлому 24 квітня як мінімум двох водорозподільних мереж Ізраїлю…». ***(Ізраїль, ймовірно, влаштував кібератаку проти Ірану – Washington Post // Дзеркало тижня. Україна (https://dt.ua/WORLD/izrayil-ymovirno-vlashtuvav-kiberataku-proti-iranu-washington-post-348137_.html). 19.05.2020).***

***

Кіберзахист критичної інфраструктури

«Специалисты из компании Pen Test Partners сообщили о проблеме, затрагивающей компьютерные системы коммерческих самолетов. Система предупреждения столкновения самолетов в воздухе (Traffic Collision Avoidance System, TCAS) может быть обманута для принудительного изменения направления самолета, находящегося в воздухе.

Исследователи разработали эффективный метод спуфинга TCAS с помощью USB-ключа для цифрового видеовещания стоимостью $10 и вредоносного транспондера для связи с самолетом. С помощью систем, имитирующих настоящие самолеты, злоумышленник может заставить самолет под управлением автопилота менять высоту в заданном направлении.

«Поддельные самолеты» могут активировать систему предотвращения столкновений в самолете, предупреждающую пилота о том, что он должен либо подняться на высоту, либо спуститься, чтобы избежать столкновения в воздухе. Как отметили эксперты, в некоторых случаях (в основном самолеты Airbus) воздушное судно автоматически следует так называемым указаниям «Resolution advisory» системы TCAS и поднимается или опускается без участия пилота.

Исследователям удалось успешно продемонстрировать данную атаку на летном тренажере…». ***(Системы коммерческих самолетов подвержены спуфингу // SecurityLab.ru (https://www.securitylab.ru/news/508092.php). 06.05.2020).***

***

Захист персональних даних

«Вы не можете сделать доступ к контенту своего веб-сайта зависимым от того, согласен ли посетитель с тем, что вы сможете обрабатывать его данные,

ставя так называемую «стену cookie». Вам. нужно соблюдать европейский закон о защите данных!» — такое недвусмысленное сообщение опубликовал Европейский совет по защите данных (European Data Protection Board, EDPB) в руководстве по работе с пользовательской информацией.

Среди прочего, руководство теперь запрещает сайтам делать доступ к ним зависимым от того, дал ли пользователь согласие на обработку своих данных (так называемая «стена cookie» или cookie wall).

Согласно европейскому законодательству, наличие разрешения пользователя является одни м из шести обязательных условий при обработке персональных данных. В соответствии с «Общим регламентом по защите данных» (General Data Protection Regulation, GDPR), разрешение должно быть понятным, конкретным, сознательным и добровольным. Однако владельцы сайтов нашли способ, как выпросить у посетителей заветное разрешение с помощью «стены cookie», и стали предоставлять пользователям доступ к своим ресурсам только в обмен на разрешение на обработку их данных.

Оператором такой «стены cookie» в Европе является организация Internet Advertising Bureau Europe, запрашивающая у посетителей сайтов согласие на обработку данных, если они хотят получить доступ к контенту. Однако проблема в том, что такое «согласие» не является добровольным, как того требует GDPR, поэтому обновленное руководство EDPB запретило использование «стены cookie».

Кроме того, в новой редакции документа уточняется, что прокрутка страниц (скроллинг) не является согласием пользователя на обработку его данных. «Такие действия, как прокрутка или пролистывание web-страницы или аналогичные действия пользователей, ни при каких обстоятельствах не могут считаться удовлетворяющими требования четких и утвердительных действий», — говорится в обновленном руководстве». ***(Европейский совет по защите данных запрещает использование «стены cookie» // РосКомСвобода (https://roskomsvoboda.org/58098/). 07.05.2020).***

***

«Специалисты из компании по кибербезопасности Cyble купили в даркнете базу из 530 тыс. логинов сервиса видеоконференций Zoom. Стоила она чуть больше $6000. Посредником при продаже выступил анонимный русскоязычный Telegram-аккаунт.

В Cyble подлинность логинов установили благодаря тому, что некоторые из них принадлежали клиентам компании.

Zoom уже не впервые попадает в столь неприятную ситуацию. Так, сначала независимые специалисты по инфобезопасности обнаружили, что сервис отправлял данные в Facebook, не защищал видеозвонки сквозным шифрованием, затем в его приложениях для Windows и Mac OS нашли несколько «дыр», которые ставят под угрозу личные данные и файлы на компьютерах, и др.

На фоне пандемии сервис стал одним из самых популярных в мире. В марте Zoom получил приток миллионов новых пользователей, использующих его сервис во время пандемии коронавируса…». ***(Более полумиллиона логинов Zoom***

выставлены на продажу в интернете // РосКомСвобода (https://roskomsvoboda.org/58029/). 04.05.2020).

***

«Так как на этой неделе отмечался всемирный день пароля, компания Microsoft поделилась интересной статистикой в своем блоге.

По данным аналитиков, все больше людей отказываются от использования традиционных паролей и предпочитают им альтернативные решения для аутентификации. Так, количество пользователей применяющих «беспарольные» решения Microsoft, достигло 150 миллионов (по сравнению со 100 миллионами в ноябре 2019 года). Эта цифра охватывает пользователей онлайн-сервисов компании, таких как Azure, GitHub, Office и Xbox.

Статистика компании включает пользователей, полагающихся в работе на решение Windows Hello (распознавание отпечатков пальцев и лиц) для доступа к Azure Active Directory (Azure AD), а также пользователей, которые применяют приложение Microsoft Authenticator и ключи с поддержкой FIDO2 для входа в различные учетные записи без паролей.

Microsoft заявляет, что одна из ее текущих целей — побудить людей чаще использовать решения многофакторной аутентификации (MFA), а также «беспарольные» методы аутентификации, что позволит в целом повысить защищенность их учетных записей. Ведь исследования компании доказывают, что большинство людей, как правило, использует один и те же пароли многократно, подвергая свои учетные записи риску и облегчая их взлом.

Также в компании отмечают, что отказ от паролей позволяет снизить затраты на техническую поддержку, поскольку у сотрудников попросту нет паролей, которые они могут забыть, а затем попросить сбросить. Так, внутри Microsoft на «беспарольную» аутентификацию перешли уже 90% сотрудников». ***(Мария Нефёдова. Microsoft: 150 млн человек уже отказались от использования паролей // Хакер (https://xakep.ru/2020/05/08/passwordless-stats/). 08.05.2020).***

***

«Многие отраслевые СМИ на этой неделе сообщили, что неизвестный злоумышленник получил доступ к учетной записи сотрудника Microsoft на GitHub и скачал содержимое ряда private-репозиториев компании. В частности, Bleeping Computer пишет, что злоумышленник пользуется псевдонимом Shiny Hunters, — он вышел на связь изданием, предоставив журналистам доказательства взлома.

Хакер утверждает, что в общей сложности сумел похитить 500 Гб данных из репозиториев софтверного гиганта и сначала собирался продать их, но потом передумал и решил слить информацию в сеть бесплатно. Судя по содержимому дампа, утечка произошла 28 марта 2020 года.

В качестве «пробника» хакер предложил всем желающим изучить дамп размером 1 Гб, опубликовав его на неназванном хак-форуме. Bleeping Computer отмечает, что некоторые из опубликованных файлов содержат текст на китайском

языке, а также ссылки на latelee.org, из-за чего сначала у многих возникли сомнения в подлинности выложенной информации.

Изучив список каталогов украденных данных, а также исходные коды из private-репозиториев, исследователи Bleeping Computer пришли к выводу, что в руки хакера в основном попали образцы кода, тестовые проекты, электронные книги и прочие маловажные данные. Аналитики ИБ-компаний Nightlion Security и Under the Breach тоже изучили утечку и согласны с мнением журналистов: Microsoft определенно не о чем беспокоиться, а среди утекших файлов бесполезно искать иходники таких продуктов, как Windows и Office.

При этом утечка, судя по всему, все же была подлинной. Если сначала некоторые инженеры Microsoft писали в социальных сетях и сообщали СМИ, что данная утечка – это фейк, теперь они удалили свои записи и отказались от своих слов. Более того, Bleeping Computer и издание ZDNet сообщают, что сразу несколько сотрудников Microsoft, пожелавшие сохранить инкогнито, подтвердили, что по крайней мере некоторая часть украденных файлов являются подлинными, но хакер не получил доступа к исходному коду каких-либо крупных проектов Microsoft.

Сотрудники Microsoft объяснили, что исходные коды таких проектов размещаются исключительно на внутренних ресурсах корпорации, а не на общедоступном GitHub. Дело в том, что внутренняя политика компании требует, чтобы учетная запись Microsoft GitHub использовалась только для размещения и совместного использования проектов и документации с открытым исходным кодом. Также учетная запись может использоваться для размещения частных проектов, которые в будущем тоже станут доступны в виде опенсорсных решений.

По данным ZDNet, хакеру удалось проникнуть в 1200 приватных репозиториев. При этом издание пишет, что большая часть похищенных файлов и каталогов, вообще не имела отношения к Microsoft (среди них есть даже известные проекты с открытым исходным кодом, публичные уже много лет). Пока неясно, каким образом эти репозитории вообще попали в список злоумышленника.

Единственная реальная проблема, судя по всему, заключается в том, что некоторые скомпрометированные проекты могли содержать токены доступа и учетные данные API, которые теперь следует отозвать и сменить.

Опираясь на данные собственных источников, журналисты ZDNet говорят, что стоящий за этим инцидентом хакер — это тот же человек, что недавно взломал Tokopedia, крупнейший интернет-магазин в Индонезии.

Официальных комментариев об этом инциденте от Microsoft пока не поступало. В компании лишь сообщили, что уже проводят расследование случившегося». ***(Мария Нефёдова. Хакер получил доступ к GitHub-репозиториям Microsoft // Хакер (https://xakep.ru/2020/05/08/microsoft-github-leak/). 08.05.2020).***

***

«Швейцарский производитель электро- и дизель-поездов Stadler сообщил о кибератаке, в результате которой злоумышленники могли похитить данные компании и ее сотрудников. Stadler насчитывает порядка 11

тыс. человек, работающих на 12 производственных объектах и в 40 сервисах по всему миру.

Согласно сообщению компании, неизвестным удалось проникнуть в корпоративную IT-сеть, заразить некоторые компьютеры вредоносным ПО и, вероятно, похитить в процессе данные со скомпрометированных устройств. Объем похищенных данных пока не установлен.

Злоумышленники связались с компанией и потребовали выкуп, пригрозив в случае неуплаты опубликовать похищенную информацию. Обнаружив взлом, Stadler предприняла все необходимые меры по сдерживанию атаки и обратилась за помощью в расследовании инцидента к ИБ-специалистам. Соответствующая жалоба также была направлена в прокуратуру. В настоящее время компания занимается восстановлением затронутых систем из резервных копий.

Хотя в уведомлении компании не уточняется, была ли атака осуществлена с помощью вымогательского ПО, все свидетельствует в пользу этой теории. Во-первых, атакующие потребовали выкуп, а во-вторых, Stadler пришлось восстанавливать из резервных копий данные, очевидно, зашифрованные или удаленные вымогателем.

Компания не уточняет число затронутых производственных объектов, однако, согласно сообщениям швейцарских СМИ, инцидент затронул все производство, как в Швейцарии, так и за границей». ***(Производитель поездов Stadler подвергся кибератаке // SecurityLab.ru (https://www.securitylab.ru/news/508161.php). 10.05.2020).***

***

«Киберпреступная группировка REvil осуществила атаку на нью-йоркскую юридическую фирму в сфере развлечений Grubman Shire Meiselas & Sacks и теперь юридические дела десятков крупнейших мировых звезд музыки и кино, в том числе Леди Гага, Элтона Джона, Роберта Де Ниро и Мадонны, подвергаются риску разоблачения. Как сообщил ресурс Cointelegraph, злоумышленники угрожают опубликовать до 756 ГБ украденных данных в девяти поэтапных выпусках.

Похищенные данные включают в себя конфиденциальные контракты, номера телефонов, адреса электронной почты, личную переписку, соглашения о неразглашении и пр. Требуемая сумма выкупа неизвестна, однако он все также должен быть выплачен в биткойнах.

Похищенные данные касаются таких звезд Голливуда и музыкальной индустрии, как AC/DC, Барбара Стрейзанд, Бетт Мидлер, KISS, U2, Мадонна, Maroon 5, Роберт Де Ниро, Элтон Джон, Джон Мелленкамп, Род Стюарт, Рики Мартин, Шанайя Твейн, KISS, The Weeknd, Лил Уэйн и Дэвид Леттерман. Фирма представляет такие компании, как Facebook, Activision, iHeartMedia, IMAX, Sony, HBO и Vice Media, а также спортсменов Леброна Джеймса, Кармело Энтони, Слоана Стивенса и Колина Каперника». ***(Группировка REvil угрожает раскрыть юридическую информацию мировых звезд // SecurityLab.ru (https://www.securitylab.ru/news/508156.php). 08.05.2020).***

***

«Хакерская группа, известная под названием ShinyHunters, выложила на продажу в даркнете персональные данные пользователей сервисов 10 компаний из США, Индонезии, Южной Кореи. Среди них: сервис для знакомств Zoosk (скомпрометировано 30 миллионов записей), сервис печати Chatbooks, который позволяет заказывать печать книг с личными фотографиями (скомпрометировано 15 миллионов записей), сервис доставки еды Home Chef (скомпрометировано 8 миллионов записей) и другие, у каждой не менее миллиона украденных записей.

Хакеры оценивают данные в $18 000. Причем это общая сумма — база каждого сервиса продается отдельно. Сообщается, что эта же группа хакеров несет ответственность за недавний взлом базы индонезийской компании Tokopedia. В результате того взлома были скомпрометированы данные 91 миллиона клиентов». ***(Персональные данные 73 миллионов человек оказались в даркнете // SecureNews (https://securenews.ru/personal-data-of-73-million-people-were-on-the-darknet/). 11.05.2020).***

***

«Tokopedia — крупная индонезийская компания стоимостью более миллиарда долларов. Компания трудится в сфере e-commerce и представляет собой локальный конкурент Amazon и AliExpress. Ежемесячная посещаемость сайта составляет более 65 миллионов человек.

На этих выходных специалисты по информационной безопасности обнаружили базу данных с записями о пользователях Tokopedia. Данные включают адреса электронной почты, хэши паролей, имена и, по словам специалистов, множество других деталей. Базу данных, содержащую 91 миллион записей в даркнете продавали всего за 5000 долларов. В настоящее время проводится расследование инцидента. Пользователям советуют сменить пароли». ***(Индонезийская компания расследует утечку 91 миллиона записей о пользователях // SecureNews (https://securenews.ru/indonesian-company-investigates-leak-of-91-million-user-records/). 04.05.2020).***

***

«Более 30 организаций гражданского общества присоединились к запуску Глобальной коалиции по шифрованию (Global Encryption Coalition), чтобы продвигать и защищать шифрование в тех странах, где оно находится под угрозой. Новую коалицию возглавляет Управляющий комитет, состоящий из Center for Democracy & Technology (CDT), Internet Society и Global Partners Digital.

«Распространение COVID-19 подчеркнуло необходимость безопасных, приватных интернет-коммуникаций. Те, кому посчастливилось иметь сильные интернет-соединения, скорее всего, делятся всё большим количеством конфиденциальных данных онлайн. В то же время правительства по всему миру рассматривают политику, которая ставит под угрозу безопасность этих данных, — сказал Грег Нойхайм, старший консультант CDT и директор проекта Freedom,

Security and Technology Project. — Шифрование позволяет людям иметь приватную и безопасную цифровую жизнь».

Работая вместе с сообществом, которое быстро вырастет и будет включать компании и технологов, CDT и коалиция помогут активистам в ключевых странах, где шифрование находится под угрозой, таких как Канада, Австралия, Индия и Бразилия, противостоять предложениям, ослабляющим шифрование. «Коалиция предупредит технологов об угрозах шифрования по всему миру и создаст механизмы, с помощью которых они смогут делать экспертный анализ для смягчения этих угроз», — сказал Мэллори Нодел, главный технический директор CDT.

«CDT очень рада возможности предоставить экспертный анализ, глобальное сотрудничество и рупор в поддержку местных усилий по защите шифрования», — добавил Нойхайм.

«Internet Society взволновано объединением усилий Center for Democracy and Technology и Global Partners Digital для формирования Глобальной коалиции по шифрованию», — сказал Джефф Уилбур, старший директор Online Trust в Internet Society. — В условиях глобальной пандемии здравоохранения, приводящей к увеличению числа наших ежедневных действий и коммуникаций в интернете, шифрование становится более важным, чем когда-либо, для сохранения безопасности людей и стран. Мы с нетерпением ожидаем совместной работы с глобальным движением членов коалиции, сфокусированным на продвижении и защите использования сильной политики и практики шифрования по всему миру»…» ***(В мире появилась Глобальная коалиция по шифрованию // РосКомСвобода (https://roskomsvoboda.org/58648/). 18.05.2020).***

***

«Загроза безпеки даних лякає і викликає недовіру IT-фахівців — про це йдеться у звіті Oracle і KPMG про хмарні загрози безпеки у 2020 р за першу третину року (Oracle and KPMG Cloud Threat Report 2020). Опитування 750 фахівців з кібербезпеки та IT по всьому світу показало, що використання принципу «латання дірок» (patchwork approach) при розв'язанні проблем безпеки даних, неправильно налаштовані сервіси та плутанина з новими моделями хмарної безпеки породили кризу довіри. І її зможуть подолати тільки ті компанії, у яких безпека стала частиною культури ведення бізнесу.

Дослідження показало, що IT-фахівці більше стурбовані безпекою даних своєї компанії, ніж безпекою у себе вдома.

IT-фахівців втричі більше турбує безпека фінансових даних та інтелектуальної власності компанії, ніж безпека власного житла.

IT-фахівці відчувають занепокоєння щодо постачальників хмарних послуг, 80% фахівців вважають, що постачальники хмарних послуг, з якими вони ведуть бізнес, стануть їхніми конкурентами на ключових для них ринках.

75% IT-фахівців вважають, що публічна хмара захищена краще, ніж їх власні ЦОД, проте 92% IT-фахівців не вірять, що їх організації повністю готові до використання безпечних публічних хмарних сервісів.

Близько 80% IT-фахівців стверджують, що недавні витоки даних, з якими зіткнулися інші організації, змусили їх посилити захист даних при розвитку бізнесу.

IT-фахівці намагаються усунути проблеми захисту даних за допомогою «латання дірок» різними рішеннями з кібербезпеки, але стикаються з практично нездійсненним завданням, через те, що ці системи рідко бувають коректно сконфігуровані.

78% організацій використовують понад 50 різних рішень для забезпечення кібербезпеки, 37% компаній використовують понад 100 таких рішень.

У організацій, де виявлено неправильно налаштовані хмарні сервіси, того року відбулося 10 і більше інцидентів з втратою даних.

59% організацій повідомили, що вони зіткнулися з цільовою фішинговою атакою на облікові дані співробітників з привілейованими хмарними обліковими записами.

Найпоширеніші типи неправильного налаштування:

- облікові записи з надлишковими привілеями (37%);
- незахищені веб-сервери та інші типи серверних навантажень (35%);
- відсутність багатофакторної аутентифікації при доступі до основних сервісів (33%).
- Перекладання відповідальності веде до плутанини та порушень безпеки
- Як ніколи раніше організації переносять в хмару все більше критично важливих для бізнесу навантажень. А висхідне споживання хмарних сервісів створює нові «сліпі зони» в безпеці, оскільки IT-підрозділи та постачальники хмарних послуг працюють над тим, щоб зрозуміти, де їх індивідуальна відповідальність за безпеку даних. Ця плутанина призводить до того, що відділи інформаційної безпеки зазнають труднощів в спробах впоратися зі зростаючим ландшафтом загроз.

Майже 90% компаній вже використовують «ПО як послугу» (SaaS), 76% — «Інфраструктуру як послугу» (IaaS), а 50% організацій мають намір перенести всі дані в хмару протягом наступних двох років.
Моделі спільної відповідальності за безпеку створюють плутанину. Тільки 8% керівників служб інформаційної безпеки заявили, що повністю розуміють модель спільної відповідальності за безпеку.
70% IT-фахівців вважають, що для захисту всього середовища в публічній хмарі потрібно занадто багато спеціальних інструментів. 75% IT-фахівців неодноразово втрачали дані при використанні хмарного сервісу.

Модель «На першому місці — безпека» залишається актуальною

Для розв'язання проблем безпеки та подолання недовіри постачальники хмарних послуг та IT-підрозділи повинні працювати разом над формуванням культури «На першому місці — безпека» (Security-First). Така модель має на увазі наймання, підготовку та утримання кваліфікованих фахівців з інформаційної безпеки, а також постійне поліпшення процесів і технологій, які допомагають усувати загрози в умовах постійно розширюється цифрового світу.

69% організацій повідомляють, що директори по ІБ (CISO) реагують на проблеми інформаційної безпеки постфактум і беруть участь в проєктах використання публічної хмари тільки після серйозного інциденту.

73% організацій мають в штаті директора з інформаційної безпеки з досвідом роботи в хмарі або планують найняти такого фахівця. Більш ніж половина компаній (53%) створили нову посаду керівника з безпеки бізнес-інформації (Business Information Security Officer, BISO), який працює у співпраці з директором по ІБ (CISO) і допомагає інтегрувати культуру безпеки в організації.

88% IT-фахівців вважають, що протягом наступних трьох років в більшості хмар стане використовуватися інтелектуальне та автоматичне внесення виправлень і оновлень для підвищення безпеки.

87% IT-фахівців вважають, що обов'язковою умовою придбання нових засобів безпеки стане наявність у них можливостей штучного інтелекту (AI) і машинного навчання (MO). Вони забезпечать кращий захист від таких загроз, як шахрайство, шкідливе ПЗ і помилки конфігурації». ***(Дослідження: штучний інтелект і машинне навчання є обов'язковими для нових засобів безпеки // Blog Imena.UA (https://www.imena.ua/blog/ai-and-machine-learning-are-mandatory-for-security/). 19.05.2020).***

***

«Британська авіакомпанія EasyJet повідомила, що постраждала від кібератаки, в результаті якої зловмисники отримали доступ до електронного листування й історії подорожей приблизно 9 млн клієнтів та даних кредитних карток понад 2000 із них. Про це йдеться на сайті компанії.

Повідомляється, що авіакомпанія зв'язується з усіма постраждалими від кіберінциденту.

У компанії наголошують, що особисті дані клієнтів, такі як паспортні дані, до зловмисників не потрапили.

Наразі невідомо, хто саме стоїть за даною кібератакою.

Національний центр кібербезпеки Великої Британії займається даним розслідуванням…» ***(Авіакомпанія EasyJet заявила про викрадення даних близько 9-ти мільйонів клієнтів // Журналист (https://journalist.today/aviakompanija-easyjet-zajavila-pro-vikradennja-danih-blizko-9-ti-miljoniv-kliientiv/). 20.05.2020).***

***

«…Дані 1,2 тисячі співробітників і членів Європарламенту потрапили у відкритий доступ. "Масштабний витік даних" торкнувся також 15 тисяч облікових записів інших фахівців у справах Євросоюзу. Про це заявив віце-президент ЄП з політики в області IT Марсель Колайя, повідомляє «Є!» з посиланням на Politico. За його словами, у відкритий доступ потрапила, в тому числі, конфіденційна інформація і зашифровані паролі. Колайя не став називати політичні об'єднання, які зачепив витік, але Politico пише, що йдеться про найбільшу політичну фракцію в Європарламенті - Європейську народну партію (ЄНП). Представник ЄНП Педро Лопес де Пабло підтвердив витік даних, в тому числі адрес електронної пошти і паролів, але назвав їх застарілими. За його словами, ці дані використовувалися

користувачами сайту в 2018 році на старому сайті ЄНП, а в 2019 році партія запустила новий сайт, сервери і актуальна база даних на якому не постраждали. “ Зараз їм нічого не загрожує, тому що в парламенті система вимагає повністю змінювати свій пароль кожні три місяці, - заявив він. Як пише видання, першими витік виявили в індійській компанії Shadowmap, яка надає послуги в сфері кібербезпеки. Її засновник Яш Кадакія сказав, що виявив файли з конфіденційною інформацією через інтернет-портал, який є частиною домену сайту Європарламенту і використовується його посадовими особами. За його словами, файли містили інформацію про тисячі людей і їхні зв'язки з політичними партіями та установами, в тому числі з Європолом, агентством ЄС з безпеки зовнішніх кордонів Frontex та інших…». ***(Європарламенті заявили про масштабний витік даних // Є Україна (http://www.ednist.info/news/99606). 17.05.2020).***

***

«У той час як Google доводиться мати справу з шпигунськими програмами Play Store, з'явилася нова проблема, яка може ще сильніше зашкодити Android-користувачів, і це стосується сервісу Firebase.

Нагадаємо, що Firebase - це платформа для розміщення додатків, куплена Google в 2014 році. За словами експертів з кібербезпеки, розробники 24 000 додатків, доступних в Play Store, неправильно налаштували системи безпеки Firebase. В результаті персональні дані, зібрані усіма цими розробниками у відповідних додатках, що знаходяться під загрозою і доступні безпосередньо на серверах Firebase. Хакери можуть скористатися даними в цілях особистої вигоди або подальшого злому акаунтів користувачів Android-смартфонів.

Конкретно, будь-який досвідчений хакер може проникнути в систему і вкрасти велику кількість особистої інформації, такої як адреси електронної пошти, паролі, ідентифікатори, номери телефонів, адреси електронної пошти або навіть IP-адреси. За даними Comparitech, деякі бази даних на Firebase навіть містять банківські реквізити та посвідчення особи!

Як ви можете собі уявити, вся ця інформація може бути продана за високими цінами в Dark Web. Отже, цей недолік являє собою значне джерело доходу для хакерів. Крім того, вони також можуть виконувати шкідливий код і впроваджувати шкідливі або вимагачі усередині додатку. І це, не насторожив пильність розробників». ***(Як 24 000 Android-додатків допомогли хакерам дізнатися особисті дані мільйонів користувачів мережі // Знай.ua (https://techno.znaj.ua/310979-yak-24-000-android-dodatkiv-dopomogli-hakeram-diznatisya-osobisti-dani-milyoniv-koristuvachiv-merezhi). 14.05.2020).***

***

«Хакерская группа Shiny Hunters утверждает, что взломала 10 компаний и в настоящее время продает похищенные у них пользовательские данные в даркнете.

Shiny Hunters – это группировка, на прошлой неделе взявшая на себя ответственность за взлом GitHub-репозиториев Microsoft, а также недавно взломавшая Tokopedia — крупнейший интернет-магазин Индонезии. Так,

изначально хакеры бесплатно слили в открытый доступ данные 15 000 000 пользователей Tokopedia, а позже выставили на продажу всю БД компании, содержащую 91 000 000 миллион записей, оценив ее в 5000 долларов США.

Видимо, прибыль от продажи данных Tokopedia воодушевила хакеров, так как теперь группа выставила на продажу украденные БД еще 10 компаний. Среди них:

- приложение для знакомств Zoosk (30 миллионов записей);
- печатный сервис Chatbooks (15 миллионов записей; компания официально подтвердила компрометацию);
- южнокорейская fashion-платформа SocialShare (6 миллионов записей);
- служба доставки еды Home Chef (8 миллионов записей);
- интернет-магазин Minted (5 миллионов записей);
- интернет-газета Chronicle of Higher Education (3 миллиона записей);
- южнокорейский мебельный журнал GGuMim (2 миллиона записей);
- медицинский журнал Mindful (2 миллиона записей);
- индонезийский интернет-магазин Bhinneka (1,2 миллиона записей);
- американская газета StarTribune (1 миллион записей).

Суммарно перечисленные базы данных насчитывают 73,2 миллиона записей, которые хакеры оценили примерно в 18 000 долларов, причем каждая база данных продается отдельно. Злоумышленники поделилась «образцами» некоторых БД с потенциальными покупателями, и журналисты издания ZDNet убедились, что хакеры продают вполне реальные пользовательские данные.

При этом подлинность некоторых БД пока проверить нельзя, хотя многие представители ИБ-сообщества, включая компании Nightlion Security, Under the Breach и ZeroFOX, считают, что Shiny Hunters не шутят и представляют собой весьма опасную хак-группу.

Также некоторые полагают, что Shiny Hunters могут быть связаны с Gnosticplayers — другой хакерской группой, которая работает по похожей схеме, была очень активна в прошлом году и продала более миллиарда учетных данных в даркнете». ***(Мария Нефёдова. Группировка Shiny Hunters выставила на продажу данные 10 компаний // Xakep (https://xakep.ru/2020/05/12/shiny-hunters-sale/). 12.05.2020).***

***

«Популярный бесплатный сервис по решению математических задач Mathway стал жертвой взлома, в результате которого в руки преступников попали более 25 млн адресов электронной почты и хешей паролей пользователей приложения.

…источником утечки является некто ShinyHunters, ранее заявивший о взломах учетной записи Microsoft в сервисе GitHub, приложения Wishbone и пр. Похищенные данные ShinyHunters предлагал на подпольных торговых площадках и хакерских форумах. По некоторым оценкам, число пользователей, данные которых оказались в продаже, превышает 200 млн.

Как пояснил изданию ShinyHunters, взлом Mathway произошел в январе 2020 года. Хакер не вдавался в подробности, но рассказал, что получил доступ к базе

данных компании, скачал информацию, а затем закрыл «лазейку» во избежание обнаружения.

В начале мая ShinyHunters выставил похищенные данные на продажу по цене примерно $4 тыс. в биткойнах или Monero на подпольных форумах, однако на прошлой неделе копия БД Mathway начала распространяться в различных Telegram-каналах, принадлежащих так называемым брокерам данных - киберпреступникам, специализирующимся на покупке и перепродаже украденной информации.

По словам представителей Mathway, компании известно об утечке, и в настоящее время ведется расследование инцидента». ***(На продажу выставлены данные 25 млн пользователей сервиса Mathway // SecurityLab.ru (https://www.securitylab.ru/news/508595.php). 24.05.2020).***

***

«В Сети выложена для бесплатного скачивания база данных 40 млн пользователей популярного мобильного приложения Wishbone. БД была опубликована на одном из хакерских форумов, где она раньше продавалась за 0,85 биткойна (порядка $8 тыс.).

В базе данных содержатся имена пользователей, электронные адреса, номера телефонов, места проживания (город/штат/страна) и хэши паролей. По словам опубликовавшего ее пользователя, пароли зашифрованы с применением SHA1, но, как показывает ее анализ, некоторые пароли зашифрованы с использованием слабого алгоритма MD5, и получить их можно с помощью доступных в интернете бесплатных инструментов. Кроме того, в БД содержались ссылки на фотографии профиля, в том числе несовершеннолетних, у которых Wishbone пользуется огромной популярностью.

Как сообщил пользователь, данные были получены в результате взлома, имевшего место ранее в нынешнем году. Последние регистрации и входы датированы январем 2020 года, что подтверждает этот факт. Ответственность за утечку взял на себя некто Шайни Хантерс (Shiny Hunters), в начале мая также заявивший о похищении 500 ГБ данных из GitHub-репозитория Microsoft.

Опубликовавший БД пользователь является так называемым дата-брокером – киберпреступником, спекулирующим на перепродаже краденых данных (один из таких дата-брокеров на днях был задержан Службой безопасности Украины). В настоящее время этот пользователь продает базы данных десятков компаний, в общей сложности содержащие более 1,5 млрд записей.

Большая часть БД содержит данные, утекшие в результате известных взломов прошлых годов. В 2017 году компания Wishbone уже подвергалась кибератаке, но в опубликованном сейчас массиве информации того времени нет». ***(В Сети опубликованы данные 40 млн пользователей Wishbone // SecurityLab.ru (https://www.securitylab.ru/news/508587.php). 22.05.2020).***

***

«В даркнете выставлена на продажу база данных более нефункционирующего хакерского форума и торговой площадки для сбыта

похищенной информации WeLeakData.com. Часть данных также была раскрыта в личных переписках хакеров, некогда пользовавшихся услугами сайта.

WeLeakData.com представлял собой форум и торговую площадку, где обсуждались, продавались и покупались базы данных, похищенные в результате утечек, и списки пар логинов и паролей, использующихся для атак с подстановкой учетных данных (credential stuffing). В конце прошлого месяца сайт неожиданно был закрыт, и появились слухи, будто его оператор был арестован, а база данных похищена или продана. С тех пор на подпольных форумах регулярно появляются объявления о желании купить утекшую БД.

Согласно новому отчету ИБ-компании Cyble, дамп базы данных форума WeLeakData.com на движке vBulletin, датированный с начала 9 января 2020 года, теперь продается на черном рынке. Как и любая другая форумная БД, она содержит логины пользователей, электронные адреса, хэши паролей, IP-адреса, с которых делались публикации на форуме, и личные сообщения. Подобная информация представляет большую угрозу для киберпреступников, поскольку с ее помощью правоохранительные органы могут отследить их и связать с известными кибератаками.

Согласно отчету Cyble, БД использовалась для запуска нового сайта Leaksmarket.com, на форуме которого опубликованы те же посты и личные сообщения от тех же пользователей из базы данных WeLeakData.com. По мнению специалистов, через некоторое время после закрытия сайт, скорее всего, был продан одному из членов форума и снова заработал». ***(Личные сообщения хакеров выставлены на продажу // SecurityLab.ru (https://www.securitylab.ru/news/508194.php). 12.05.2020).***

***

«Популярна останнім платформа для онлайн-конференцій Zoom почне відключати користувачів для того, щоб змусити їх перейти на більш безпечну версію програми.

Раніше у Zoom неодноразово відбувалися великі витоки призначених для користувача даних, в результаті чого сервіс піддавався жорсткій критиці з боку фахівців з кібербезпеки. Для вирішення проблема компанія випустила версію Zoom 5.0 з 256-бітовим шифруванням AES, яка повинна суттєво підвищити безпеку. Також в оновленні поліпшено функції управління конфіденційністю.

Вже з сьогоднішнього дня компанія починає відключати користувачів, що використовують стару версію програмного забезпечення. Це зроблено для того, щоб вони не могли відмовитися від поновлення перед тим, як продовжити використання відео конференцій». ***(Митник Михайло. Zoom починає відключати користувачів // TechnoPortal.com.ua (https://technoportal.com.ua/programy/50010). 30.05.2020).***

***

«Базы данных ElasticSearch, предположительно управляемые подразделением Advanced Wireless Network (AWN) крупного оператора

мобильной связи в Таиланде Advanced Info Service (AIS), с около 8 млрд интернет-записей миллионов тайских пользователей находились в Сети в открытом доступе.

Исследователь безопасности Джастин Пейн (Justin Paine) обнаружил незащищенные паролем базы данных, содержащие DNS-запросы и данные сетевого протокола Netflow в Сети. По словам Пейна, любой может быстро собрать необходимую информацию о действиях пользователя в режиме реального времени. Используя обнаруженные данные, любой человек мог узнать информацию о подключенных устройствах в доме интернет-пользователя, установленном антивирусном программном обеспечении, используемых браузерах и посещаемых соцсетях.

Пейн предупредил AIS об утечке данных 13 мая. Компания в течении недели не реагировала на уведомление, и Пейн сообщил об инциденте Национальной компьютерной группе реагирования на чрезвычайные инциденты Таиланда (ThaiCERT). Вскоре базы данных были отключены.

NetFlow — сетевой протокол, разработанный компанией Cisco Systems для сбора информации об IP-трафике и мониторинга сетевого трафика. Анализируя данные о потоках, можно получить представление о потоке и объеме сетевого трафика». ***(8 млрд записей тайских интернет-пользователей оказались в Сети // SecurityLab.ru (https://www.securitylab.ru/news/508625.php). 25.05.2020).***

***

Кіберзлочинність та кібертероризм

«GoDaddy, крупнейший в мире регистратор доменов, обслуживающий примерно 19 млн клиентов по всему миру, подвергся кибератаке…

Злоумышленники скомпрометировали ряд хостинговых аккаунтов, используя украденные логины и пароли. Сам инцидент произошёл в конце октября 2019 г., но только сейчас GoDaddy опубликовал результаты расследования и разослал пострадавшим клиентам уведомления о случившемся.

Компания указывает, что нет никаких признаков того, что злоумышленники добавляли или изменяли какие бы то ни было файлы на хостинговых ресурсах, к которым получили доступ:

«Недавно мы обнаружили подозрительную активность на определённом подмножестве наших серверов и немедленно принялись за расследование. Выяснилось, что неавторизованный индивидуум получил доступ к вашим реквизитам доступа, используемым для SSH-соединения с вашим хостинговым аккаунтом».

В электронном письме GoDaddy также говорится, что нарушение ограничено только учетными записями хостинга и не касается учетных записей клиентов или личной информации, хранящейся в них. Отмечается, что не было обнаружено никаких доказательств того, что какие-либо файлы были изменены или добавлены в затронутые учетные записи, однако в письме не говорится, были ли файлы просмотрены или скопированы.

В связи с этим, все учетные записи затронутых хостинговых учетных записей были сброшены, и в электронном письме была приведена процедура, которую клиенты должны выполнить, чтобы восстановить доступ к соответствующим учетным записям хостинга. GoDaddy также рекомендовал «в целях предосторожности» пользователям проверять свои учетные записи хостинга.

Расследование пока ещё далеко от завершения. Доступ злоумышленников к системам компании был закрыт, и GoDaddy пытается разобраться — какое потенциальное воздействие может быть оказано на её среду. Пострадавшим от атаки компания готова предоставить бесплатные услуги по восстановлению безопасности, а также удалит вредоносные программы. GoDaddy выражает сожаление о произошедшем…». ***(Из-за утечки данных крупнейший регистратор доменов GoDaddy сбросил пароли // РосКомСвобода (https://roskomsvoboda.org/58045/). 06.05.2020).***

***

«…Специалисты по кибербезопасности зафиксировали резкое увеличение количества попыток украсть учетные записи Microsoft Teams. Об этом пишет Forbes.

Microsoft Teams была запущена в марте 2017 года. С начала марта 2020 года аудитория платформы выросла с 44 млн до более чем 75 млн активных пользователей в сутки.

Компания Abnormal Security сообщила, что зафиксировала рассылку от 15 000 до 50 000 писем, копирующих вид официальных сервисных сообщений Microsoft, но со ссылками на мошеннические адреса. Страницы и доменные адреса, на которых пользователю предлагают ввести данные своего аккаунта, копируют аналогичные ресурсы Microsoft.

При этом мошенники применили ряд технических средств, таких как множественная переадресация, чтобы обмануть автоматические системы защиты от спама.

Специалисты предостерегают, что одна и та же учетная запись используется и для доступа к Teams, и для облачного сервиса Microsoft 365. Таким образом, взлом учетной записи Microsoft Teams может привести к утечке внутренней переписки либо документов компаний, использующих сервис». ***(Евгений Радченко. Зафиксирована массовая атака на учетные записи Microsoft Teams // Независимый Регион (https://nr2.com.ua/tehnologii/2020/05/05/zafiksirovana-massovaia-ataka-na-ychetnye-zapisi-microsoft-teams/). 05.05.2020).***

***

«Специалисты компании Wordfence предупредили о новой масштабной вредоносной кампании, нацеленной на сайты под управлением WordPress. Только за последние семь дней злоумышленники попытались взломать порядка 1 млн сайтов.

Кампания началась 28 апреля 2020 года, и уже через несколько дней объем фиксируемого Wordfence вредоносного трафика превысил обычные показатели в 30 раз. Судя по полезной нагрузке, которую злоумышленники пытаются внедрить

на атакуемые сайты, за большинством атак стоит одна и та же киберпреступная группировка. Полезная нагрузка представляет собой вредоносный JavaScript-код, переадресовывающий пользователей на вредоносные ресурсы и пользующийся сеансом администратора для внедрения бэкдора в header темы.

Кроме того, злоумышленники эксплуатируют давно известные уязвимости, позволяющие менять домашний URL-адрес сайта на тот же домен, что используется в полезной нагрузке XSS для переадресации посетителей на сайты с вредоносной рекламой. Наиболее популярными уязвимости являются: межсайтовый скриптинг в плагине Easy2Map, Blog Designer (обе исправлены в 2019 году) и теме Newspaper (исправлена в 2016 году), а также обновление опций в WP GDPR Compliance (исправлена в 2018 году) и Total Donations (исправлена в 2019 году).

По данным Wordfence, в прошлом эта группировка осуществляла куда менее масштабные кибератаки, но в последнее время она существенно усилила активность – только за один день 3 мая специалисты зафиксировали более 20 млн попыток взлома свыше полумиллиона сайтов. За месяц было выявлено более 24 тыс. IP-адресов, отправляющих запросы, совпадающие с атаками на 900 тыс. сайтов». ***(Киберпреступники атаковали 1 млн сайтов под управлением WordPress // Goodnews.ua (https://goodnews.ua/technologies/kiberprestupniki-atakovali-1-mln-sajtov-pod-upravleniem-wordpress/). 06.05.2020).***

***

«Fresenius, крупнейший в Европе оператор частных больниц и основной поставщик продуктов и услуг для диализа, стал жертвой кибератаки с использоваением вымогательского ПО. Как сообщают источники KrebsOnSecurity, инцидент нарушил работу некоторых систем, но уход за пациентами продолжается.

Базирующаяся в Германии Fresenius включает четыре независимых предприятия: Fresenius Medical Care, ведущий поставщик услуг для людей, страдающих почечной недостаточностью; Fresenius Helios, крупнейший в Европе оператор частных больниц; Fresenius Kabi, поставляющее фармацевтические препараты и медицинские приборы; и Fresenius Vamed, управляющий медицинскими учреждениями.

Один из сотрудников Fresenius Kabi в США сообщил, что компьютеры в здании его компании были взломаны, и кибератака затронула каждую часть деятельности компании по всему миру. В ходе атаки было использовано вымогательское ПО Snake, представляющее собой относительно новый вредонос. Операторы Snake атакуют в основном крупные компании, отключают их IT-системы и требуют выкуп в биткойнах за доступ к данным.

«Я могу подтвердить, что IT-системы Fresenius стали жертвой вредоносного ПО. В качестве меры предосторожности были предприняты шаги для предотвращения дальнейшего распространения. Мы также проинформировали соответствующие следственные органы, и хотя некоторые функции в компании в настоящее время ограничены, обслуживание пациентов продолжается», — сообщил представитель Fresenius.

По словам исследователей безопасности, вымогательское ПО Snake несколько уникально тем, что оно пытается идентифицировать IT-процессы, связанные с инструментами управления предприятием и крупными автоматизированными системами управления технологическим процессом. Вредонос написан на языке Golang и обладает более высоким уровнем обфускации, чем другие вымогатели.

После запуска Snake удаляет теневые копии томов компьютера, а затем отключает многочисленные процессы, связанные с системами SCADA, виртуальными машинами, системами промышленного управления, инструментами удаленного управления, программным обеспечением для управления сетью и пр. Затем он шифрует файлы на устройстве, пропуская те, которые находятся в системных папках Windows, и различные системные файлы». ***(Крупнейший в Европе оператор частных больниц пострадал от вымогателя Snake // SecurityLab.ru (https://www.securitylab.ru/news/508120.php). 07.05.2020).***

***

«Операторы вымогательского ПО атаковали компьютерные системы тайваньской государственной энергетической компании CPC Corp.

Компания CPC Corp представляет собой важный национальный актив, ответственный за доставку нефтепродуктов и импорт сжиженного природного газа. Как сообщили представители компании, несмотря на то, что кибератака не повлияла на производственные процессы, она помешала попыткам некоторых клиентов использовать платежные карты CPC Corp для покупки газа.

Согласно данным сервиса VirusTotal, два вредоносных файла, использованных в ходе атаки, были идентифицированы как вымогательское ПО.

Власти Тайваня в настоящее время ведут расследование и пока не назвали виновника кибератаки на CPC Corp. Официальный web-сайт компании был отключен некоторое время, но CPC Corp вскоре восстановила работу своих IT-систем и в публичном заявлении пообещала «внедрить более строгую систему обнаружения киберугроз». ***(Тайваньская энергетическая госкомпания подверглась атаке вымогателей // SecurityLab.ru (https://www.securitylab.ru/news/508085.php). 06.05.2020).***

***

«В настоящее время ведется масштабная вредоносная кампания, в рамках которой были взломаны системы различных компаний. Киберпреступники активно сканируют Сеть на предмет серверов с установленным программным обеспечением Salt, используемым для управления и автоматизации серверов внутри центров обработки данных, кластеров облачных серверов и корпоративных сетей. По словам команды разработчиков платформы для ведения блогов Ghost, преступники эксплуатировали уязвимости обхода аутентификации (CVE-2020-11651) и обхода каталога (CVE-2020-11652) в Salt с целью получить контроль над главным сервером.

Несмотря на то, что преступники имели доступ к сайтам Ghost(Pro) и биллинг-сервисам Ghost.org, они не похитили финансовую информацию или учетные данные пользователей. Вместо этого они загрузили майнер криптовалюты.

Попытка майнинга вызвала нагрузку процессоров и перегрузила большинство компьютерных систем, немедленно предупредив специалистов о проблеме. Разработчики Ghost отключили все серверы, исправили системы и через несколько часов снова возобновили их работу.

По словам некоторых специалистов, атаки, скорее всего, проводились с помощью автоматического сканера уязвимостей, который обнаруживал устаревшие Salt-серверы, а затем автоматически эксплуатировал две уязвимости для установки вредоносного ПО.

«Вполне возможно, что виновники данных атак даже не знают, какие компании они взламывают в настоящее время. Уязвимые Salt-серверы зафиксированы в банках, web-хостингах и компаниях из списка Fortune 500», — сообщили эксперты.

Компания Saltstack, разработавшая программное обеспечение Salt, уже выпустила исправления для данных уязвимостей. В настоящее время в интернете обнаружено около 6 тыс. уязвимых Salt-серверов». ***(Преступники взломали блог-платформу Ghost и установили криптомайнер // SecurityLab.ru (https://www.securitylab.ru/news/508041.php). 05.05.2020).***

***

«Национальное управление по кибербезопасности получило сообщения о кибератаках на израильские веб-сайты и заявило, что справляется с ситуацией.

СМИ на иврите приводят скриншоты из социальных сетей, на которых фигурирует фраза "будь готов к большому сюрпризу" на иврите и на английском языке, а также изображение избитого и окровавленного премьер-министра Биньямина Нетаниягу (Benjamin Netanyahu), плавающего на фоне взрывов в Тель-Авиве.

Официально не сообщается, кто стоит за терактами. Однако, на изображениях можно рассмотреть иранские флаги и символы. Считается, что взлому поспособствовала уязвимость в плагине на платформе "WordPress". В число жертв кибератаки попали местные власти Мицпе-Рамона и Рамат-ха-Шарона, а также сеть "Cofix", "United Hatzalah" и персональный веб-сайт депутата Кнессета Ницана Горовица (Nitzan Horowitz), о чем сообщает ресурс "Ynet".» ***(На десятки израильских сайтов совершено нападение // ISRAland Online Ltd (http://www.isra.com/news/245558). 21.05.2020).***

***

«Команда израильских ИБ-специалистов рассказала о новой DNS-проблеме NXNSAttack, которая может использоваться для значительной амплификации DDoS-атак.

Исследователи рассказывают, что проблема влияет на рекурсивные DNS-серверы, а также процесс делегирования DNS. И хотя атаки NXNSAttack могут быть реализованы по-разному, основные шаги в любом случае будут одинаковыми:

Злоумышленник отправляет DNS-запрос на рекурсивный DNS-сервер. Запрос для домена, типа attacker.com, который управляется через подконтрольный хакеру авторитативный DNS-сервер.

Так как рекурсивный DNS-сервер не авторизован резолвить этот домен, он перенаправит операцию вредоносному DNS-серверу злоумышленника.

Вредоносный DNS-сервер отвечает рекурсивному DNS-серверу, заявляя, что делегирует операцию резолвинга DNS длинному списку name-серверов. Этот список содержит тысячи поддоменов для сайта жертвы.

Рекурсивный DNS-сервер перенаправляет DNS-запрос всем поддоменам в этом списке, создавая огромную нагрузку на авторитативный DNS-сервер жертвы.

В итоге злоумышленник, эксплуатирующий проблему NXNSAttack, может добиться амплификации простого DNS-запроса в 2–1620 раз по сравнению с его - первоначальным размером. Такая нагрузка может привести к сбою DNS-сервера жертвы, а когда DNS-сервер отключится, пользователи не смогут попасть на атакованный сайт, так как домен сайта резолвится не сможет.

Эксперты пишут, что коэффициент амплификации пакетов будет зависеть от конкретного ПО, работающего на рекурсивном DNS-сервере, но в большинстве случаев амплификация будет во много раз больше, чем при использовании других методов.

По мнению авторов NXNSAttack, в настоящее время такие DDoS-атаки являются одними из наиболее опасных, ведь злоумышленники могут проводить затяжные и мощные кампании, автоматизировав DNS-запросы и имея в своем распоряжении всего несколько устройств.

Перед проблемой NXNSAttack уязвимы такие решения, как ISC BIND (CVE-2020-8616), NLnet labs Unbound (CVE-2020-12662), PowerDNS (CVE-2020-10995), а также CZ.NIC Resolver Knot (CVE-2020-12667) и коммерческие DNS-сервисы, таких крупных компаний, как Cloudflare, Google, Amazon, Microsoft, Oracle (DYN), Verisign, IBM Quad9 и ICANN.

На протяжении последних нескольких месяцев эксперты тесно сотрудничали с производителями ПО для DNS, сетями доставки контента и DNS-провайдерами, чтобы обезопасить от NXNSAttack DNS-серверы по всему миру.

Патчи для уязвимостей NXNSAttack активно выпускаются уже несколько недель, и они призваны предотвратить злоупотребление процессом делегирования DNS. Администраторам рекомендуется как можно скорее обновить ПО своего DNS-резолвера до последней версти». ***(Мария Нефёдова. Атака NXNSAttack позволяет усилить DDoS в 1620 раз // Xakep (https://xakep.ru/2020/05/20/nxnsattack/). 20.05.2020).***

***

«Согласно ежегодному долкаду Verizon по киберпреступности, опубликованному во вторник, мотивация материальной выгоды превзошла шпионаж в качестве главной причины для взлома данных за прошлый год.

В отчете говорится, что около 9 из 10 кибератак были финансово мотивированы на основе изучения более 32 000 инцидентов и почти 4 000 подтвержденных взломов в 81 стране.

В докладе Verizon Business 2020 по исследованию нарушений данных установлено, что количество подтвержденных нарушений данных удвоилось по сравнению с предыдущим годом. Поскольку пандемия коронавируса вынуждает людей находиться дома, ожидается, что число кибератак на предприятия возрастет.

Об этом также свидетельствует недавний хакерский взлом клиентской базы британской авиакомпании EasyJet, который привел к утечке данных 9 млн. пассажиров.

В докладе отмечается, что 86% киберпреступлений были совершены из-за денег, а не по причине шпионажа. Кража учетных данных, фишинг и компрометация деловых электронных писем стали причиной 67% кибератак.

Чем больше предприятий перешло на веб-решения, тем больше хакеров стали охотиться за их базами данных. Согласно отчету, нарушения в веб- и облачных приложениях выросли до 43%, что вдвое больше, чем в предыдущем году.

Такие корпорации, как Facebook, Salesforce, Google и Amazon расширили работу на удаленке, по крайней мере, до конца этого года, и ожидается, что еще больше компаний последуют их примеру. Генеральный директор Verizon Business Group Тами Эрвин (Tami Erwin) сказал, что «цифровое преобразование» модели «работа на дому» во время пандемии коронавируса продемонстрировало ряд «красных флажков» для кибербезопасности.

«Многие компании в конечном итоге отправляют сотрудников на работу из дома, не задумываясь над тем, что будет с некоторыми элементами их безопасности в будущем», - заявил Эрвин в интервью агентству Reuters. «Я думаю, что сотрудники, работающие дома, определенно, более уязвимы для кибератак».

Эрвин сказал, что компании могут защитить себя от кибератак, если сотрудники будут обучены защите от фишинга и других мошеннических методов доступа к конфиденциальной информации». ***(Романов Роман. Доклад: материальная выгода превосходит шпионаж как основной мотив киберпреступлений // Internetua (https://internetua.com/doklad-materialnaya-vygoda-prevoshodit-shpionaj-kak-osnovnoi-motiv-kiberprestuplenii). 19.05.2020).***

***

«Издание Bleeping Computer рассказывает, что операторы вымогательского ПО стали использовать новую тактику, позволяющую получить от жертв больше денег. Теперь создатели малвари требуют у пострадавших компаний два выкупа: один за расшифровку данных, а другой за удаление информации, которую хакеры похитили во время атаки. В случае неуплаты злоумышленники угрожают опубликовать эти данные в открытом доступе.

Журналисты напоминают, что еще в конце 2019 года создатели вымогательской малвари стали действовать по новой схеме. Все началось с операторов шифровальщика Maze, которые начали публиковать файлы, похищенные ими у атакованных компаний, если жертвы открывались платить.

Хакеры завели для таких «сливов» специальный сайт, и уже скоро их примеру последовали другие группировки, включая Sodinokibi, DopplePaymer, Clop, Sekhmet, Nephilim, Mespinoza и Netwalker.

Теперь к ним присоединились авторы вымогателя Ako, однако они пошли даже дальше своих "коллег". Группировка заставляет некоторые компании платить выкуп дважды: за расшифровку файлов и за удаление украденных данных. В качестве примера на сайте Ako опубликованы данные одной из жертв: компания выплатила 350 000 долларов за расшифровку информации, однако хакеры все равно опубликовали ее файлы на своем сайте, так как не получили «второй выкуп» за удаление украденных файлов.

Один из операторов Ako ответил на вопросы Bleeping Computer и подтвердил, что двойное вымогательство используется только для некоторых жертв: всё зависит от размера компании и типа украденных данных. Как правило, размер второго выкупа колеблется от 100 000 до 2 000 000 долларов США, то есть обычно превышает стоимость расшифровки данных.

Злоумышленники утверждают, что некоторые компании вообще предпочитают заплатить именно за удаление данных, но не за их расшифровку. К примеру, этим путем пошли неназванные медицинские организации из США, у которых были украдены конфиденциальные данные пациентов, номера социального страхования и так далее. Подтвердить или опровергнуть эти заявления преступников журналистам не удалось.

«Компании с большим доходом пугаются, когда мы говорим об украденных файлах. Так что это мотивация для других компаний, которые должны заплатить», — объясняют хакеры». ***(Мария Нефёдова. Вымогатели стали требовать второй выкуп за удаление похищенных файлов // Xakep (https://xakep.ru/2020/05/14/ako-double-ransom/). 14.05.2020).***

***

«Исходный код для бортовых компьютеров микроавтобусов Mercedes-Benz оказался в онлайн доступе. Его обнаружил швейцарский программист Тилль Котманн. Он через гугл поиск нашел Git-портал, принадлежащий Daimler AG — материнской компании Mercedes-Benz. Тилль смог зарегистрировать аккаунт на портале, после чего скачал 580 репозиториев, содержащих исходный код. Код предназначен для компонента OLU — технологии, которая связывает автомобиль с облачными сервисами и позволяет разработчикам создавать приложения для отслеживания автомобиля на дороге, получения данных о его состоянии, заморозке функций автомобиля в случае угона и других целей. Изначально утечка казалась безобидной, но специалисты позже выяснили, что некоторые данные могут быть использованы злоумышленниками для будущих атак на информационные системы Daimler». ***(Ненастроенные права доступа к репозиториям с кодом для автомобилей Mercedes привели к утечке // SecureNews (https://securenews.ru/unconfigured-permissions-for-repositories-with-code-for-mercedes-cars-leaked/). 19.05.2020).***

***

«Возможности систем, установленных на ключевых объектах «умного» производств, во много раз превышают необходимые для выполнения целей, для которых они были развёрнуты, и злоумышленники могут обратить эти «лишние» мощности себе на пользу.

Компания Trend Micro опубликовала результаты исследования Threats and Consequences: A Security Analysis of Smart Manufacturing Systems, посвящённого атакам на промышленные объекты. В нём описывается, как современные хакеры могут использовать нестандартные векторы атаки, чтобы выводить из строя «умное» оборудование на производстве, и даются рекомендации в части поддержания кибербезопасности для специалистов по операционным технологиям.

Для работы над этим исследованием специалисты Trend Micro объединили усилия с Миланским техническим университетом (Politecnico di Milano), который предоставил свою лабораторию Industry 4.0 с реальным производственным оборудованием от лидеров отрасли. На примере этого оборудования было продемонстрировано, как киберпреступники могут использовать функции и уязвимости в объектах промышленного интернета вещей в своих целях, например, для промышленного шпионажа или получения финансовой выгоды.

«В прошлом киберпреступники применяли для атак на производственное оборудование традиционное вредоносное ПО, которое можно было обезвредить при помощи обычных средств защиты сетевой инфраструктуры и конечных устройств. Современные же хакеры предпочитают разрабатывать специализированные инструменты, которые используют сами операционные технологии, чтобы избежать обнаружения, — отметил Билл Малик (Bill Malik), вице-президент направления инфраструктурных стратегий вTrend Micro. — В ходе работы над исследованием мы выявили, что есть целый ряд возможных векторов атак, целью которых станут подобные уязвимости объектов индустрии 4.0. В результате промышленным предприятиям может быть нанесён ощутимый ущерб, как финансовый, так и репутационный. Для борьбы с этими новыми атаками мы порекомендовали бы специализированные решения для промышленного интернета вещей, которые способны выявлять и устранять сложные целевые угрозы».

«Политехнический университет Милана считает обеспечение безопасности объектов индустрии 4.0 и повышение надёжности систем их автоматизации и управления одной из своих важнейших задач. Особенно это актуально в связи с тем, что эти объекты становятся всё более важной частью современного производства и оказывают всё большее влияние на бизнес-сферу», — отмечают Джакомо Тавола (Giacomo Tavola), профессор Миланского технического университета, работающий в области разработки и менеджмента производственных систем, и Стефано Дзанеро (Stefano Zanero), доцент того же университета и специалист по вопросам кибербезопасности.

В ключевых объектах «умного» производства в основном используются проприетарные системы, но по своей вычислительной мощности они вполне сравнимы с традиционным ИТ-оборудованием. Это значит, что возможности таких систем во много раз превышают необходимые для выполнения целей, для которых они были развёрнуты, и злоумышленники могут обратить эти «лишние» мощности себе на пользу. Хотя в таких системах чаще всего используются проприетарные

языки, они, как и в случае с атаками на ИТ-системы, могут применяться для ввода вредоносного кода, получения доступа к другим объектам сети или кражи конфиденциальной информации без риска обнаружения.

«Умные» производственные системы изначально проектируются и развёртываются как изолированные объекты, но эта изоляция разрушается по мере роста взаимодействия между информационными и операционными технологиями в производстве. Из-за применения этого подхода такие системы по умолчанию почти лишены механизмов для борьбы с вредоносным ПО и проведения проверок целостности.

К числу систем и оборудования, уязвимых для взлома, относятся, например, системы управления производством (MES), интерфейсы «человек-машина» (HMI) и настраиваемые объекты промышленного интернета вещей. Они являются слабым звеном в системе безопасности производственного объекта, которое хакеры могут использовать, чтобы повредить изготавливаемые товары, вызвать неисправности оборудования или внести изменения в рабочие процессы, что приведёт к выпуску бракованной продукции.

В исследовании предлагаются комплексные меры для защиты от атак и снижения их негативного воздействия, включая:

- глубокую инспекцию пакетов, которая поддерживает протоколы операционных технологий и способна выявить аномальные пакеты данных на уровне сети;
- регулярные проверки целостности, которые помогут обнаружить изменённые хакерами компоненты ПО на конечных устройствах;
- использование подписи исполняемого кода в устройствах промышленного интернета вещей, включая зависимые объекты и ПО, например, библиотеки от сторонних производителей;
- анализ рисков, который затрагивает не только физическую безопасность производства, но и ПО для его автоматизации;
- цепочки сертификатов для всех данных и программного обеспечения в «умных» производственных средах;
- применение инструментов для обнаружения и распознавания уязвимостей/«программных закладок» в сложном производственном оборудовании;
- применение «песочниц» и разделение привилегий для ПО промышленного оборудования». ***(Опубликовано исследование, посвящённое атакам на промышленные объекты // IKSMEDIA.RU (http://www.iksmedia.ru/news/5663102-Trend-Micro-opublikovala-issledovan.html). 12.05.2020).***

***

«Pitney Bowes, компания с оборотом более 5 млрд долларов и 3 тысячами патентов в областях обработки почты, мобильных платежей, шифрования, лазерной печати и других, подверглась атаке вируса-вымогателя. Ответственность за атаку несет хакерская группа Maze, использующая одноименный вирус.

Группировка опубликовала скриншоты, по которым можно сделать вывод, что в их руках оказались данные сотрудников компании, важная финансовая информация и информация о клиентах.

Однако представители компании заявляют, что все не так страшно. Они сразу же привлекли к работе сторонних специалистов по информационной безопасности. В результате атаку удалось остановить до того, как вирус зашифрует данные, и хакеры успели получить доступ лишь к ограниченному объему информации. На данный момент следов присутствия в корпоративной сети неавторизованных пользователей нет, но расследование инцидента продолжается.

Это уже вторая за 7 месяцев подобная атака на Pitney Bowes. По информации Microsoft, Maze — одна из нескольких хакерских группировок, которые совершали атаки на больницы в период эпидемии коронавируса.» ***(Хакерская группировка Maze атаковала крупную коммерческую компанию // SecureNews (https://securenews.ru/hacker-group-maze-attacks-a-large-commercial-company/). 12.05.2020).***

***

«Исходный код оригинальной консоли Microsoft Xbox и код Windows NT 3.5 утекли в Сеть. Исходный код Xbox включает ядро операционной системы оригинальной консоли, кастомной версии Windows 2000. Как сообщили представители Microsoft изданию The Verge, компании известно об инциденте, и в настоящее время ведется расследование.

Хотя утекшая ОС консоли Xbox включает среды разработки, эмулятор Xbox Development Kit для тестирования и внутренние документы, это мало чем поможет разработчикам самодельных игр под Xbox. Энтузиасты и раньше в частном порядке обменивались исходным кодом и кодом ядра, и эта утечка вряд ли станет для них особенно полезной.

Неофициальные эмуляторы в течение многих лет пытались воспроизвести это ядро, но пока что поддержка есть только у сорока игр, в то время как официальных насчитывается порядка 900. У Microsoft есть собственные эмуляции для игр под Xbox и Xbox 360, однако они доступны только для Xbox One, но не для Windows-ПК.

Как уже упоминалось, помимо исходного кода Xbox в Сеть утекла практически финальная сборка Windows NT 3.5. Код включает все необходимые инструменты для разработки и позволит энтузиастам хорошенько изучить операционную систему. Поддержка Windows NT 3.5 закончилась в декабре 2001 года, и сейчас она используется только на ограниченном количестве устройств, поэтому утечка не будет иметь существенных последствий». ***(Исходный код оригинальной Xbox и код Windows NT 3.5 утекли в Сеть // SecurityLab.ru (https://www.securitylab.ru/news/508565.php). 22.05.2020).***

***

«В четверг, 21 мая, компания Sophos опубликовала новые сведения о серии кибератак на свои межсетевые экраны XG.

Напомним, в прошлом месяце стало известно об эксплуатации уязвимости нулевого дня в межсетевых экранах Sophos XG. По словам исследователей, узнав об инциденте, производитель выпустил экстренные обновления безопасности, и атакующие быстро изменили свою тактику, заменив первоначальную полезную нагрузку, инфостилер, вымогательским ПО. Как обнаружили исследователи, межсетевые экраны, на которых установлено исправление, блокировали последующие попытки установки вымогательского ПО.

Первоначальные попытки кибератак были предприняты 22-26 апреля. Злоумышленники проэксплуатировали уязвимость (CVE-2020-12271) в межсетевых экранах Sophos XG, позволяющую осуществить SQL-инъекции. Атакующие нацелились на встроенный сервер PostgreSQL и установили на устройство вредоносное ПО.

Как сообщают специалисты Sophos, первоначальной полезной нагрузкой был троян Asnarök, собирающий имена и пароли для доступа к межсетевому экрану Sophos. Кроме того, атакующие оставляли два файла, играющие роль бэкдоров, обеспечивающие им контроль над устройствами.

Производитель быстро выпустил экстренное обновление, автоматически разосланное не все уязвимые устройства, и злоумышленники были вынуждены изменить свою тактику. Новая атака включает следующие этапы:

EternalBlue – эксплоит для уязвимости в Windows SMB для инфицирования внутренних сетей, защищенных межсетевым экраном;

DoublePulsar – имплант для ядра Windows, предоставляющий доступ к компьютерам во внутренней сети;

Ragnarok – вымогательское ПО.

По словам исследователей, новая тактика не срабатывает. Выпущенное Sophos экстренное обновление удаляет все следы вредоносных программ, в том числе двух бэкдоров, и в итоге финальная вредоносная нагрузка (вымогательское ПО) не устанавливается». ***(Хакеры пытались установить вымогательское ПО через уязвимость в Sophos XG // SecurityLab.ru (https://www.securitylab.ru/news/508559.php). 22.05.2020).***

***

«Израильский разработчик шпионского ПО NSO Group управлял web-доменом, замаскированным под сайт команды безопасности Facebook, чтобы обманом заставить пользователей нажимать на вредоносные ссылки и устанавливать ПО для взлома сотовых телефонов.

Бывший сотрудник NSO Group предоставил изданию Motherboard IP-адрес сервера, который использовался для заражения телефонов с помощью вредоносного ПО Pegasus. Оказавшись на зараженном устройстве, Pegasus способен собирать учетные данные для доступа к облачным сервисам Google Диск, Facebook Messenger и iCloud. Шпионская программа может проводить все операции без «инициирования двухфакторной аутентификации или отображения уведомления о несанкционированном доступе».

Как сообщило издание, данный IP-адрес в течение 2015 и 2016 годов был связан с 10 доменами. Некоторые из них были созданы так, чтобы казаться

безобидными для пользователя. Например, замаскированы под ресурсы, якобы позволяющие отписаться от рассылки электронных писем или текстовых сообщений. Другие домены выдавали себя за сайт команды безопасности Facebook и ресурсы по отслеживанию посылок от FedEx.

В конце 2016 года компания MarkMonitor, занимающаяся поиском вредоносных доменов, приобрела замаскированный под Facebook сайт и через два месяца передала управление компании Facebook, чтобы злоумышленники не могли злоупотреблять им». ***(Разработчик шпионского ПО маскировался под Facebook для помощи клиентам // SecurityLab.ru (https://www.securitylab.ru/news/508537.php). 21.05.2020).***

***

«Министерство обороны Японии начало расследование предположительной утечки данных, которая могла произойти в прошлом году в результате масштабной кибератаки на компанию Mitsubishi Electric Corp. Как сообщило японское издание Asahi Shimbun, злоумышленники могли получить доступ к информации, касающейся разработки гиперзвуковых ракет.

По словам представителей компании, кибератака была осуществлена с целью промышленного шпионажа. Данные ракеты предназначены для точных ударов по целям после уклонения от противоракетной обороны противника. Ракеты предназначены для полета не только на невероятно высоких скоростях, но и по различным траекториям. Спецификации, вероятно, включали такую информацию, как дальность полета ракеты, требуемый уровень теплостойкости и тяги.

Министерство обороны Японии начало собственную разработку ракет в 2018 году, и Японское агентство по закупкам, технологиям и логистике (ATLA) предоставило оборонным компаниям спецификации вооружений в рамках тендера на разработку проекта, в том числе Mitsubishi Electric.

По результатам расследования Mitsubishi Electric, преступники проникли в сеть компании, воспользовавшись уязвимостями в программном обеспечении компьютерных систем, а также оборудования связи дочерних компаний в Китае.

В организации кибератаки подозреваются преступные группировки Black Tech и Tick. По словам представителей Министерства обороны, Национального полицейского управления и комиссий по общественной безопасности, группировки находятся под контролем китайских военных, поскольку Black Tech имеет тесные связи с военным подразделением, базирующимся в Ухане, а Tick сотрудничает с подразделением в Шанхае». ***(Кибератака на Mitsubishi Electric могла привести к утечке данных о сверхзвуковой ракете // SecurityLab.ru (https://www.securitylab.ru/news/508512.php). 20.05.2020).***

***

«Неизвестные злоумышленники атаковали узел авторизации одного из мощнейших суперкомпьютеров Великобритании ARCHER. Согласно уведомлению системных администраторов, SSH-ключи пользователей могли быть скомпрометированы в результате кибератаки, поэтому рекомендуется сменить

пароли и SSH-ключи для ARCHER, если они также используются для авторизации на других ресурсах.

По словам системных администраторов, помимо ARCHER злоумышленники атаковали целый ряд высокопроизводительных научных компьютеров по всей Европе. В настоящее время проводится расследование инцидента при участии Национального центра кибербезопасности Великобритании (National Cyber Security Centre, NCSC) при Центре правительственной связи.

Как сообщил источник издания The Register, сервисом ARCHER пользуются специалисты в области вычислительной биологии, в том числе для моделирования дальнейшего распространения коронавируса, и вражеские государства могли осуществить атаку с целью похитить результаты исследований или вовсе сорвать их.

ARCHER представляет собой суперкомпьютер Cray XC30, оснащенный 118 080 процессорами Intel Xeon E5. В этом месяце он должен был быть списан и заменен новым компьютером ARCHER2, но в связи с пандемией COVID-19 списание пришлось отложить. ARCHER расположен в Эдинбургском университете и занимает 334-е место в топ-500 мощнейших суперкомпьютеров в мире…». ***(Злоумышленники атаковали суперкомпьютер ARCHER // SecurityLab.ru (https://www.securitylab.ru/news/508313.php). 14.05.2020).***

***

«В прошлом году из-за вредоносного ПО немецкий машиностроительный концерн Rheinmetall Automotive некоторое время терял по $4 млн в неделю. Инцидент является ярким примером того, как вредоносное ПО может сорвать производство, однако многие владельцы промышленных предприятий по-прежнему относятся к киберугрозам как к чему-то абстрактному и не верят, что нечто-подобное может произойти и с ними.

Главный исследователь ИБ-компании Trend Micro Федерико Магги (Federico Maggi) решил опровергнуть это заблуждение и совместно с коллегами представил 60-страничное исследование с описанием различных методов атак на производственные предприятия. Целью работы было доказать, что причиной атаки не обязательно является какая-либо одна уязвимость или система – для заражения сетей предприятия вредоносным ПО смекалистый хакер может воспользоваться множеством различных способов.

В частности, исследователи представили атаку на оборудование, используемое для сверления отверстий в игрушечных телефонах. Они показали, как с помощью атаки на цепочку поставок можно повлиять на систему контроля температуры и вызвать аварийный режим. Для заражения производственного оборудования вредоносным ПО исследователи использовали библиотеки.

Магги начал с популярного магазина приложений от швейцарского техногиганта ABB, куда инженеры загружают коды для промышленных роботов. Исследователь обнаружил в нем уязвимость (в настоящее время проблема уже исправлена), позволившую ему загрузить собственный код. Как только код был установлен на инженерную рабочую станцию, Магги смог собрать нужные данные

о ней. Поскольку песочница отсутствовала, исследователь мог просматривать и похищать файлы с помощью простого плагина.

Магги также использовал «цифрового близнеца» - оцифрованную копию заводского оборудования или процесса, применяемую на производстве для проверки производительности. Исследователь обнаружил уязвимость в ПО для управления «цифровым близнецом» и показал, как злоумышленник может манипулировать кодом. Теоретически, злоумышленник может заставить оборудование производить продукцию по некорректным инженерным проектам.

Отчет исследователей содержит несколько рекомендаций по безопасности для смягчения атак, включая проверку программного обеспечения рабочих станций. Однако для защиты от некоторых представленных в нем атак на цепочки поставок потребуется довольно много времени». ***(Представлена атака на завод через магазин приложений // SecurityLab.ru (https://www.securitylab.ru/news/508296.php). 13.05.2020).***

***

«Использование пиратских интернет-ресурсов для просмотра и скачивания фильмов несет опасность заражения компьютера вредоносной программой, а также потерей персональных данных, следует из сообщения Роскачества.

«Загружая данные из такого источника, вы рискуете заразить свой компьютер вредоносной программой. Это может привести к тому, что киберпреступники завладеют вашими персональным данными, документами, личными переписками и многим другим сокровенным», – передает РИА «Новости» сообщение организации.

Роскачество отмечает, что пиратскими принято называть сайты, где предоставляется возможность бесплатно посмотреть или скачать фильм или сериал, а скачивание нелицензионного контента нередко осуществляется с помощью торрент-трекеров.

Эксперты предупреждают, что киберпираты могут получить возможность следить за пользователем через микрофон или веб-камеру, выполнять от его имени действия в интернете, в том числе в мошеннических целях. Также любой неосторожный клик по рекламе на пиратском онлайн-кинотеатре может привести к загрузке вредоносного программного обеспечения или переходу на зловредный сайт.

«Еще одной старой уловкой является уведомление о необходимости обновить Flash Player, без которого якобы посмотреть фильм не удастся, но пользователь при этом скачивает самый настоящий вирус, который впоследствии может использовать его компьютер как марионетку, бота для атак», – говорится в сообщении.

Роскачество отмечает, что судебная практика приравнивает торрент-файлы к нарушениям авторского права, и скачивание и хранение на компьютере нелегального контента может повлечь за собой ответственность гражданина.

«В случае с физическими лицами в РФ случаи привлечения к ответственности за скачивание нелегальных файлов на личный компьютер практически отсутствуют (в отличие от случаев использования пиратского ПО в

компаниях), но необходимо четко понимать, что любое хранение заведомо пиратского контента – нелегально», – предупреждают эксперты…». ***(Дмитрий Зубарев. Роскачество предупредило об опасности пиратских сайтов // Деловая газета «Взгляд» (https://vz.ru/news/2020/5/22/1040763.html). 22.05.2020).***

***

«Сегодня команда исследователей кибербезопасности Check Point Research опубликовала результаты исследования Global Threat Index за апрель 2020 года. Исследователи отмечают несколько спам-кампаний, связанных с коронавирусом (COVID-19), которые распространяют новый вариант трояна Agent Tesla: всего он затрагивает 3% организаций во всем мире.

Новый вариант Agent Tesla был модифицирован для кражи паролей Wi-Fi. Также троян умеет получать учетные данные электронной почты из клиента Outlook с целевых ПК. В течение апреля Agent Tesla был распространенным вложением в нескольких вредоносных кампаниях, связанных с COVID-19. Подобные спам-рассылки пытаются заинтересовать жертву якобы важной информацией о пандемии, чтобы она загрузила вредоносные файлы. Одна из этих кампаний была разослана якобы от Всемирной организации здравоохранения с темами: URGENT INFORMATION LETTER: FIRST HUMAN COVID19 VACCINETEST/RESULT UPDATE — «СРОЧНОЕ ОПОВЕЩЕНИЕ: ПЕРВОЕ ТЕСТИРОВАНИЕ ВАКЦИНЫ ОТ COVID-19 НА ЧЕЛОВЕКЕ / РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ». Это еще раз подчеркивает, что хакеры используют последние события в миру и страх населения, чтобы повысить эффективность своих атак.

«Спам-кампании с Agent Tesla, которые мы наблюдали весь апрель, показывают, насколько хорошо злоумышленники подстраиваются под информационную повестку, и как спокойно обманывают ничего не подозревающих жертв. Преступники сосредоточены на организации фишинговых атак для кражи личных и корпоративных данных пользователей. Поэтому для любой организации очень важно регулярно обучать своих сотрудников, регулярно информируя их о новейших инструментах и методах преступников. Сейчас это особенно актуально, так как большая часть компаний перевели своих сотрудников на удаленный режим», — рассказывает Василий Дягилев, глава представительства Check Point Software Technologies в СНГ.

Самое активное вредоносное ПО в мире в апреле

В этом месяце Dridex затронул 4% организаций во всем мире, XMRig и Agent Tesla — 4% и 3% соответственно.

Dridex— банковский троян, поражающий ОС Windows. Dridex распространяется с помощью спам-рассылок и наборов эксплойтов, которые используют WebInjects для перехвата персональных данных, а также данных банковских карт пользователей.

XMRig— программное обеспечение с открытым исходным кодом, впервые обнаруженное в мае 2017 года. Используется для майнинга криптовалюты Monero.

Agent Tesla— усовершенствованная RAT. AgentTesla заражает компьютеры с 2014 года, выполняя функции кейлоггера и похитителя паролей. Вредоносная программа способна отслеживать и собирать вводимые данные с клавиатуры

жертвы, делать скриншоты и извлекать учетные данные, относящиеся к различным программам, установленным на компьютер жертвы (включая Google Chrome, Mozilla Firefox и Microsoft Outlook).

Самые распространенные уязвимости апреля 2020

В апреле «Удаленное выполнение кода MVPower DVR» было самой распространенной уязвимостью, которая затронула 46% организаций во всем мире. На втором и третьем месте соответственно — OpenSSL TLS DTLS Heartbeat Information Disclosure (затронула 41% организаций) и Удаленное внедрение команд по протоколу HTTP – 40% организаций во всем мире.

Удаленное выполнение кода MVPower DVR. В устройствах MVPower DVR существует уязвимость удаленного выполнения кода. Злоумышленник может использовать эту уязвимость для выполнения произвольного кода в уязвимом маршрутизаторе с помощью специально созданного запроса.

OpenSSL TLS DTLS Heartbeat Information Disclosure (CVE-2014-0160; CVE-2014-0346). В OpenSSL существует уязвимость, позволяющая раскрыть содержимое памяти на сервере или на подключенном клиенте. Уязвимость связана с ошибкой при обработке пакетов Heartbeat TLS / DTLS.

Удаленное внедрение команд по протоколу HTTP. Злоумышленники удаленно используют эту уязвимость, отправляя жертве специальный запрос. Успешная эксплуатация позволит злоумышленнику выполнить произвольный код на устройстве жертвы.

Самые активные мобильные угрозы апреля 2020

xHelper — вредоносное приложение для Android, активно с марта 2019 года, используется для загрузки других вредоносных приложений и отображения рекламы. Приложение способно скрывать себя от пользовательских и мобильных антивирусных программ и переустанавливать себя, если пользователь удаляет его.

Lotoor — программа использует уязвимости в операционной системе Android, чтобы получить привилегированный root-доступ на взломанных мобильных устройствах.

AndroidBauts— рекламное ПО, предназначенное для пользователей Android, которое фильтрует IMEI, IMSI, местоположение GPS и другую информацию об устройстве и позволяет устанавливать сторонние приложения на мобильные устройства.

Полный список топ-10 семейств вредоносных программ за апрель можно найти в блоге Check Point». ***(В рассылках на тему COVID распространяется троян для кражи паролей // IGate (https://igate.com.ua/news/24522-v-rassylkah-na-temu-covid-rasprostranyaetsya-troyan-dlya-krazhi-parolej). 26.05.2020).***

***

«В Японии в результате хакерской атаки на крупнейшего телекоммуникационного оператора страны NTT Communications могла произойти утечка оборонных данных. Речь идет об информация, связанной с коммуникациями, которые используют японские Силы самообороны. Об этом сообщает агентство Kyodo.

В настоящее время министерство обороны страны совместно с NTT Comunication ведет расследование обстоятельств случившегося.

По данным агентства, информация, которая могла быть похищена, включает в себя данные о коммуникационном оборудовании, а также чертежи и планы японских военных объектов, включая военно-морскую базу Йокосука.

В общей сложности хакеры получили несанкционированный доступ более чем к 100 файлам.

В то же время подчеркивается, что похищенные документы не носили статуса «секретных». Однако, как отмечается, каналы связи между министерством обороны и Силами самообороны страны могут оказаться под угрозой.

Также NTT Communications заявила, что из-за несанкционированного доступа к ее сети могла быть похищена информация о 621 клиентских компаніях». ***(Власти Японии подозревают утечку оборонных данных из-за кібератаки // ООО «Медиахолдинг «Репортер» (https://reporter-ua.com/2020/05/29/360501_vlasti-yaponii-podozrevayut-utechku-oboronnyh-dannyh-iz-za-kiberataki). 29.05.2020).***

***

«Check Point опубликовала результаты расследования киберинцидента, связанного с хищением 1,1 млн фунтов. 16 декабря 2019 г. в службу реагирования на инциденты Check Point's Incident Response Team (CPIRT) обратились сразу три финансовые компании, попросив провести расследование ряда случаев утечки средств с совместного банковского счета. Оказалось, что злоумышленники при помощи четырех транзакций попытались вывести на сторонние счета сумму в размере 1,1 млн фунтов стерлингов. Из них удалось вернуть только 570 тыс. фунтов.

Ранее группа CPIRT исследовала похожий случай. Хакерам удалось похитить $1 млн со счета китайской венчурной компании, которые предназначались для израильского стартапа.

В своем исследовании специалисты раскрывают историю группы киберпреступников, которой дали название «Флорентийский банкир». Исследователи рассказывают, как происходят такие типы атак как Business Email Compromise (BEC), как злоумышленники наблюдают за своими жертвами в течение нескольких месяцев, как они постепенно переводят сотни тысяч долларов из ничего не подозревающих организаций в свои карманы.

Целью группировки стали четыре крупные компании финансового сектора из Великобритании и Израиля. Эти компании еженедельно проводят значительные суммы денег новым партнерам и сторонним организациям. Кроме того, все они используют почтовый сервис Office 365.

В качестве метода атаки мошенники выбрали таргетированную фишинговую рассылку. Письма приходили топ-менеджерам компаний — генеральным или финансовым директорам — которые отвечали за денежные операции.

В этом случае злоумышленники выбрали двух сотрудников для отправки им фишинговых писем, один из которых предоставил необходимые данные. Одна фишинговая кампания может длиться неделями или месяцами, пока мошенники не

получат полное представление о всей финансовой активности компаний. Для успешной реализации злоумышленники используют различные тактики, чередуют методы и меняют списки получателей.

С помощью фишинговой рассылки мошенники получали доступ к учетной записи электронной почты жертвы, чтобы получить информацию: какие каналы жертва использует для осуществления денежных переводов; какие отношения связывают жертву с третьими лицами — клиентами, адвокатами, бухгалтерами и банками; какие сотрудники в компании занимают ключевые позиции.

Группировка «Флорентийский банкир» может провести дни, недели или даже месяцы, занимаясь разведкой и терпеливо конспектируя бизнес-схемы и процессы.

После тщательного изучения внутриорганизационных процессов мошенники начинали изолировать жертву от коммуникации как с третьими лицами, так и с коллегами, создавая определенные правила для почтового ящика. Эти правила направляют любые электронные письма с интересующими хакеров данными в папку, за которой они следят, реализуя тип атаки «Человек посередине». Так, например, если в письмах упоминались такие слова, как «счет-фактура», «возвращено» или «отказано», они перемещались в папку, которая не используется жертвой.

Следующий шаг злоумышленников — создание фальшивых доменов, которые визуально практически идентичны доменам партнёров и третьих лиц, с которыми жертва ведет коммуникацию по почте. После этого, мошенники рассылали жертвам письма с фальшивых доменов, продолжая либо уже существующую переписку, либо создавая новую. Например, если коммуникация проходит между доменами finance-firm.com и banking-service.com хакеры могут использовать очень похожие на них вариации finance-firms.com и banking-services.com. Злоумышленники начинают отправлять электронные письма, для чего, либо создают новую ветку писем, либо продолжают диалог в прежней. Таким образом им удается обмануть жертву, которая предполагает, что по-прежнему общается с легитимным представителем компании.

Получив высокий уровень контроля над почтой, мошенники начинают отправлять жертвам ложные банковские реквизиты, применяя следующие техники: перехват актуальных переводов. Хакеры узнают из писем о том, что планируется перевод денег. Используя информацию и инфраструктуру, подготовленную на третьем этапе, мошенники предоставляют «новые» реквизиты, тем самым направляя средства на свои собственные банковские счета. Так, группировка «Флорентийский банкир» выяснила, что в одной из сделок, третья сторона предложила использовать банковский счет в Великобритании для ускорения процесса, однако получающая сторона сообщила, что у них такой возможности нет. Перехватив письмо жертвы, мошенники воспользовались ситуацией и предоставили стороне-отправителю альтернативный счет в банке Великобритании со своими реквизитами; генерация новых запросов на банковский перевод. Изучив на этапе разведки всю цепочку реализации денежного перевода, злоумышленники узнают процедуру, цикл согласования, ключевых игроков скомпрометированной компании и банков, которые проводят транзакции; В этом случае мошенники просмотрели почтовую переписку между организацией и банком, с помощью

которого она переводит деньги. Используя эту информацию, группа хакеров связалась с сотрудником компании, который отвечает за взаимодействие с банком, и оповестила об изменении процедуры перевода денег.

Группа «Флорентийский банкир» ведет беседу, пока третье лицо не утвердит новые банковские реквизиты и не подтвердит транзакцию. Если банк отклоняет транзакцию из-за несоответствия в валюте счета, имени получателя или по любой другой причине, злоумышленники исправляют отклонения, пока деньги не попадут в их собственные руки.

Так произошла и в этот раз. Злоумышленники следили за перепиской с банковским контактом, вносили необходимые исправления и сумели заставить стороны совершить транзакцию на свой мошеннический счет. В ходе этой атаки группе хакеров удалось перехватить три операции и безвозвратно перевести себе 600 тыс. фунтов стерлингов.

В ходе расследования случая Флорентийских банкиров, командой Check Point была собрана криминалистическая информация и проведено наблюдение различных доменов, вовлеченных в эту операцию. В общей сложности мошенники использовали семь различных доменов. Некоторые из них были имитацией существующих, другие были созданы с использованием сайта для обслуживания фишинговых страниц.

Используя информацию WHOIS сервиса (регистрация доменного имени, email, номер телефона), исследователи Check Point обнаружили еще 39 доменов, зарегистрированных в период с 2018-2020 г. Очевидно, что эти домены также были созданы для проведения подобного рода атак, а значит, у хакеров были планы и на другие компании.

В ходе расследования были обнаружены улики, которые могут помочь определить местонахождение группировки: все письма и транзакции, перехваченные мошенниками, были на английском языке; в течение двух месяцев, которые хакеры провели в среде компании-жертвы, они работали с понедельника по пятницу; банковские счета мошенников находились в Гонконге и Англии; некоторые электронные письма на иврите содержали потенциально полезные сведения, которые не были использованы злоумышленниками. Это позволяет сделать вывод, что они не владеют данным языком; для осуществления банковских переводов было использовано имя одной из гонконгских компании, которая была либо поддельной, либо ранее зарегистрированной, но не действующей.

Частный акционерный капитал и венчурный капитал стали прибыльной мишенью для BEC-афер. Венчурные инвесторы часто осуществляют переводы больших денежных сумм новым партнерам, что привлекает мошенников.

Группа «Флорентийский банкир», похоже, уже успела отточить навыки на нескольких атаках на протяжении, как минимум, нескольких лет. Злоумышленники доказали свою находчивость, быстро адаптируясь к новым ситуациям.

Методы, которые использовала группировка «Флорентийский банкир», особенно техника двойных доменов, представляют серьезную угрозу не только для скомпрометированной компании, но и для ее партнеров. Даже после обнаружения и удаления хакеров из сети компании-жертвы злоумышленники могут продолжить использовать организации партнеров, клиентов или банков жертвы в своих целях.

Корпоративная электронная почта является ключевой целью для дальнейшего проникновения мошенников в сеть организации. Фишинговые электронные письма, которые побуждают сотрудников раскрыть учетные данные своей организации или кликнуть по вредоносной ссылке или файлу, могут нанести огромный ущерб компании. Для обеспечения безопасности организациям Check Point советует использовать решения, предотвращающие угрозу фишинга, регулярно информировать сотрудников о методах хакерских атак и правилах поведения в сети. При осуществлении транзакции рекомендуется позвонить и убедиться, действительно ли отправитель запрашивает перевод средств. При обнаружении мошеннической атаки, уведомите об этом всех своих партеров. Любое промедление может сыграть на руку хакерам». ***(Check Point расследовала киберинцидент, связанный с хищением более 1 млн фунтов // Компьютерное Обозрение(https://ko.com.ua/check_point_rassledovala_kiberincident_svyazannyj_s_hishheniem_bolee_1_mln_funtov_133107). 22.05.2020).***

***

«Компания Trend Micro Incorporated опубликовала доклад Shifts in Underground Markets: Past, Present, and Future («Динамика изменений подпольных рынков: прошлое, настоящее и будущее»), в котором приводятся данные о киберпреступных операциях и схемах купли-продажи товаров и услуг среди киберкриминальных группировок.

«В этом докладе подробно освещается информация об угрозах, исходящих от глобальных киберпреступных сетей, которую мы собираем и анализируем, что позволяет нам предупреждать, подготавливать и обеспечивать защиту наших корпоративных клиентов и партнёров, — заявил Эд Кабрера (Ed Cabrera), директор по вопросам кибербезопасности в Trend Micro. — Это исследование помогает нам заблаговременно информировать компании и организации о таких возникающих угрозах, как заражение машин программами-вымогателями с поддержкой сервисов синтеза изображений (Deepfake), боты на основе искусственного интеллекта, предоставление доступа в качестве услуги (Access-as-a-Service) и высоконаправленная подмена SIM-карт. Многоуровневый подход к таким угрозам с учётом имеющихся рисков является жизненно важным механизмом минимизации опасностей, связанных с этими и другими набирающими популярность инструментами киберпреступников».

В докладе говорится также, что предпринимаемые решительные усилия правоохранительных органов, по-видимому, оказывают существенное влияние на киберпреступные группировки. Несколько форумов были закрыты по решению правоохранительных структур глобального уровня, в то время, как на остальных форумах наблюдаются проблемы с входом в систему и на них постоянно ведутся DDoS-атаки, что влияет на степень полезности подобных ресурсов.

Потеря доверия привела к созданию нового сайта под названием DarkNet Trust, который предназначен для проверки поставщиков и повышения анонимности пользователей. На других подпольных рынках были введены новые меры безопасности, в частности, платежи напрямую от покупателя к поставщику,

многоуровневая политика идентификации при совершении сделок с криптовалютой, шифрование сообщений и запрет на JavaScript.

Помимо этого, в докладе Trend Micro раскрываются изменения рыночных тенденций в отношении товаров и услуг киберпреступников с 2015 года. Коммерциализация привела к снижению цен на большинство товаров. К примеру, стоимость услуг шифрования упала с 1000 долларов США в месяц до 20 долларов, в то время как стоимость универсальных ботнетов упала с 200 до 5 долларов в день. Цены на другие товары, включая программы-вымогатели, трояны удалённого доступа (RAT), учётные данные онлайн-аккаунтов и спам-сервисы, оставались стабильными, что свидетельствует о сохраняющемся спросе на подобного рода продукты.

Тем не менее, исследование специалистов Trend Micro наглядно показало высокий спрос на другие услуги, такие как ботнеты, образованные устройствами интернета вещей с новыми не обнаруживаемыми вариантами вредоносного ПО — они продаются за 5000 долларов. Также особой популярностью пользуются фальшивые новости и услуги киберпропаганды, где базы данных избирателей продаются за сотни долларов, а аккаунты игроков в такие игры, как Fortnite, могут принести в среднем около 1000 долларов.

К числу представляющих значимость выводов исследования можно отнести и появление рынков для:

- сервисов с поддержкой синтеза изображений (Deepfake), используемых для шантажа посредством разоблачения частной жизни интимного характера или обхода требований проверки фотографий на некоторых сайтах;
- игровых ботов на основе искусственного интеллекта, предназначенных для прогнозирования схем бросков костей и комплексного взлома Roblox CAPTCHA;
- предоставления доступа как услуги к взломанным устройствам и корпоративным сетям — стоимость для компаний из списка Fortune 500 может достигать 10 000 долларов США, и некоторые такие сервисы включают предоставление доступа с правами чтения и записи;
- учётных записей пользователей носимых устройств, доступ к которым может позволить киберпреступникам реализовывать мошеннические схемы с гарантией на устройства посредством направления владельцам фальшивых запросов на их замену.

Тенденции в киберпреступном подполье, вероятно, продолжат изменяться в течение нескольких месяцев после окончания пандемии COVID-19 в мире, поскольку возможности для атак продолжают развиваться. Для защиты от постоянно меняющейся картины угроз специалисты Trend Micro рекомендуют применять многоуровневый подход к защите от угроз новейшего типа и снижению рисков корпоративной безопасности». ***(Выявлено отсутствие доверия в киберпреступном подполье // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5666874-Vyyavleno-otsutstvie-doveriya-v-kib.html). 29.05.2020).***

***

«По данным Check Point Software, 27% компаний во всем мире столкнулись с атаками на мобильные устройства сотрудников ––– это демонстрирует явную тенденцию к росту атак шестого поколения.

По данным Check Point, в настоящее время мы являемся свидетелями эпидемии мобильного рекламного ПО — одной из наиболее распространенных форм киберугроз, нацеленной на сбор личной информации с устройства пользователя. Примерно 4 миллиарда человек заходят в интернет со смартфона. Тем не менее, компании редко заботятся о безопасности мобильных устройств сотрудников. Отчет кибербезопасности Check Point за 2020 год показывает, что в 2019 году 27% компаний подверглись кибератакам из-за того, что смартфоны не были достаточно защищены.

«Для кражи конфиденциальных данных и доступа к корпоративной сети организации нужно всего одно взломанное мобильное устройство, — рассказывает Василий Дягилев, глава представительства Check Point Software Technologies в России и СНГ. — С каждым днем создается все больше и больше усовершенствованных мобильных угроз. Мобильное рекламное ПО, одна из разновидностей вредоносных программ, которая постоянно показывает рекламные сообщения на смартфоне и используется киберпреступниками для проведения кибератак шестого поколения».

Откуда приходит мобильное вредоносное ПО

Основная проблема с рекламным ПО — понять, как и где заразился смартфон. Рекламное программное обеспечение разработано так, чтобы проникнуть на устройство незамеченным. Удаление этого подобных вирусных программ может быть чрезвычайно сложным. При этом собираемая ими информация, например, данные об операционной системе устройства, геолокация, файлы и прочее, может представлять серьезную угрозу безопасности.

Рекламное ПО, как правило, распространяется через мобильные приложения — например, как дополнительная нагрузка. По данным Statista, для пользователей Android в Google Play доступно 2,5 миллиона приложений, в Apple Store — 1,8 миллиона приложений. Из этих цифр видно, что у подобных атак есть много возможностей — а значит, киберпреступники продолжат фокусироваться на мобильных устройствах.

В качестве одного из примеров нового мобильного рекламного ПО можно привести вредоносную программу Agent Smith, которую в прошлом году обнаружили исследователи Check Point. Тогда Agent Smith заразил около 25 миллионов мобильных устройств по всему миру, при этом пользователи даже не заметили этого. Программа имитировала приложение Google и использовала все известные уязвимости в системе Android, автоматически заменяя установленные приложения версиями, содержащими вредоносный код. Agent Smith также использовал ресурсы устройств, отображая фейковую рекламу, которая могла красть банковские учетные данные и прослушивать разговоры». ***(Мобильное рекламное ПО: чума среди вредоносных программ // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5665281-Mobilnoe-reklamnoe-PO-chuma-sredi.html). 22.05.2020).***

***

«Эксперты Kaspersky ICS CERT обнаружили серию таргетированных атак на организации, расположенные в различных странах мира. На начало мая 2020 года известны случаи атак на системы в Японии, Италии, Германии и Великобритании. Среди жертв атак были, в том числе, поставщики оборудования и программного обеспечения для промышленных предприятий.

В качестве начального вектора атаки злоумышленники используют фишинговые письма с текстом, написанным на целевом для каждой конкретной жертвы языке. Причем малварь, используемая в этой атаке, выполняет деструктивную активность только в том случае, если операционная система имеет локализацию, соответствующую языку, использованному в фишинговом письме. Например, в случае атаки на компанию из Японии текст фишингового письма и документ Microsoft Office, содержащий вредоносный макрос, написаны на японском, а для успешной расшифровки модуля вредоноса ОС должна иметь японскую локализацию.

Исследователи сообщают, что злоумышленники применяют утилиту Mimikatz для кражи аутентификационных данных, находящихся на зараженной системе, и развития атаки внутри сети предприятия, однако конечная цель преступников пока остается неизвестной, и расследование продолжается.

Интересно, что макросы из упомянутых вредоносных документов расшифровывают и запускают PowerShell скрипт (HEUR:Trojan.PowerShell.Generic), который случайно выбирает один из записанных в нем URL-адресов, ведущих на публичные хостинги изображений (imgur.com и imgbox.com). Оттуда скачивается изображение, расположенное по ссылке, и начинается процедуру извлечения данных.

Данные сокрыты в изображении при помощи методов стеганографии и извлекаются малварью из пикселей, номера которых заданы алгоритмом. Использование стеганографии позволяет злоумышленникам обойти некоторые средства защиты, в частности, сканеры сетевого трафика.

Извлеченные из картинки данные последовательно закодированы алгоритмом Base64, зашифрованы алгоритмом RSA и снова закодированы Base64. Аналитики отмечают, что в качестве ключа расшифровки используется текст исключения (exception), и для этого код скрипта намеренно содержит ошибку. При этом текст исключения будет зависеть от локализации операционной системы – по всей видимости, вредоносный скрипт в каждой конкретной атаке готовится злоумышленниками для жертв из определенной страны.

Расшифрованные и раскодированные данные представляют собой еще один PowerShell-скрипт, который запускается на выполнение. Он тоже декодирует часть своего содержимого при помощи Base64, после чего распаковывает полученный буфер с данными при помощи алгоритма Deflate. В результате вредоносная программа получает еще один PowerShell скрипт – обфусцированный экземпляр вредоносной программы Trojan-PSW.PowerShell.Mimikatz.

Как уже было сказано выше, утилита Mimikatz и ее аналоги используются злоумышленниками для кражи аутентификационных данных учетных записей Windows, сохраненных на скомпрометированной системе. Эти сведения могут быть

использованы для получения доступа к другим системам внутри сети предприятия и развития атаки. Особенно опасной ситуацией является попадание в руки злоумышленников данных учетных записей, имеющих права доменного администратора.

Эксперт резюмируют, что применение описанных методик, а также точечный характер заражений говорят о таргетированной направленности атак. Вызывает беспокойство специалистов и тот факт, что среди жертв атаки присутствуют подрядчики промышленных предприятий. Если аутентификационные данные сотрудников организации-подрядчика попадут в руки злоумышленников, это может привести ко многим негативным последствиям, начиная с кражи конфиденциальных данных, заканчивая атаками на промышленные предприятия через средства удаленного администрирования, используемые підрядчиком». ***(Мария Нефёдова. Промышленные предприятия подвергаются атакам с использованием стеганографии // Хакер (https://xakep.ru/2020/05/29/steganography-targeted-attacks/). 29.05.2020).***

***

Діяльність хакерів та хакерські угруповування

«Киберпреступная группировка пыталась скомпрометировать серверы Всемирной Организации Здравоохранения с помощью вредоносных писем, отправленных якобы от имени Британской вещательной корпорации и Американского совета по внешней политике (American Foreign Policy Council, AFPC), сообщило информагентство Bloomberg.

…атаки начались 3 апреля нынешнего года и имели целью кражу паролей и кодов двухфакторной аутентификации к учетным записям сотрудников ВОЗ для последующего заражения вредоносным ПО серверов организации. Фишинговые письма содержали укороченную ссылку Google, ведущую на вредоносный домен.

По мнению специалиста компании Clearsky Cyber Security Охада Зайденберга (Ohad Zaidenberg), кибератаки могут быть делом рук иранской APT Charming Kitten, на что указывают используемые в кампании домены mobiles.identifier-services-session[.]site, sgnldp[.]live, а также сервис bitli.pro, которые ранее были замечены в предыдущих атаках группировки.

Директор по информационной безопасности ВОЗ Флавио Аггио (Flavio Aggio) отказался комментировать инциденты, но подтвердил, что организация подверглась «очень умным атакам». По его словам, все попытки взлома оказались безуспешными.

Американский совет по внешней политике - неправительственный аналитический центр при Конгрессе США, основными объектами исследований которого являются Россия и другие страны бывшего СССР, Китай, Евразия и Иран. Совет занимается мониторингом политики этих стран в области ПРО, контроля оружия, энергобезопасности, шпионажа, развития в указанных странах демократии и рыночной экономики». ***(Хакеры атакуют ВОЗ под видом исследователей и***

журналистов // SecurityLab.ru (https://www.securitylab.ru/news/508152.php). 08.05.2020).

***

«Специалисты из компании Check Point обнаружили текущую кампанию по кибершпионажу, нацеленную на правительственные организации в Австралии, Индонезии, Филиппинах, Вьетнаме, Таиланде, Мьянме и Брунее. Как отметили эксперты, китайская киберпреступная группировка Naikon APT оставалась незамеченной в течение как минимум пяти лет и все еще продолжает осуществлять атаки.

Naikon APT, являвшаяся одной из самых активных группировок в Азии до 2015 года, провела серию кибератак в Азиатско-Тихоокеанском регионе. Naikon APT действовала на протяжении последних пяти лет и использовала новый бэкдор под названием Aria-body. Как пояснили исследователи, целью группировки является сбор разведданных и шпионаж за правительствами целевых стран.

RAT Aria-body способен создавать и удалять файлы и каталоги, делать скриншоты, выполнять поиск файлов, собирать метаданные файлов, информацию о системе и местоположении. Некоторые последние версии Aria-body также оснащены возможностями для кейлоггинга и загрузки других расширений. Помимо эксфильтрации всех собранных данных на C&C-сервер, бэкдор способен выполнять и другие команды.

«Это включает в себя не только обнаружение и кражу определенных документов с зараженных компьютеров и сетей внутри правительственных учреждений, но также извлечение съемных дисков с данными, создание скриншотов, кейлоггинг, и сбор хищение данных», — пояснили эксперты.

В качестве начального вектора атаки Naikon APT отправляет электронные письма с вредоносными вложениями в правительственные учреждения высшего уровня, а также гражданские и военные организации. Письма после открытия устанавливали шпионское ПО, которое отправляло конфиденциальные данные на C&C-серверы.

В ходе одной из последних атак преступники из Naikon APT выдавали себя за представителей иностранного правительства. Злоумышленники загружали на системы жертвы бэкдор Aria-body, а вредоносные электронные письма содержали RTF-файл с компоновщиком эксплойтов под названием RoyalBlood, который устанавливал загрузчик (intel.wll) в системную папку запуска Microsoft Word («% APPDATA%\Microsoft\Word\STARTUP»).

Эксперты отметили, что тактика с использованием RoyalBlood также применялась группировкой Vicious Panda в ходе кампании против правительственных учреждений Монголии». ***(Naikon APT на протяжении пяти лет атакует правительственные организации // SecurityLab.ru (https://www.securitylab.ru/news/508126.php). 07.05.2020).***

***

«Специалисты из компании Bitdefender сообщили о вредоносной кампании по кибершпионажу, организованной киберпреступной

группировкой Chafer APT (также известной как APT39 или Remix Kitten). Преступники ранее атаковали телекоммуникационную и туристическую отрасли на Ближнем Востоке с целью сбора конфиденциальной информации, служащей геополитическим интересам страны. По словам экспертов, некоторые кибератаки датируются 2018 годом.

APT39 атакует свои цели посредством фишинговых писем с вредоносными вложениями и использованием разнообразных бэкдоров с целью повышения привилегий, проведения внутренней разведки и обеспечения персистентности.

В ходе атак на компании и организации в Кувейте преступники создавали учетную запись пользователя на компьютерах жертв и выполняли злонамеренные действия в сети, включая сканирование сети с помощью инструмента CrackMapExec для тестирования окружения Windows/Active Directory, сбор учетных данных авторизованных в системе пользователей с помощью инструмента Mimikatz, и перемещение по сети. Как отметили эксперты, большая часть преступной активности осуществлялась в пятницу и субботу, совпадая с выходными на Ближнем Востоке.

Атака на организации в Саудовской Аравии включала использование социальной инженерии с целью обмануть жертву и запустить инструмент для удаленного доступа (RAT). Один из обнаруженных компонентов, «snmp.exe», также присутствует на системах некоторых жертв в Кувейте под названием «imjpuexa.exe», указывая на связь между данными атаками». ***(Иранская APT атаковала критическую инфраструктуру в Кувейте и Саудовской Аравии // SecurityLab.ru (https://www.securitylab.ru/news/508556.php). 22.05.2020).***

***

«Хакеры-«мстители» решили взять правосудие в свои руки и самостоятельно наказать «мошеннические» компании с помощью вымогательского ПО и DDoS-атак.

На прошлой неделе была обнаружена новая вымогательская программа MilkmanVictory, по словам ее авторов, созданная специально для атак на мошенников. В беседе с BleepingComputer представители киберпреступной группировки CyberWare заявили, что начали атаковать компании, «мошенничающие с кредитами». По их словам, эти компании обещают кредит, но сначала просят внести оплату. Однако после внесения оплаты никакой кредит не выдается.

В ходе атаки киберпреступники отправляют жертве фишинговое письмо с ссылкой на вредоносный исполняемый файл, замаскированный под PDF-документ. Кроме того, они осуществляют DDoS-атаки на сайт компании.

Вымогательское ПО представляет собой вайпер, позволяющий связаться с операторами, но не сохраняющий ключ шифрования. Вместо записки с требованием выкупа MilkmanVictory оставляет сообщение следующего содержания: «Здравствуйте! Этот компьютер был уничтожен с помощью вымогательское ПО MilkmanVictory, поскольку мы знаем, что вы мошенники! Хакеры CyberWare».

«Я не прошу денег, потому что мошенники не заслуживают получать деньги, обманывая невинных людей», - сообщил один из хакеров.

По словам киберпреступников, они атаковали не угодившую им немецкую кредитную компанию Lajunen Loan с помощью DDoS и вымогательского ПО.

Вымогательское ПО MilkmanVictory создано на базе HiddenTear. Другими словами, даже если вымогатель не сохраняет ключи шифрования, файлы все равно можно расшифровать с помощью брутфорса. Жертвы HiddenTear могут расшифровать свои файлы с помощью декриптора от Майкла Гиллеспи (Michael Gillespie)». ***(Хакеры-«мстители» атакуют мошенников // SecurityLab.ru (https://www.securitylab.ru/news/508553.php). 21.05.2020).***

***

«Эксперты компании Check Point установили личность бразильского хакера, известного под псевдонимами VandaTheGod, Vanda de Assis и SH1N1NG4M3.

Активность злоумышленника началась примерно в 2013 году, и он утверждает, что связан с этичной хак-группой Brazilian Cyber Army, а также заявляет, что входил в состав хакерской группы UGNazi, члены которой были арестованы еще в 2012 году.

По данным сайта Zone-H, который агрегирует и сортирует случаи дефейсов, на счету VandaTheGod, за период с июля 2019 года по февраль 2020 года, взлом и порча 4820 ресурсов (в том числе принадлежащих правительственным организациям и корпорациям в 40 странах).

И хотя эти инциденты, судя по оставленным на сайтах сообщениям, были частью хактивистской кампании, направленной на борьбу с коррупцией в правительстве, VandaTheGod также похищал данные и пытался продавать украденную корпоративную информацию и о данные платежных карт. К примеру, в какой-то момент он продавал медицинские записи 1 000 000 пациентов из Новой Зеландии за 200 долларов.

Исследователи Check Point внимательно изучили поведение VandaTheGod в интернете и заметили, что сайт хакера был зарегистрирован в бразильском городе Уберландии. Также на одном из скриншотов, размещенных хакером в Twitter, была видна вкладка браузера, открытая для учетной записи Facebook «Vanda De Assis (VandaTheGod)». Другой скриншот демонстрировал вкладку с инициалами MR и поиск лиц с этими инициалами в Уберландии привел исследователей к профилю в Facebook, владелец которого явно поддерживал деятельность Brazilian Cyber Army.

Дальнейший анализ показал, что одна и та же фотография мужчины, держащего бутылку виски, была размещена как в профиле Vanda de Assis в Facebook, так и в профиле человека с инициалами MR. Более того, мебель и обстановка на другой фотографии, опубликованной MR в Facebook, полностью совпадала с обстановкой на фото, опубликованном VandaTheGod в Twitter.

В своем отчете эксперты Check Point не раскрывают имя хакера, но сообщают, что компания уже предала все собранную информацию в правоохранительные органы.

«VandaTheGod провел множество успешных хакерских атак, но в итоге потерпел неудачу с точки зрения OPSEC, так как оставлял множество следов, особенно в начале своей хакерской “карьеры”, которые и привели нас к его настоящей личности.

В конечном итоге мы смогли связать личность VandaTheGod с конкретным гражданином Бразилии из города Уберландия и передали полученные результаты [расследования] правоохранительным органам, чтобы те могли принять меры», — резюмируют исследователи». ***(Мария Нефёдова. Бразильский хактивист дефейснул около 5000 сайтов // Xakep (https://xakep.ru/2020/05/29/vandathegod/). 29.05.2020).***

***

«Правительство Германии в очередной раз предупредило о киберпреступной группировке Berserk Bear, долгое время атакующей инфраструктуру страны. Как сообщает издание CyberScoop, на прошлой неделе Федеральная разведывательная служба (BND), Федеральная служба защиты конституции (BfV) и Федеральное управление информационной безопасности (BSI) направили операторам критической инфраструктуры уведомление безопасности.

Согласно уведомлению, группировка Berserk Bear атакует предприятия электро- и водоснабжения. Как сообщается в документе, ранее в нынешнем году специалисты обнаружили в сетях одной из неназванных компаний признаки «удаленной компрометации». Для доступа к сетям атакуемых компаний киберпреступники используют атаки на цепочки поставок.

С помощью как общедоступного, так и специально написанного вредоносного ПО злоумышленники укрепляются в атакуемой сети с целью похищения информации или доступа к производственным системам. Никаких следов разрушительного воздействия кибератак обнаружено не было…». ***(Группировка Berserk Bear атакует инфраструктуру Германии // SecurityLab.ru (https://www.securitylab.ru/news/508692.php). 27.05.2020).***

***

«По данным аналитиков Red Canary, недавно обнаруженная хак-группа Blue Mockingbird активна с конца 2019 года и уже взломала тысячи корпоративных систем. Исследователи пишут, что Blue Mockingbird атакует доступные из интернета серверы, на которых работают приложения ASP.NET, использующие уязвимые версии фремворка Telerik.

Против таких серверов хакеры используют уязвимость CVE-2019-18935 и устанавливают на них веб-шеллы. Затем злоумышленники прибегаю к помощи Juicy Potato, чтобы получить привилегии администратора, изменить настройки сервера и обеспечить себе постоянное присутствие в системе. В конечном итоге хакеры устанавливают на взломанные машины майнер XMRRig для добычи криптовалюты Monero (XMR).

Эксперты Red Canary отмечают, что если общедоступные IIS-серверы подключены к внутренней сети компании, хакеры попытаются распространить свою атаку и на внутренние системы, используя слабо защищенные RDP и SMB.

Специалисты признают, что пока у них нет полной картины активности этого ботнета, но они считают, что группировка Blue Mockingbird уже заразила как минимум 1000 систем. Так как этот вывод базируется на тех ограниченных данных, что доступны аналитикам, реальное количество заражений наверняка превышает этот прогноз.

«Как любая ИБ-компания, мы видим лишь ограниченный участок ландшафта угроз, и не можем знать точный масштаб данной угрозы, — пишут в Red Canary. — В частности, эта угроза затронула лишь небольшой процент организаций, чьи эндпоинты мы отслеживаем. Однако мы зафиксировали около 1000 случаев заражения в этих организациях за короткий промежуток времени».

Основная опасность этой вредоносной кампании состоит в том, что уязвимый UI Telerik может быть частью приложений ASP.NET, которые работают с новейшими и актуальными версиями ПО, но сам компонент Telerik при этом может быть серьезно «просрочен», тем самым подвергая компании рискам атак. К сожалению, многие компании и разработчики могут вообще не знать о том, что UI Telerik присутствует в составе их приложений, что опять же подвергает их риску.

Напомню, что об опасности уязвимости в UI Telerik (CVE-2019-18935) недавно предупреждало Агентство национальной безопасности США, назвав его одной из наиболее используемых для установки веб-шеллов проблем. Также в мае 2020 года Австралийский центр кибербезопасности включил эту уязвимость в список наиболее эксплуатируемых багов, которые использовались для атак на австралийские организации в 2019 и 2020 годах.

Так как зачастую компании вообще не имеют возможности обновить уязвимые приложения, им рекомендуется защищаться от попыток эксплуатации CVE-2019-18935 на уровне брандмауера». ***(Мария Нефёдова. Группировка Blue Mockingbird взломала тысячи корпоративных систем // Xakep (https://xakep.ru/2020/05/26/blue-mockingbird/). 26.05.2020).***

***

Вірусне та інше шкідливе програмне забезпечення

«IoT-ботнет Cereals появился еще в 2012 году, а пика своей активности достиг в 2015, ког да насчитывал около 10 000 зараженных устройств. Все это время Cereals использовал всего одну уязвимость и атаковал NAS и NVR компании D-Link, объединяя их в ботнет.

Долгие годы ботнет ускользал от внимания большинства ИБ-специалистов, а сейчас и вовсе почти прекратил свое существование. Дело в том, что уязвимые устройства D-Link, на которых Cereals паразитировал, начали устаревать и выходить из строя, то есть их становится все меньше и меньше. Кроме того, распад ботнета ускорил вымогатель Cr1ptT0r, который уничтожал конкурирующую

малварь на зараженных устройствах и удалил малварь Cereals со многих девайсов D-Link зимой 2019 года.

Теперь, когда ботнет и уязвимые устройства, которые он эксплуатировал, исчезают, эксперты компании Forcepoint решили опубликовать отчет о деятельности малвари, ведь более можно не опасаться того, что исследование привлечет внимание других преступников к уязвимым девайсам и спровоцирует появление новых ботнетов.

Эксперты пишут, что Cereals можно назвать уникальным явлением, так как ботнет использовал лишь одну уязвимость на протяжении всех восьми лет своей «жизни». Эта уязвимость была связана с функцией SMS-уведомлений, которая присутствовала в прошивках NAS и NVR компании D-Link. Баг позволял создателю Cereals отправлять вредоносные HTTP-запросы на встроенные серверы уязвимых девайсов и выполнять команды с правами root. Таким образом оператор ботнета и заражал устройства своей малварью.

Исследователи отмечают, что по своей функциональности ботнет был весьма продвинутым. Так, если атака удавалась, Cereals поддерживал на устройствах до четырех активных бэкдоров, старался пропатчить атакованные девайсы, чтобы другие злоумышленники не могли атаковать их, и распределял ботов по 12 небольшим подсетям.

Однако все эти усилия, по сути, пропадали впустую и не имели под собой никакой цели. Аналитики Forcepoint полагают, что Cereals был чьим-то хобби или проектом, созданным ради шутки (предполагается, что автора малвари зовут Стефан, и он проживает в Германии).

Дело в том, что ботнет не занимался DDoS-атаками, не пытался атаковать какие-либо еще девайсы, кроме вышеупомянутых, не пытался получить доступ к пользовательским данным, хранящимся на зараженных устройствах. Вместо этого все эти годы Cereals просто методично скачивал аниме». ***(Мария Нефёдова. Восемь лет ботнет Cereals существовал лишь с одной целью: скачивать аниме // Хакер (https://xakep.ru/2020/05/08/cereals/). 08.05.2020).***

***

«Специалисты Malwarebytes рассказали об интересной MageCart-кампании, для осуществления которой хак-группа создала вредоносный сайт для размещения favicon и маскировки вредоносного кода.

…изначально название MageCart было присвоено одной хак-группе, которая первой начала использовать так называемые веб-скиммеры на сайтах для хищения данных банковских карт. Хакеры взламывают сайты, а затем внедряют на их страницы вредоносный код, который записывает и похищает данные платежных карт, когда пользователи вводят их во время оформления заказа.

Этот подход оказался настолько успешным, что у группировки вскоре появились многочисленные подражатели, а название MageCart стало нарицательным, и теперь им обозначают целый класс подобных атак. И если в 2018 году исследователи RiskIQ идентифицировали 12 таких группировок, то в конце 2019 года, по данным IBM, их насчитывалось уже около 40.

Исследователи Malwarebytes пишут, что обнаруженная ими недавно хак-группа вывела свои операции на совершенно новый уровень сложности. Аналитики компании выявили вредоносную кампанию, расследуя серию странных взломов, единственной целью которых была подмена favicon на взломанных сайтах.

Новые favicon представляли собой файлы изображений, размещенные на сайте MyIcons.net, и не содержали вредоносного кода. И хотя на первый взгляд эта подмена выглядела вполне невинной, эксперты обнаружили на всех пострадавших сайтах веб-скиммеры, а с новыми favicon что-то было не в порядке.

Как показало дальнейшее расследование, хитрость заключалась в том, что сайт MyIcons.net предоставлял легитимный файл favicon для всех страниц атакованного ресурса, кроме тех, где размещались формы оформления заказа.

На страницах оформления заказа MyIcons.net подменял обычный favicon вредоносным файлом JavaScript, который создавал поддельную форму оплаты и воровал введенные в нее данные карты пользователя.

Эксперты отмечают, что владельцы сайтов, заметившие обращения к MyIcons.net, обнаружили бы безвредный портал для хостинга favicon. Однако на самом деле данный сайт выступал клоном легитимного портала IconArchive.com и служил обычной ширмой для проведения атак.

Кроме того, стоит отметить, что данный сайт был размещен на те же серверах, которые ранее использовались в других скиммерских операциях, что несколько недель назад заметили специалисты компании Sucuri». ***(Мария Нефёдова. Хакеры научились прятать веб-скиммеры за favicon сайтов // Хакер (https://xakep.ru/2020/05/07/favicon-skimmer/). 07.05.2020).***

***

«Согласно новому отчету «Лаборатории Касперского» о сложных целевых атаках (APT), в I квартале возросло количество случаев распространения вредоносных программ и заражения ими посредством мобильных платформ. Причем некоторые APT-кампании были сосредоточены исключительно на мобильных устройствах.

«Лаборатория Касперского» недавно опубликовала отчеты о ряде подобных вредоносных кампаний. Среди них масштабная атака типа watering hole, нацеленная на пользователей в Гонконге, в ходе которой на смартфоны жертв устанавливался LightSpy – многофункциональный зловред для iOS. Также эксперты сообщили об угрозе PhantomLance, нацеленной на пользователей Android-устройств в Южной Азии. Примечательно, что в рамках обеих кампаний успешно использовались различные онлайн-платформы – от форумов и социальных сетей до магазинов приложений.

Также в течение первых трех месяцев продолжала набирать обороты APT-активность в Азии. В частности, различные атаки затрагивали Юго-Восточную Азию и такие страны, как Корея и Япония. По наблюдениям экспертов «Лаборатории Касперского», новые APT-группировки реализовывали нестандартные и иногда малобюджетные вредоносные кампании. Они устанавливали свое присутствие в регионе наряду с известными CactusPete и Lazarus.

APT-группировки, активные в Азии, не единственные, кто создавал и использовал мобильные импланты. Например, TransparentTribe провела вредоносную кампанию с помощью нового модуля под названием USBWorm. Эти злоумышленники, нацеленные жертв в Афганистане и Индии, разработали имплант, предназначенный для заражения Android-устройств. Использованный зловред представлял собой модифицированную версию Android RAT под названием AhMyth – вредоносной программы с открытым исходным кодом, который был доступен на GitHub.

Кроме того, начиная с середины марта, различные APT-группировки эксплуатировали тему коронавируса для привлечения жертв. Среди них Kimsuky, IronHasky, Hades и DarkHotel.

Для защиты от целевых атак «Лаборатория Касперского» рекомендует принимать следующие меры: предоставить сотрудникам центров мониторинга угроз (SOC) доступ к самым свежим данным об угрозах и обеспечить им возможность быть в курсе новейших инструментов, техник и тактик, используемых злоумышленниками; внедрить решение для защиты конечных устройств. Решение должно включать в себя защиту мобильных устройств, а также обеспечивать контроль приложений; внедрить решение корпоративного уровня, которое детектирует сложные угрозы на сетевом уровне на ранней стадии; поскольку многие целевые атаки начинаются с фишинга или других методов социальной инженерии, необходимо повышать осведомленность сотрудников о кибербезопасности». ***(APT-группировки переходят на мобильные устройства // Компьютерное Обозрение (https://ko.com.ua/apt-gruppirovki_perehodyat_na_mobilnye_ustrojstva_132857). 04.05.2020).***

***

«Национальный центр реагирования на компьютерные инциденты Республики Беларусь (CERT.BY) обнаружил в национальном сегменте интернета активность бэкдор-трояна семейства Pteranodon. В основном вредонос используется для атак на государственные структуры, но иногда также встречается на домашних компьютерах. К настоящему времени признаки заражения были обнаружены более чем на 400 устройствах.

Инфицирование трояном происходит через фишинговые письма с вредоносными документами, содержащими макросы. После активации макросов и установки на взломанной системе Pteranodon позволяет своим операторам похищать конфиденциальные данные жертвы и устанавливает дополнительные вредоносные модули.

Для выявления Pteranodon на компьютере рекомендуется проверить наличие его промежуточных файлов в str_AppDataPath + «\Microsoft\Windows\Start Menu\Programs\Startup\security.vbs». Ключ реестра: «HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run» /v «OfficePlugin». ***(Белорусские госструктуры атакует троян Pteranodon // SecurityLab.ru (https://www.securitylab.ru/news/508045.php). 05.05.2020).***

***

«Издание Bleeping Computer сообщает о необычной хакерской кампании, развернутой в этом месяце.

На прошлой неделе ИБ-специалист, известный под псевдонимом GrujaRS, первым заметил появление не совсем обычного шифровальщика MilkmanVictory. Как оказалось, эту малварь создали хакеры из группы CyberWare, и основной задачей данного вредоноса является не вымогательство выкупа за расшифровку данных, как это бывает обычно, а уничтожение информации. Дело в том, что шифровальщик был создан для атак против мошенников.

Представители группировки CyberWare сначала заявили о себе в Twitter, а потом согласились ответить на вопросы журналистов Bleeping Computer. Хак-группа объясняет, что основной целью их кампании являются фирмы, занимающиеся так называемым кредитным мошенничеством.

«Жертвы рассказывают, что им обещали дать кредит, но оказалось, что сначала нужно было заплатить [мошенникам], чтобы в итоге не получить ничего», — говорят хакеры.

В частности группировка атаковала немецкую компанию Lajunen Loan, чей сайт в настоящее время недоступен. Участники CyberWare обрушили DDoS-атаку на ресурс, а также направили на адреса компании фишинговые письма, несущие заражение MilkmanVictory. Эти послания содержат ссылки на вредоносные исполняемые файлы, замаскированные под файлы PDF.

Шифровальщик MilkmanVictory был задуман как вайпер (wiper, от английского to wipe — «стирать»). То есть эта малварь умышленно не сохраняет ключ шифрования и не предлагает пострадавшим связаться с хакерами для оплаты выкупа. Вместо этого послание, которое оставляет после себя малварь, гласит:

«Здравствуйте! Этот компьютер был уничтожен шифровальщиком MilkmanVictory, потому что мы знаем, что вы мошенник! Хакеры CyberWare :-)».

В CyberWare подчеркнули, что они не вымогают у скамеров деньги, так как мошенники, ворующие средства у невинных людей, подобного не заслуживают.

Журналисты Bleeping Computer отмечают, что MilkmanVictory был построен на основе известного опенсорсного шифровальщика Hidden Tear, который давно изучен ИБ-экспертами. Это означает, что даже если ключ шифрования не был сохранен, пострадавшие данные все равно можно восстановить. К примеру, для этого можно использовать бесплатный инструмент Hidden Tear Decryptor, созданный известным ИБ-экспертом Майклом Гиллеспи». ***(Мария Нефёдова. Хак-группа CyberWare атакует мошенников, используя для этого шифровальщик // Xakep (https://xakep.ru/2020/05/21/milkmanvictory/). 21.05.2020).***

***

«В этом месяце ИБ-эксперты и правоохранители обратили свое внимание на шифровальщик ProLock, недавно атаковавший одного из крупнейших производителей банкоматов – компанию Diebold Nixdorf.

Специалисты Group-IB посвятили малвари большой отчет. Они рассказывают, что шифровальщик появился в марте 2020 года и является преемником малвари PwndLocker, активной с конца 2019 года (вредонос был

переименован в ProLock после того, как эксперты Emsisoft нашли способ расшифровки файлов PwndLocker). Атаки ProLock чаще всего нацелены на финансовые и медицинские организации, государственные учреждения и сектор розничной торговли.

Исследователи Group-IB пишут, что операторы ProLock используют два основных вектора распространения малвари: троян QakBot (Qbot) и незащищенные RDP-серверы со слабыми паролями.

И если с взломом RDP-серверов все ясно, то использование QakBot является весьма интересным вектором распространения. Раньше данный троян связывали с другим семейством шифровальщиков, MegaCortex, но теперь им пользуются операторы ProLock.

Как правило, сам QakBot распространяется через фишинговые кампании. Фишинговое письмо может содержать прикрепленный документ Microsoft Office или ссылку на вредоносный файл, находящийся в облачном хранилище, например, Microsoft OneDrive. Также известны случаи загрузки QakBot другим трояном, Emotet, который широко известен своим участием в кампаниях, распространявших вымогателя Ryuk.

После загрузки и открытия зараженного документа пользователю предлагается разрешить выполнение макросов, в случае успеха осуществляется запуск PowerShell, который позволит загрузить и запустить полезную нагрузку QakBot с командного сервера.

Также предупреждение о ProLock в этом месяце выпустили и специалисты ФБР. Они объясняют, что шифровальщик, судя по всему, вручную управляется операторами, то есть устанавливается в сетях скомпрометированных организаций вручную, а не автоматически.

Хакерские группы нередко взламывают или покупают доступ к взломанной сети какой-либо компании у других злоумышленников. Они берут скомпрометированный хост под контроль, а затем используют его для бокового распространения по сети. Внедрение шифровальщиков происходит уже после этого, в ручном режиме, когда злоумышленники максимально расширят свой доступ.

Именно таким образом операторы ProLock используют Qakbot. Это не уникальный случай: ранее эксперты обнаруживали, что вымогатели Ryuk и Maze часто появляются на компьютерах, ранее зараженных трояном TrickBot, а вымогатель DopplePaymer идет рука об руку с малварью Dridex. При этом пока остается неясным, был ли ProLock создан теми же авторами, что и Qakbot, или операторы ProLock покупают доступ к зараженным Qakbot хостам и сотрудничают с другой хак-группой.

Также ФБР предупредило, что инструмент для расшифровки данных, который жертвам ProLock предоставляют сами злоумышленники, зачастую работает некорректно и не помогает спасти информацию, даже если выкуп был выплачен.

«Расшифровщик потенциально может испортить файлы размером более 64 Мб и привести к повреждению целостности файла, примерно на 1 байт на каждый 1 Кб для файлов свыше 100 Мб», — предупреждает ФБР». ***(Мария Нефёдова.***

Шифровальщик ProLock объединил усилия с трояном QakBot // Xakep (https://xakep.ru/2020/05/19/prolock/). 19.05.2020).

***

«Прошло уже три года после эпидемии шифровальщика WannaCry, из-за которой пострадали компании и организации по всему миру, а ландшафт ИБ навсегда изменился. Напомню, что исследователи и власти единогласно возложили ответственность за произошедшее на северокорейских хакеров, а правительство США даже предъявило заочные обвинения вполне конкретному подозреваемому.

На этой неделе, чтобы отметить годовщину, специалисты ФБР, Министерства обороны США и Агентства по кибербезопасности и защите инфраструктуры, организованного при Министерстве внутренней безопасности США (DHS CISA) раскрыли информацию о трех новых вредоносах, авторство которых приписывают северокорейской хак-группе Lazarus, также известной как Hidden Cobra. О новых вредоносах не только рассказали в докладе, но и загрузили образцы на VirusTotal.

Напомню, что власти США публикуют информацию о северокорейский малвари с 2017 года и к настоящему моменту рассказали уже 28 различных угрозах. Идея этой инициативны заключается в том, чтобы сделать информацию о малвари публичной и доступной. Тогда государственный и частный секторы смогут без труда обнаруживать и блокировать атаки с использованием описанных вредоносов, а это усложнит жизнь северокорейским хакерам, вынуждая их постоянно работать над новыми версиями своих инструментов, эксплоитов и малвари.

На этой неделе огласке предали информацию о следующих угрозах:

COPPERHEDGE — троян удаленного доступа (RAT), способный запускать произвольные команды, выполнять разведку и похищать данные. Были обнаружены шесть разных вариантов.

TAINTEDSCRIBE — вредоносный имплант (троян), который устанавливается на взломанные системы для получения и выполнения команд злоумышленников. Использует FakeTLS для аутентификации сессий, а для шифрования применяет алгоритм Linear Feedback Shift Register (LFSR). Основной исполняемый файл маскируется под Microsoft's Narrator.

PEBBLEDASH — еще один имплант, который имеет возможность загружать, выгружать, удалять и выполнять файлы; включать доступ Windows CLI; создавать и завершать процессы, и так далее.

Эксперт «Лаборатории Касперского» Костин Райю пишет, что все три разновидности вредоносного ПО действительно связаны с известными северокорейскими хак-группами. По его словам, код опубликованных образцов схож с кодом вредоноса Manuscrypt, который был обнаружен «Лабораторией Касперского» в 2017 году и использовался для атак на криптовалютные биржи». **(Мария Нефёдова. В честь годовщины атак WannaCry власти США рассказали о новой северокорейской малвари // Xakep (https://xakep.ru/2020/05/15/dprk-malware/). 15.05.2020).**

***

«Эксперты компаний Avast и ESET проанализировали малварь, которую использовала неизвестная китайская APT-группировка, шпионившая за неназванными телекоммуникационной и газовой компаниями, а также правительственным учреждением в Центральной Азии. Аналитики ESET дали этой кампании название Mikroceen.

В своих операциях хак-группа использовала бэкдоры, чтобы получить постоянный доступ к корпоративным сетям своих жертв. Основываясь на полученных данных, исследователи предполагают, что ранее эта же группа была причастна к другим атакам в Монголии, России и Беларуси, и активна как минимум 2017 года.

Данную теорию эксперты подкрепляют тем, что хакеры, во-первых, использовали троян Gh0st RAT, который давно и часто применяется китайскими APT-группами. Во-вторых, аналитики обнаружили явные сходства в коде использованных хакерами вредоносов.

Изученные бэкдоры позволяли хакерам управлять файлами жертв (удалять, читать, перемещать, проверять наличие), делать снимки экрана, вмешиваться в работу процессов и сервисов, а также выполнять консольные команды и скрывать признаки своего присутствия в системе. По команде малварь могла передавать данные компании-жертвы на свой управляющий сервер, а зараженные устройства могли играть роль прокси-сервера или прослушивать определенный порт на каждом сетевом интерфейсе.

«Группа, стоящая за этой атакой, часто перекомпилирует свои кастомные инструменты (которые, в дополнение к бэкдорам, включали Mimikatz и Gh0st RAT), чтобы избежать обнаружения антивирусными решениями. В итоге мы имеем большое количество образцов малвари, причем бинарники часто защищены VMProtect, что затрудняет анализ», – отмечает Луиджино Камастра, исследователь Avast.

Специалисты уже сообщили о своих выводах CERT и попытались связаться с пострадавшей телекоммуникационной компанией, однако пока ответов от пострадавших организаций получить не удалось. Учитывая, что группировка по-прежнему активна, а изученные инциденты удалось связать с атаками на другие цели, исследователи полагают, что мы еще услышим об этой хак-группе, и она продолжат атаковать цели и в других странах». ***(Мария Нефёдова. Китайские хакеры атаковали телекоммуникационную и газовую компании в Центральной Азии // Xakep (https://xakep.ru/2020/05/15/mikroceen/). 15.05.2020).***

***

«Аналитики компании ESET обнаружили инфраструктуру ранее неизвестной малвари Ramsay с весьма интересными возможностями. Дело в том, что Ramsay предназначен для сбора данных с компьютеров, которые изолированы от внешнего мира. Проникнув в такую систему, вредонос собирает файлы Word и другие конфиденциальные документы, прячет их в скрытом контейнере и ждет возможности передать данные вовне.

«Мы обнаружили первый экземпляр Ramsay на VirusTotal, — рассказывают эксперты. — Данный образец был загружен из Японии, и он привел нас к открытию дополнительных компонентов и версий платформы».

Малварь, созданная для кражи информации с машин, физически изолированных от любых сетей и потенциально опасной периферии, встречается весьма редко. Такие компьютеры в основном используются в правительственных системах и корпоративных сетях, и, как правило, на них хранятся секретные документы, а также другая закрытая и конфиденциальная информация, включая, например, интеллектуальную собственность.

Исследователи ESET пишут, что им удалось обнаружить три разные версии Ramsay, одна из которых была скомпилирована в сентябре 2019 года (Ramsay 1), а две другие — в начале и конце марта 2020 года (Ramsay 2.a и 2.b).

Обычно Ramsay проникает в систему через вредоносные документы, которые распространяются через фишинговые письма или с помощью USB-накопителя. Затем малварь использует старую RCE-проблему в Microsoft Office, чтобы "развернуться" в системе.

Все версии вредоноса отличаются друг от друга и заражают жертв разными способами, однако суть остается неизменной: проникнув в систему, малварь должна просканировать зараженный компьютер, собрать файлы Word, PDF и ZIP в скрытой папке и подготовить их к последующей передаче вовне.

Некоторые версии имеют и специальный модуль распространения, который добавляет копии Ramsay ко всем файлам PE, обнаруженным на съемных дисках и среди сетевых ресурсов. Исследователи полагают, что малварь могла использовать этот механизм для распространения, чтобы добираться до изолированных машин и сетей. Ведь пользователи могут перемещать зараженные исполняемые файлы между различными уровнями корпоративной сети, и в конечном итоге малварь попадет в изолированные системы.

Аналитики ESET признаются, что не сумели определить, каким образом Ramsay извлекает собранные на изолированных машинах данные. Также эксперты не делали конкретных выводов относительно атрибуции Ramsay, однако отмечается, что малварь имеет сходство с вредоносном Retro, разработанным южнокорейской хак-группой DarkHotel». ***(Мария Нефёдова. Вредонос Ramsay предназначен для атак на ПК, изолированные от внешнего мира // Xakep (https://xakep.ru/2020/05/14/ramsay/). 14.05.2020).***

***

«Специалисты из компании Trend Micro сообщили о вредоносной кампании, в ходе которой киберпреступная группировка Tropic Trooper на протяжении нескольких лет использует вредоносное ПО USBferry для осуществления атак направленного фишинга на физически изолированные сети тайваньских и филиппинских военных организаций, военно-морских ведомств, государственных учреждений, военных госпиталей и даже национального банка.

По словам экспертов, USBferry способен выполнять различные команды, поддерживать скрытность в средах и похищать важные данные через USB-

хранилище. Вредоносная кампания началась еще в 2018 году, однако анализ данных показал, что атаки с использованием USBferry осуществляются как минимум с 2014 года. Преступники сосредоточены на краже конфиденциальной информации и разведданных, связанных с обороной и военно-морским флотом, из целевых сетей.

Исследователи в ходе анализа обнаружили три версии вредоноса USBferry с различными вариантами и компонентами.

Первая версия содержит небольшой компонент TROJ_YAHOYAH. Вредоносная программа пытается проверить наличие подключаемого USB-модуля на целевой машине и копирует установщик USBferry в USB-накопитель. Действия варьируются в целевых средах; некоторые из них выполняют команды, исходные целевые файлы или списки папок, а также копируют файлы с физически изолированных хостов на скомпрометированные хосты.

Вторая версия имеет те же возможности, что и первая, и объединяет компоненты в один исполняемый файл. Данная версия изменяет местоположение вредоносного ПО и его имя на UF — сокращение от USBferry.

Третья сохраняет возможности предыдущих версий и улучшает скрытность в целевой среде, находясь в памяти rundll32.exe.

Tropic Trooper в последнее время изменила способ использования USBferry в своих атаках. Группировка использует стратегию заражения USB-червем и размещает установщик вредоносного ПО через USB в физически изолированном хосте. Вредонос поверяет подключение к сети и если обнаруживает, что сеть недоступна, он пытается собрать информацию с целевой машины и скопировать собранные данные на USB-накопитель. Таким образом, USB отфильтровывает информацию и отправляет ее обратно на C&C-сервер.

Tropic Trooper в ходе атак также использовала бэкдоры WelCome To Svchost 3.2 20110818, Welcome To IDShell 1.0 20150310 и Hey! Welcome Server 2.0.

Среди других инструментов, используемых Tropic Trooper, эксперты обнаружили средство ретрансляции портов, взаимодействующее с бэкдорами, загрузчики полезной нагрузки и инструменты сканирования портов, доступных в Сети». ***(Группировка Tropic Trooper годами атакует сети военно-морских ведомств // SecurityLab.ru (https://www.securitylab.ru/news/508344.php). 15.05.2020).***

***

«В течение последних 4 месяцев специалисты подразделения Unit 42 компании Palo Alto Networks следили за киберпреступной группировкой Hangover (также известной как Neon, Viceroy Tiger, MONSOON), которая использовала вредоносное ПО BackConfig. Жертвами киберпреступников стали правительственные и военные организации в Южной Азии.

BackConfig обладает различными функциями, в том числе возможностью сбора информации о системе и кейлогинга, а также загрузки и выполнения дополнительных полезных нагрузок. Последние версии вредоноса содержат модульные компоненты, облегчающие обновление и повторное использование кода. Как отметили эксперты, преступники также пытаются избежать «песочницы»

и других систем автоматического анализа, разделяя вредонос на отдельные компоненты, не вызывающие подозрений.

Заражение системы происходит через документ Microsoft Excel (XLS), доставляемый через скомпрометированные легитимные web-сайты, URL-адреса которых передаются по электронной почте. В документах используется макрос-код на языке Visual Basic for Applications (VBA), который при включении запускает процесс установки нескольких вредоносных компонентов.

Цель вредоносной программы состоит в том, чтобы обеспечить преступникам возможность загружать и выполнять исполняемые файлы, а также загружать и запускать пакетные файлы для запуска команд на целевой системе.

По словам специалистов, образец вредоносного ПО содержит некоторые интересные статические артефакты, в том числе самозаверяющие цифровые сертификаты, используемые для подписи исполняемого файла, предполагающего использование программного обеспечения от компании Foxit Software Incorporated. Неизвестно, почему операторы вредоноса выбрали данную компанию для подражания, но их использование имен файлов и URL-адресов позволяет лучше замаскировать вредоносное ПО.

Практически во всех случаях киберпреступники использовали вредоносные документы, требующие взаимодействия с пользователем, и только один раз за последние несколько месяцев группировка использовала эксплоиты для избежания необходимости выполнения пользователем какого-либо этапа установки». ***(APT Hangover нацелилась на правительственные организации в Южной Азии // SecurityLab.ru (https://www.securitylab.ru/news/508303.php). 14.05.2020).***

***

«Британская фирма в области кибербезопасности Sophos сообщила о новом вирусе-вымогателе Ragnar Locker, который запускает виртуальную машину для доступа к файлам пользователей и обхода антивирусов.

Специалисты в области информационной безопасности отметили, что благодаря запуску виртуальной машины Ragnar Locker обходит антивирусы и шифрует файлы. При этом вирус-шифровальщик, как правило, атакует корпоративные сети, а не частных пользователей.

Хакеры требуют действительно впечатляющие суммы за расшифровку файлов. Так, за код для расшифровки данных компании Energias de Portugal они запросили 1 850 BTC (около $17 млн по текущему курсу). В случае отказа от выплаты биткоинов злоумышленники пригрозили продать корпоративные тайны компании конкурентам.

Специалисты Sophos рассказали, что для заражения компьютера вирус использует уязвимости в системе удаленного рабочего стола Windows. После получения административных привилегий Ragnar Locker запускает виртуальную машину с урезанной копией Windows XP под названием «Micro XP v0.82».

«Операторы обнаружили новый вирус-вымогатель, который использует виртуальную машину для обхода продуктов по компьютерной безопасности. Как и другие подобные вирусы, Ragnar Locker крадет данные, чтобы убедить жертву заплатить выкуп. Если выкуп не будет выплачен, то данные публикуются на сайте

группы в анонимной сети Tor», – рассказал специалист по кибербезопасности из компании Emsisoft Бретт Каллоу.

Он также подчеркнул, что компании, который подверглись атакам подобных вирусов, оказываются в незавидном положении. Даже при выплате выкупа у них остается лишь обещание хакеров о том, что те не опубликуют или не продадут полученные данные». ***(Новый вирус-вымогатель атакует крупные корпорации // LetKnow OÜ (https://letknow.news/news/novyy-virus-vymogatel-atakuet-krupnye-korporacii-37538.html). 25.05.2020).***

***

«Компания ESET обнаружила новую версию бэкдора ComRAT известной группы киберпреступников Turla (также известная как Snake), которая активна уже больше десяти лет. Особенностью обновленного бэкдора является использование веб-интерфейса Gmail для получения команд и кражи данных.

Бэкдор позволяет похищать конфиденциальные документы, и с 2017 года он использовался для атак минимум на три правительственные учреждения. Специалисты ESET нашли признаки использования последней версии ComRAT в начале 2020 года, что подтверждает высокую активность группы Turla сегодня. Обновленный бэкдор использует совершенно новый код и имеет более сложный функционал, чем его предыдущие версии.

Как правило, ComRAT используется для похищения конфиденциальных данных. В некоторых случаях киберпреступники даже разворачивали исполняемый файл .NET для взаимодействия с центральной базой данных MS SQL Server жертвы, которая содержит документы организации. Операторы вредоносных программ использовали общедоступные облачные сервисы, такие как OneDrive и 4shared для кражи данных. Последняя версия бэкдора Turla может выполнять много других действий на зараженных компьютерах, например, загружать дополнительные программы.

«Высокий уровень сложности функционала вредоносного программного обеспечения группы киберпреступников позволяет избегать обнаружения программами по безопасности и длительное время оставаться на одних и тех же устройствах, — объясняет Матье Фау, исследователь компании ESET. — Кроме того, последняя версия бэкдора ComRAT способна обойти некоторые меры контроля безопасности с помощью использования веб-интерфейса Gmail, поскольку она не зависит от любого вредоносного домена»…». ***(Киберпреступники используют веб-интерфейс Gmail для кражи даннях // Компьютерное Обозрение (https://ko.com.ua/kiberprestupniki_ispolzuyut_veb-interfejs_gmail_dlya_krazhi_dannyh_133159). 27.05.2020).***

***

«Разработчики GitHub выпустили предупреждение о появлении новой малвари Octopus Scanner, которая распространяется по сайту через вредоносные Java-проекты.

Octopus Scanner был обнаружен в проектах, управляемых с помощью Apache NetBeans IDE, инструмента, который используется для написания и компиляции

Java-приложений. После наводки, полученной в марте от ИБ-исследователи, разработчики нашли 26 репозиториев, содержащих малварь. Список репозиториев к предупреждению, к сожалению, не прилагается.

Представители GitHub объясняют, что когда пользователи скачивали любой из этих 26 проектов, малварь вела себя как самораспространяющийся червь и продолжала заражать локальные компьютеры. Octopus Scanner сканировал рабочую станцию в поисках локальной установки IDE NetBeans и внедрялся в другие Java-проекты жертвы.

Малварь была приспособлена для работы с Windows, macOS и Linux, и в конечном счете загружала троян удаленного доступа (RAT), позволяя своим операторам покопаться в файлах на компьютере жертвы в поисках конфиденциальной информации.

GitHub сообщает, что кампания Octopus Scanner длилась несколько лет. Самый старый образец малвари был загружен в VirusTotal в августе 2018 года. И хотя на GitHub было обнаружено только 26 репозиториев со следами Octopus Scanner, эксперты полагают, что за последние два года было заражено гораздо больше проектов.

Судя по всему, настоящей целью этих атак было размещение RAT на машинах людей, работающих над важными проектами или в крупных компаниях, разрабатывающих ПО. Это позволяло атакующим похищать конфиденциальную информацию о грядущих релизах, проприетарном исходном коде и даже внедрять бэкдоры в корпоративное или другое ПО с закрытым исходным кодом.

«Интересно, что эта вредоносная программа специально атаковала NetBeans, поскольку на сегодня это не самая распространенная Java IDE.

Если создатели малвари потратили время на имплементацию этой малвари именно под NetBeans, это может означать, что либо это была целевая атака, либо у них, вероятно, уже были имплементации вредоносного ПО для таких билд-систем, как Make, MsBuild, Gradle и так далее, и оно могло распространяться незаметно», — пишут специалисты GitHub». ***(Мария Нефёдова. Вредонос Octopus Scanner обнаружен на GitHub // Xakep (https://xakep.ru/2020/05/29/octopus-scanner/). 29.05.2020).***

***

«В последних версиях Android компания Google строго ограничила ресурсы и элементы, к которым у приложений есть доступ. Тем не менее, существует множество подозрительных приложений, запрашивающих разрешения на действия, не требующиеся им для работы. К примеру, специалисты из VPNpro обнаружили в Google Play Store целый ряд таких приложений, в общей сложности установленных более чем на 150 млн устройств.

Разработчиком приложений, названных специалистами VPNpro «шпионским ПО», является зарегистрированная в Ханчжоу китайская компания QuVideo. Разработчик известен своим популярным видеоредактором VivaVideo, насчитывающим порядка 100 млн установок из Google Play Store. В 2017 году VivaVideo наряду еще с 40 китайскими приложениями было признано властями Индии вредоносной или шпионской программой.

По словам экспертов, обнаруженные ими приложения от QuVideo, в частности VivaVideo, запрашивают «опасные разрешения», в том числе разрешение на чтение и запись файлов на внешние накопители и доступ к геолокационным данным, которые видеоредактору ни к чему. Речь идет о приложениях SlidePlus (1 млн установок), а также о платной версии VivaVideo.

Кроме того, QuVideo принадлежит индийское приложение VidStatus, установленное на 50 млн устройствах. Программа запрашивает сразу девять опасных разрешений, в том числе доступ к геолокационным данным, контактам и спискам звонков. ПО признано вредоносным компанией Microsoft, так как содержит скрытый троян для удаленного доступа AndroidOS/AndroRat. Подобные трояны способны похищать средства с банковских счетов, криптовалютных кошельков и PayPal-аккаунтов.

В Apple App Store исследователи обнаружили четыре приложения от QuVideo – VivaVideo, SlidePlus, VivaCut и Tempo. В Google Play Store приложения VivaCut и Tempo также присутствуют, но их издателями значатся другие разработчики». ***(Китайское шпионское ПО загружено из Google Play Store более 150 млн раз // SecurityLab.ru (https://www.securitylab.ru/news/508735.php). 29.05.2020).***

***

«Специалисты «Доктор Веб» обнаружили, что на YouTube появляются ролики, в которых рассказывается о появлении мобильной версии игры Valorant (и потенциальным жертвам предлагают ее установить). Под видом этой игры на Android-устройства попадает троян, с помощью которого хакеры зарабатывают на участии в партнерских программах.

Те, кто следит за игровыми новостями, знают, что Valorant по-прежнему находится в разработке и пока доступна лишь в рамках бета-теста (и только для компьютеров под управлением ОС Windows). Однако мошеннические ролики смонтированы таким образом, что процесс игры на экране мобильного устройства выглядит правдоподобно.

Для большей убедительности такие видео сопровождаются подробным описанием, а также множеством комментариев пользователей, которые якобы успешно установили игру на свои мобильные устройства. Все эти отзывы, разумеется, являются фальшивыми.

Для загрузки игры пользователям предлагают посетить сайт, внешне похожий на официальный сайт проекта Valorant. На этом ресурсе размещены две ссылки, по которым на мобильное устройство якобы можно загрузить игру.

Если посетитель сайта попытается загрузить игру для устройства под управлением iOS, его перенаправят на сайт партнерской программы. Если же попытка скачивания происходит с Android-устройства, на него загружается APK-файл с трояном Android.FakeApp.176. Поскольку этот файл загружается не из официального каталога Google Play, на большинстве современных устройств для его установки потребуется изменить соответствующие настройки системы безопасности.

Вредоносное приложение имитирует процесс запуска игры, однако затем предлагает «разблокировать» ее, выполнив идентификацию устройства. Для этого от пользователя требуется скачать и установить два других приложения.

Если согласие на «разблокировку» получено, троян открывает в браузере сайт того же партнерского сервиса, что и в случае с iOS-устройствами. После проверки ряда параметров этот сайт перенаправляет пользователя на сайт другой партнерской программы. На нем представлены задания, которые посетителю необходимо выполнить для получения вознаграждения. В рассматриваемом экспертами случае от пользователя требуется установить и запустить игру из каталога Google Play, а также принять участие в онлайн-опросе.

По сути, такие сайты представляют собой типичные сервисы для заработка на кликах, накрутке счетчиков посещений, рекламе различного ПО и накрутке числа его установок, а также на монетизации онлайн-опросов и других маркетинговых кампаний в интернете.

Некоторые из подобных сервисов действительно дают пользователям обещанные вознаграждения, например, когда то или иное задание выполняется для пополнения внутриигрового баланса или получения определенных бонусов в играх.

Однако в случае с трояном Android.FakeApp.176 пользователи не получают обещанной им игры. Мобильной версии Valorant попросту не существует, а единственная задача подделки — загрузить сайт партнерского сервиса, в результате чего мошенники получат вознаграждение за счет жертвы…». ***(Мария Нефёдова. Под видом мобильной версии игры Valorant распространяется троян // Xakep (https://xakep.ru/2020/05/29/fake-valorant/). 29.05.2020).***

***

«Специалисты компании Qihoo 360 раскрыли подробности об одном из крупнейших ботнетов в Китае под названием DoubleGuns. Данный ботнет атакует только китайских пользователей и насчитывает миллионы жертв.

DoubleGuns представляет собой троян для заражения устройств под управлением Windows. Вредонос используется с июля 2017 года, когда исследователи Qihoo 360 впервые обнаружили его ранний вариант. За последние три года троян мало изменился. Он по-прежнему попадает на устройства через зараженные приложения (в основном, нелицензионные игры), распространяемые на китайских сайтах (в соцсетях и на игровых форумах).

Главная задача вредоноса остается прежней – установка на устройства MBR- и VBR-буткитов, а также всевозможных вредоносных драйверов с последующим похищением учетных данных для авторизации в локальных приложениях, в особенности Steam. Кроме того, он играет роль модуля для отображения рекламы и спама.

Более старые версии DoubleGuns также перехватывали трафик легитимных порталов электронной коммерции и переадресовывали пользователей на их вредоносные копии. Однако в последних версиях трояна данный функционал отсутствует.

Когда ботнет достиг таких размеров, что его уже нельзя было игнорировать, специалисты Qihoo 360 скооперировались с коллегами из компании Baidu для его

уничтожения. 14 мая нынешнего года они провели совместную операцию по отключению ряда элементов инфраструктуры ботнета, большая часть которых использовала принадлежащий Baidu сервис для хостинга изображений Tieba. Тем не менее, отключение ботнета является временным, поскольку остальные элементы его инфраструктуры по-прежнему работают». ***(Китайский ботнет DoubleGuns насчитывает миллионы жертв // SecurityLab.ru (https://www.securitylab.ru/news/508676.php). 27.05.2020).***

***

«Издание Bleeping Computer предупреждает, что новая версия трояна AnarchyGrabber ворует пароли и токены пользователей, отключает 2ФА и распространяет малварь среди друзей жертвы. И для всего этого злоумышленники модифицируют официальный клиент Discord.

Как правило, злоумышленники распространяют AnarchyGrabber через Discord, выдавая трояна за игровой чит, хакерский инструмент или пиратский софт. Если жертва клюнула на эту удочку, после установки троян модифицирует JavaScript-файлы клиента Discord, чтобы превратить его в малварь, которая способна похитить токен пользователя. Используя этот токен, хакеры получают возможность войти в Discord под видом своей жертвы.

Однако на прошлой неделе была замечена новая версия AnarchyGrabber, содержащая ряд новых функций. Теперь малварь носит название AnarchyGrabber3, похищает пароли жертв в формате простого текста, а также может использовать зараженный клиент Discord для дальнейшего распространения угрозы среди всех друзей пострадавшего. Отмечается, что похищенные таким способом пароли могут использоваться для взлома учетных записей на других сайтах.

После установки AnarchyGrabber3 использует файл %AppData%\Discord\[version]\modules\discord_desktop_core\index.js клиента Discord для загрузки других JavaScript-файлов, добавленных малварью. Как видно на иллюстрации ниже, при запуске Discord модифицированный скрипт загружает файл с именем inject.js из новой папки 4n4rchy.

Затем этот файл загрузит в клиент другой вредоносный файл — discordmod.js. Эти скрипты разлогинивают пользователя из клиента Discord и предлагают ему войти в приложение заново.

Как только жертва осуществляет вход, модифицированный клиент Discord пытается отключить двухфакторную аутентификацию для учетной записи. Затем клиент использует веб-хук для передачи адреса электронной почты, имени пользователя, токена, обычного текстового пароля и IP-адреса на специальный канал Discord, находящийся под контролем злоумышленников.

После этого «подправленный» клиент Discord ждет дальнейших команд от своих операторов. Одна из них может приказать взломанным клиентам Discord разослать вредоносные сообщения всем друзьям жертвы, содержащее все ту же малварь. Исследователи пишут, что этот компонент облегчает преступникам распространение AnarchyGrabber3, а также может применяться для распространения других типов вредоносных программ.

Издание предупреждает, что основная опасность AnarchyGrabber заключается в том, что большинство его жертв даже не знают о том, что были заражены. Так, после запуска исполняемого файла AnarchyGrabber3 и изменения файлов клиента Discord, троян практически никак не проявляет себя и не запускается снова. То есть вредоносного процесса, который мог бы обнаружить антивирус, попросту нет, а зараженный компьютер все равно остается частью ботнета.

Фактически, единственный способ удалить AnarchyGrabber3 — это удалить клиент Discord и установить его заново». ***(Мария Нефёдова. Хакеры превратили Discord в инструмент для кражи паролей // Хакер (https://xakep.ru/2020/05/27/anarchygrabber/). 27.05.2020).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Европол сообщил, что на прошлой неделе польские и швейцарские правоохранительные органы арестовали пять польских хакеров из группировки Infinity Black. Данная группировка специализировалась на продаже украденных учетных данных и инструментов для взлома.

По данным правоохранителей, группировка существовала с конца 2018 года и была известна главным образом тем, что управляла сайтом Infinity[.]black, где продавались дампы с различными учетными данными. Такие «коллекции» создавались путем агрегации имен пользователей и паролей, утекших в открытый доступ во время различных инцидентов.

…группа имела собственные каналы в Discord, магазины на e-commerce платформе Shoppy.gg, а также ряд «официальных» тем на нескольких хакерских форумах. На этих каналах и форумах участники Infinity Black активно рекламировали свой сайт с дампами, а также различные хакерские инструменты и скрипты для проведения credential stuffing атак.

Также сообщается, что члены Infinity Black и сами использовали подобные хакерские инструменты. Напомню, что под термином credential stuffing обычно подразумеваются ситуации, когда имена пользователей и пароли похищаются с одних сайтов, а затем используются против других. То есть злоумышленники имеют уже готовую базу учетных данных (приобретенную в даркнете, собранную самостоятельно и так далее) и пытаются использовать эти данные, чтобы авторизоваться на каких-либо сайтах и сервисах под видом своих жертв. Именно так использовала свои «сборники» учетных данных Infinity Black.

По информации Европола, в основном группировка атаковала онлайн-сервисы, работающие с различными программами лояльности. С помощью credential stuffing атак участники Infinity Black получали доступ к чужим учетным записям, а затем продавали их другим хакерам, которые впоследствии обменивали чужие баллы лояльности на дорогие электронные устройства.

Швейцарские власти тоже расследуют деятельность группы, так как Infinity Black получила доступ к большому количеству учетных записей, принадлежащих швейцарским пользователям, а затем продала доступ к ним другим злоумышленникам, что привело к финансовым потерям среди граждан страны.

«Хотя потери [пользователей] оцениваются в 50 000 евро, хакеры имели доступ к учетным записям [эксплуатация которых могла повлечь] возможные убытки в размере 610 000 евро, — заявляет Европол. — Мошенники и хакеры, в том числе несовершеннолетние, были разоблачены, когда использовали украденные данные в магазинах Швейцарии».

Сообщается, что во время арестов и обысков в домах подозреваемых польская полиция изъяла электронное оборудование, внешние жесткие диски и аппаратные кошельки для криптовалюты на общую сумму около 100 000 евро.

Полицейские также конфисковали две онлайн-платформы с БД, которые содержали более 170 000 000 украденных учетных данных. Считается, что одной из них была DataSense[.]Pw. Оригинальный же сайт Infinity Black среди них не числится, так как он прекратил работу еще в прошлом году, и его закрыли сами члены группировки.

Судя по всему, лидер хак-группы, известный как Azatej, тоже был арестован. Его отсутствие почти сразу заметили пользователи хак-форумов, где Azatej регулярно бывал и рекламировал хакерские инструменты. Среди других участников Infinity Black есть люди, известные под никами Macien, TheN3RoX и Kay, но пока сложно сказать, кто из них был задержан властями». ***(Мария Нефёдова. Европол сообщил об аресте членов польской хак-группы Infinity Black // Хакер (https://xakep.ru/2020/05/06/infinity-black/). 06.05.2020).***

***

«Сотрудники правоохранительных органов Польши и Швейцарии при содействии Европола и Евроюста пресекли деятельность киберпреступной группировки InfinityBlack, занимавшейся продажей похищенных учетных данных, созданием и распространением вредоносного ПО и хакерских инструментов, а также мошенничеством.

29 апреля 2020 года сотрудники польской полиции провели шесть обысков в пяти регионах страны и арестовали пятерых предполагаемых участников InfinityBlack. В ходе обысков было изъято электронное оборудование, внешние жесткие диски и аппаратные криптовалютные кошельки, содержащие порядка €100 тыс. каждый. Также были отключены две платформы с базами данных, насчитывающими более 170 млн входов.

Основным источником дохода InfinityBlack являлась кража учетных данных участников программ лояльности и продажа их другим, менее технически подкованным преступным группировкам, которые обменивали заработанные в программе лояльности баллы на дорогие электронные устройства.

Группировка была поделена на три команды, и каждая из них выполняла свои задачи. Разработчики занимались созданием инструментов для проверки качества похищенных баз данных, тестировщики проверяли соответствие данных, а

руководители проектов распространяли подписки на программы лояльности за криптовалюту.

Хакеры написали сложный скрипт, с помощью которого им удалось получить доступ к большому количеству учетных записей пользователей в Швейцарии. Хотя размер ущерба оценивается в €50 тыс., у злоумышленников был доступ к учетным записям с потенциальными потерями в размере более €610 тыс». ***(Полиция ликвидировала киберпреступную группировку InfinityBlack // SecurityLab.ru (https://www.securitylab.ru/news/508075.php). 06.05.2020).***

***

«…румынские правоохранители прекратили деятельности хакерской группы PentaGuard, которая намеревалась заразить больницы страны вымогательским ПО. Трое подозреваемых были арестованы в Румынии, и еще один в Республике Молдова.

По данным ИБ-компании KELA, группировка PentaGuard существует примерно с 2000 года. В частности, в то далекое время злоумышленники участвовали в массовом дефейсе (1, 2) нескольких правительственных и военных сайтов, включая румынский сайт Microsoft.

В последние годы группировка избегала подобных атак и не привлекала к себе внимания, но сохраняла активность на хакерских форумах и вновь попала в поле зрения специалистов в январе 2020 года, когда вновь стала практиковать дефейсы

Румынское Управление по борьбе с организованной преступностью и терроризмом заявляет, члены группы имели в своем распоряжении такую малварью, как трояны и вымогатели, инструменты для дефейса сайтов и эксплуатации SQL-инъекций, которые обычно используются для взлома веб-серверов и хищения данных.

Правоохранители и сотрудники румынских спецслужб убеждены, что в ближайшее время хакеры из PentaGuard намеревались разослать сотрудникам больниц фишинговые письма, якобы содержащие важную информацию о COVID-19, чтобы заразить компьютеры медицинских учреждений шифровальщиками и нарушить их работу.

Местные СМИ, со ссылкой на собственные источники в полиции, пишут, что эти атаки должны были стать своеобразной формой протеста хакеров, которые выступают против карантинных мер, введенных в стране из-за пандемии коронавируса». ***(Мария Нефёдова. В Румынии арестовали хак-группу PentaGuard, готовившую вымогательские атаки на больницы // Хакер (https://xakep.ru/2020/05/18/pentaguard-arrested/). 18.05.2020).***

***

«Американские правоохранители сообщил об аресте и экстрадиции из Таиланда гражданина Украины Дениса Ярмака, также известного под псевдонимом GakTus. По данным американских властей, Ярмак был членом известной хак-группы FIN7.

Напомню, что группа FIN7 активна с середины 2015 года. Группировка подозревается в атаках на американские компании из сегмента ритейла, а также ресторанно-гостиничного бизнеса. Также FIN7 долгое время активно сотрудничала с группой Carbanak: злоумышленники обменивались инструментами и методами атак, в результате чего многие эксперты ставили между группировками своеобразный «знак равенства».

Преступников из FIN7 интересует, прежде всего, финансовая информация, например, данные о платежных картах или учетные данные для доступа к компьютерам финансовых департаментов. Получив необходимые сведения, злоумышленники крадут деньги и переводят их на оффшорные счета.

Согласно данным Министерства юстиции США, с 2015 года группировка атаковала более 100 компаний и организаций на территории США, взломав тысячи различных систем. Только в США хакеры похитили свыше 15 000 000 платежных карт, скомпрометировав более 6500 PoS-терминалов. Затем эти данные перепродавались в даркнете третьим лицам.

При этом нельзя забывать, что группировка также действовала и в других странах, включая Великобританию, Австралию, Францию, и от атак FIN7 пострадали такие крупные компании, как Chipotle Mexican Grill, Chili's, Arby's, Red Robin, Jason's Deli. Напомню, что по данным «Лаборатории Касперского», по данным на 2015 год группировке суммарно удалось похитить около миллиарда долларов.

Согласно судебным документам, Денис Ярмак, как и другие участники группировки, раскрыл свое настоящее имя, чтобы получить оплату за «работу» в FIN7. В логах чатов, датированных 2017 годом, Ярмак передает другому члену FIN7 учетные данные пользователя из скомпрометированной компании в США, а также внутреннюю системную информацию о жертве и ряд документов.

Американские власти получили ордер на доступ к аккаунту Ямарка в Gmail, где содержались фотографии его украинских паспортов и другие документы, удостоверяющие личность.

«В ходе расследования было установлено, что одним из методов работы группировки была проверка их вредоносных программ антивирусами, отключенными от интернета. Этот метод позволял определить, определяется ли вредоносная программа антивирусным продуктом как вредоносная, но без предоставления копии малвари антивирусным компаниям», — отмечается в судебном документе.

Еще одна бумага из суда, датированная 20 мая 2020 года, сообщает, что в настоящее время власти стремятся скрыть информацию еще об одном человеке, который сейчас тоже находится под следствием и с которым Ярмак общался в прошлом году…». ***(Мария Нефёдова. Власти США арестовали еще одного участника хак-группы FIN7 // Xakep (https://xakep.ru/2020/05/28/fin7-arrest/). 28.05.2020).***

***

«Специалист Технического университета Эйндховена в Нидерландах продемонстрировал новый метод атаки на компьютеры на базе Windows или Linux с поддержкой порта Thunderbolt, позволяющий взломать устройства менее чем за пять минут.

С помощью новой техники, получившей название Thunderspy, возможно обойти экран авторизации (и даже шифрование жесткого диска) на заблокированных или находящихся в режиме сна компьютерах, изменить настройки безопасности и получить доступ к данным на устройстве. Хотя в большинстве случаев для эксплуатации уязвимости потребуется вскрыть корпус ПК, атака не оставляет следов и занимает всего несколько минут, пояснил автор метода Бьорн Руйтенберг (Björn Ruytenberg).

Новый метод относится к типу атак известных как «evil maid» («злая горничная»), в которых злоумышленник, имеющий физический доступ к ПК, может обойти локальную аутентификацию. По словам Руйтенберга, пока единственным способом защититься от атаки Thunderspy является отключение порта Thunderbolt.

После выхода доклада об атаке Thunderclap, позволяющей украсть информацию непосредственно из памяти ОС с помощью периферийных устройств, компания Intel представила механизм безопасности Kernel DMA Protection, который блокирует подключенные устройства Thunderbolt 3 и не дает им доступа к функции Direct Memory Access до момента, пока не будут выполнен определенный набор процедур.

Данная функция предотвращает атаку Thunderspy, однако проблема заключается в том, что этот механизм отсутствует в ПК, выпущенных до 2019 года, поясняет исследователь. Более того, многие произведенные до 2019 года периферийные устройства Thunderbolt не поддерживают данную технологию.

Специалисты изучили несколько моделей ПК Dell, HP и Lenovo и обнаружили, что в ПК Dell отсутствует функция Kernel DMA Protection (в том числе в устройствах, выпущенных после 2019 года), а в случае HP и Lenovo только несколько моделей используют технологию. Уязвимость не затрагивает компьютеры на базе Apple macOS.

По словам представителей HP, в «большинстве коммерческих ПК мобильных рабочих станций HP с поддержкой Sure Start Gen5 и выше» реализована защита от атак Thunderspy. В Lenovo сообщили, что изучают ситуацию.

Thunderbolt — технология периферийного подключения, разработанная Intel совместно с Apple, которая позволяет передавать данные, видео, аудио и электроэнергию через один порт.

HP Sure Start — технология, разработанная компанией HP (Hewlett-Packard) для защиты BIOS компьютера. Отвечает за безопасность BIOS и включает функцию Dynamic Protection, которая проверяет BIOS не только при изменении состояния устройства, но также в течение дня с регулярными інтервалами». ***(ПК с поддержкой Thunderbolt можно взломать менее чем за 5 минут // SecurityLab.ru (https://www.securitylab.ru/news/508172.php). 11.05.2020).***

***

«Специалисты Университета имени Давида Бен-Гуриона в Негеве (Израиль) продемонстрировали способ похищения данных с физически изолированной системы через блок питания. В ходе атаки POWER-SUPPLaY ученым удалось превратить блок питания компьютера в аудиоколонку, способную незаметно передавать данные с атакуемого хоста посредством звуковых волн.

По словам руководителя исследования Мордехая Гури, POWER-SUPPLaY позволяет похищать данные с устройств, лишенных динамиков. С помощью специально разработанного вредоносного ПО исследователи превратили блок питания компьютера в примитивную аудиоколонку, генерирующую базовые звуковые волны. Следует отметить, что целью исследования было лишь изучить способ извлечения данных с физически изолированной системы, но не способы ее заражения вредоносным ПО.

Как пояснил Гури, атакующий может управлять электрическим током в конденсаторах блока питания и вызывать явление, известное как «поющий» конденсатор. При данном феномене конденсатор генерирует звуковые волны, когда через него проходит переменный ток с разной частотой. Управляя частотой переменного тока, вредоносное ПО может управлять звуковыми волнами и благодаря этому прятать в них данные.

Принимать генерируемые «поющим» конденсатором звуковые сигналы может расположенный неподалеку приемник (например, смартфон). Устройство декодирует сигнал и по интернету передаст перехваченные данные злоумышленнику.

Отличительная черта POWER-SUPPLaY – вредоносное ПО не требует никаких особых привилегий. Атака работает на ПК, серверах, встроенных системах и IoT-устройствах без радиоэлементов. Минусы атаки – медленная передача данных, невозможность передачи данных на большие расстояния (максимальное расстояние составляет 6 м) и влияние фонового шума на качество звуковых волн.

«Пение» конденсатора – одно из описаний пьезоэлектрического эффекта. На самом деле является вибрацией конденсатора на печатной плате, вызывающей слабый шум.

Пьезоэлектрический эффект – эффект возникновения поляризации диэлектрика под действием механических напряжений». ***(Похитить данные с физически изолированного ПК можно через его блок питания // SecurityLab.ru (https://www.securitylab.ru/news/508059.php). 05.05.2020).***

***

«Группа немецких и итальянских ученых разработали новую атаку, позволяющую обойти разделение между технологиями Wi-Fi и Bluetooth, используемыми на одном устройстве (смартфоне, ноутбуках и планшетах). Атака, получившая название Spectra, работает на «комбинированных» чипах, обрабатывающих различные виды беспроводной связи, в том числе Wi-Fi, Bluetooth, LTE и пр.

«Новый класс уязвимостей Spectra базируется на том факте, что передача данных происходит в одном спектре, и беспроводные чипы должны разрешать доступ к каналу», - сообщили исследователи в коротком анонсе своего будущего доклада на конференции Black Hat.

Если говорить точнее, Spectra базируется на механизме сосуществования, используемом «комбинированными» чипами для быстрого переключения между беспроводными технологиями. По словам исследователей, хотя эти механизмы повышают производительность, они также делают устройство уязвимым к атакам по сторонним каналам.

Ученые проанализировали «комбинированные» чипы Broadcom и Cypress, используемые в миллионах устройств, в том числе в iPhone, MacBook и смартфонах серии Samsung Galaxy S. Им удалось убрать барьер между Wi-Fi и Bluetooth, обрабатывающимися отдельными ядрами ARM. Они атаковали чип с помощью вредоносного беспроводного трафика, а затем «сломали» границы между двумя беспроводными технологиями.

Результаты атаки могут быть разными. Если коротко, Spectra позволяет осуществить DDoS-атаку на доступ к спектру. Метаданные о пакете позволяют раскрывать информацию, такую как время нажатия клавиш на Bluetooth-клавиатуре в ядре Wi-Fi D11.

Исследователи также идентифицировали область общего ОЗУ, позволяющую выполнять код через Bluetooth в Wi-Fi. Это приравнивает удаленное выполнение кода через Bluetooth к удаленному выполнению кода через Wi-Fi, что значительно увеличивает поверхность атаки.

Хотя в исследовании изучались чипы Broadcom и Cypress, по словам ученых, Spectra может затрагивать и другие устройства. Подробности об атаке пока не публикуются. Доклад исследователей будет представлен на online-конференции Black Hat в августе». ***(Эксперты «сломали» барьер между Wi-Fi и Bluetooth // SecurityLab.ru (https://www.securitylab.ru/news/508585.php). 22.05.2020).***

***

«Дослідники фірми F-Secure, яка спеціалізується на кібербезпеки, створили алгоритм, який зміг зламати майже половину тестів CAPTCHA (які перевіряють, не використовує програму або програми комп'ютер замість людини) в поштовому сервісі Microsoft Outlook. Це означає, що система є ненадійною, адже вона була створена щоб протистояти напливу “ботів” на різних сервісах, але тепер самі боти здатні ламати цю систему.

Сам злом зробили з допомогою нейронної мережі, яка здатна навчатися і покращувати свою систему з кожним разом. Якщо на початку розробки нейромережа могла пройти лише 20% від усіх випадків захисту, то тепер кожна друга “капча” піддається злому». ***(Николай Олефиренко. Експерти з безпеки навчили робота зламувати CAPTCHA, система захисту перетворилася на небезпеку // Знай.ua (https://techno.znaj.ua/313359-eksperti-z-bezpeki-navchili-robota-zlamuvati-captcha-sistema-zahistu-peretvorilasya-na-nebezpeku). 26.05.2020).***

***

«Команда китайских исследователей нашла новый способ усиления HTTP-трафика для выведения из строя web-сайтов и сетей доставки контента (CDN). Представленная ими DoS-атака под названием RangeAmp базируется на некорректной реализации HTTP-атрибута Range Requests.

Запросы Range являются частью стандарта HTTP и позволяют клиенту (как правило, браузеру) запрашивать у сервера только определенную часть (диапазон) файлов. Данная функция была создана для приостановки и возобновления трафика в контролируемых (пауза/возобновление действия) или неконтролируемых (перегрузка или отключение сети) ситуациях.

По словам китайских исследователей, с помощью вредоносных запросов Range злоумышленник может усиливать ответную реакцию серверов и CDN. У атаки RangeAmp есть два варианта. Первый, RangeAmp Small Byte Range (SBR), предполагает отправку вредоносного запроса Range провайдеру сети доставки контента. Это усиливает трафик к целевому серверу и в конечном итоге вызывает отказ в обслуживании атакуемого сайта.

Второй вариант атаки, RangeAmp Overlapping Byte Ranges (OBR), также предполагает отправку вредоносного запроса Range провайдеру сети доставки контента. Однако в данном случае трафик направляется через другие серверы CDN, усиливается внутри сетей доставки контента и вызывает сбой серверов CDN. В результате недоступной становится как сама CDN, так и многие другие сайты.

Из двух вариантов атаки сильнее усиливает трафик вариант SBR. В ходе исследования специалистам удалось усилить трафик в 724-43330 раз. Вариант OBR сложнее в осуществлении и позволяет усилить трафик в 7500 раз. Однако он также является более опасным, поскольку позволяет вывести из строя тысячи сайтов одновременно.

Исследователи протестировали RangeAmp в отношении 13 провайдеров сетей доставки контента и обнаружили, что все они уязвимы к данной атаке. Шесть из них также уязвимы к варианту OBR (при использовании в определенных комбинациях).

Специалисты в должном порядке уведомили провайдеров CDN об уязвимости, и 12 из 13 исправили ее. В список исправивших входят: Akamai, Alibaba Cloud, Azure, Cloudflare, CloudFront, CDNsun, CDN77, Fastly, G-Core Labs, Huawei Cloud, KeyCDN и Tencent Cloud. От провайдера StackPath исследователи не смогли добиться никакого ответа». ***(DoS-атака RangeAmp способна вывести из строя тысячи сайтов одновременно // SecurityLab.ru (https://www.securitylab.ru/news/508637.php). 26.05.2020).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Эксперты компании F-Secure обнаружили две критические уязвимости в опенсорсном фреймворке SaltStack Salt, широко использующемся в дата-

центрах и облачных серверах. Обе проблемы набрали 10 баллов из 10 возможных по шкале оценки уязвимостей CVSS и обе допускают удаленное выполнение произвольного кода.

Уязвимости получили идентификаторы CVE-2020-11651 и CVE-2020-11652, и позволяют злоумышленнику выполнить произвольный код на удаленных серверах в дата-центрах и облачных средах.

Так, одна уязвимость представляет собой обход аутентификации: неаутентифицированным сетевым клиентам по ошибке предлагалась полная функциональность. В некоторых случаях атакующий мог даже получить токен для доступа с правами root к master-серверу и выполнять произвольные команды на серверах с активным демоном salt-minion.

Второй баг — это обход каталога, возникший из-за некорректной очистки недоверенных входных данных, что в результате обеспечивало неограниченный доступ ко всей файловой системе сервера с root-правами. Для использования уязвимости необходима аутентификация, но получить ее можно через эксплуатацию проблемы CVE-2020-11651.

Разработчики SaltStack Salt уже устранили найденные специалистами проблемы, выпустив версии 2019.2.4 и 3000.2, но исследователи F-Secure отмечали, что в сети доступно более 6000 потенциально уязвимых систем, и все они могут не успеть обновиться вовремя.

Хотя специалисты F-Secure не обнародовали PoC-эксплоиты для этих проблем, они предупреждали, что, скорее всего, злоумышленники без труда создадут надежные экплоиты самостоятельно уже в ближайшие дни, так как эксплуатация багов весьма проста. К сожалению, именно так и произошло. К настоящему моменту в сети уже появилось немало PoC-эксплоитов, и при помощи уязвимостей в SaltStack Salt были атакованы блогинговая платформа Ghost, удостоверяющий центр Digicert, серверы LineageOS и так далее. Известно, что в некоторых случаях злоумышленники устанавливают бэкдоры на взломанные серверы, в других случаях разворачивают на серверах майнеры». ***(Мария Нефёдова. Уязвимости в SaltStack Salt поставили под угрозу множество дата-центров // Хакер (https://xakep.ru/2020/05/06/saltstack-salt-rces/). 06.05.2020).***

***

«Исследователи безопасности из компании VPNpro проанализировали 20 самых популярных VPN-сервисов и обнаружили, что две из них содержат уязвимости, которые злоумышленники могут проэксплуатировать для перехвата соединение с целью отправки поддельных обновлений и установки вредоносных программ или кражи пользовательских данных.

PrivateVPN, Betternet, TorGuard и CyberGhost позволяли осуществить перехват подключения, однако только PrivateVPN и Betternet позволяли злоумышленникам отправлять поддельные обновления. PrivateVPN автоматически выполняла установку обновления, а Betternet только предлагала пользователю сделать это.

По словам специалистов, преступник мог с помощью MitM-атаки перехватить контроль над VPN-соединением целевого пользователя и отправить

поддельное обновление программного обеспечения. В наиболее вероятных сценариях злоумышленник обманом мог убедить жертву подключиться к вредоносной сети Wi-Fi в общедоступном месте или каким-нибудь образом получить доступ к целевому маршрутизатору.

Поддельное обновление программного обеспечения могло привести к установке вредоносного ПО на устройстве жертвы, в том числе вымогателей, инфостиллеров или майнеров криптовалюты.

Эксперты сообщили командам PrivateVPN и Betternet о своих находках в середине февраля, и они выпустили исправления для данных уязвимостей». ***(Популярные VPN-сети подвергали пользователей риску кибератак // SecurityLab.ru (https://www.securitylab.ru/news/508139.php). 07.05.2020).***

***

«Исследователи из команды Trend Micro Zero Day Initiative (ZDI) опубликовали информацию о пяти неисправленных уязвимостях в Windows, четыре из которых имеют высокую степень риска.

Три уязвимости нулевого дня, получившие идентификаторы CVE-2020-0916, CVE-2020-0986 и CVE-2020-0915, набрали 7 баллов из 10 возможных по шкале оценки уязвимостей CVSS. По сути, три эти проблемы могут позволить злоумышленнику повысить свои привилегии в уязвимой системе до уровня текущего пользователя. К счастью, злоумышленникам, которые решат эксплуатировать эти баги, сначала придется получить низко привилегированный доступ к целевой системе.

Корень этих проблем заключается в хост-процессе драйвера принтера splwow64.exe, работающем в user-mode: предоставляемые пользователем входные данные не проходят должной валидации перед разыменованием указателя.

Тот же процесс splwow64.exe подвержен еще одной, менее серьезной проблеме, отслеживаемой как CVE-2020-0915. Уязвимость набрала лишь 2,5 балла по шкале CVSS и тоже возникает из-за отсутствия должной валидации предоставляемых пользователем данных.

Эксперты пишут, что уведомили Microsoft об этих проблемах еще в декабре 2019 года, и компания намеревалась включить патчи для них в состав майского «вторника обновлений». Однако уложиться в этот срок инженеры компании не сумели, и пока исследователям ZDI были предоставлены лишь бета-версии патчей для тестирования, а конечные пользователи исправлений не получали.

Еще одну уязвимость, которая не имеет идентификатора CVE, специалисты ZDI выявили в январе текущего года. Этот баг так же позволяет злоумышленникам повышать свои привилегии и связан с тем, как система обрабатывает профили подключений WLAN. Исследователи считают, что этот баг можно оценить примерно на 7 баллов по шкале CVSS. В данном случае хакеру тоже сначала придется получить доступ к целевой системе, и лишь потом эксплуатировать проблему.

«Создав вредоносный профиль, злоумышленник может узнать учетные данные для учетной записи компьютера. Атакующий может использовать эту

уязвимость для повышения своих привилегий и выполнения кода в контексте администратора», — пишут эксперты.

Интересно, что инженеры Microsoft вообще не намерены исправлять эту проблему, во всяком случае, не в ближайшем будущем». ***(Мария Нефёдова. Эксперты Zero Day Initiative рассказали о пяти 0-day уязвимостях в Windows // Xakep (https://xakep.ru/2020/05/20/windows-0days-3/). 20.05.2020).***

***

«Эксперты рассказали о новой проблеме в протоколе Bluetooth, получившей название BIAS (Bluetooth Impersonation AttackS). Баг получил идентификатор CVE-2020-10135 и представляет угрозу для классической версии Bluetooth, она же Basic Rate/Enhanced Data Rate, Bluetooth BR/EDR или просто Bluetooth Classic.

В сводную команду исследователей вошли ученые из Швейцарского федерального технологического института в Лозанне (EPFL), Центра информационной безопасности имени Гельмгольца в Германии (CISPA), а также из Оксфордского университета.

Стоит отметить, что летом 2019 года эти же люди рассказали миру о другой Bluetooth-уязвимости, KNOB (CVE-2019-9506).

Корень новой проблемы BIAS заключается в том, как устройства с поддержкой Bluetooth обрабатывают ключ связи (link key), также известный как долгосрочный ключ. Данный ключ генерируется, когда два Bluetooth-устройства впервые соединяются (сопрягаются). По сути, они «договариваются» о долгосрочном ключе, который будут использовать для получения ключей сессий в будущем, чтобы не вынуждать владельцев устройств каждый раз вновь проходить длительный процесс сопряжения.

Исследователи объясняют, что обнаружили проблему в процессе аутентификации после сопряжения девайсов. Данный баг позволяет злоумышленнику выдать себя за ранее сопряженное устройство, пройти аутентификацию и подключиться к другому устройству, не зная ключа связи, который ранее был установлен между ними.

По сути, осуществив атаку BIAS, злоумышленник может получить доступ к другому устройству с поддержкой Bluetooth Classic или даже перехватить контроль над ним.

Эксперты опробовали свою атаку против широкого спектра устройств, включая смартфоны (iPhone, Samsung, Google, Nokia, LG, Motorola), планшеты (iPad), ноутбуки (MacBook, HP Lenovo), наушники (Philips, Sennheiser) и одноплатные компьютеры (Raspberry Pi, Cypress). Все проверенные устройства оказались уязвимы перед BIAS.

«Поскольку эта атака затрагивает практически все устройства “говорящие по Bluetooth”, в декабре 2019 года мы провели ответственное раскрытие проблемы и привлекли к делу Bluetooth Special Interest Group (Bluetooth SIG) — организацию по стандартизации, которая контролирует разработку стандартов Bluetooth, — чтобы убедиться, что будут созданы и применены средства для обхода уязвимости», — говорят эксперты.

Специалисты Bluetooth SIG уже выпустили собственный пресс-релиз, в котором уверяют, что базовая спецификация Bluetooth была обновлена: злоумышленники не смогут осуществить даунгрейд Bluetooth Classic и понизить соединение с надежного метода аутентификации (secure) до legacy, что и делало атаку BIAS возможной.

Стоит отметить, что, по словам экспертов, если объединить BIAS с упомянутой выше проблемой KNOB, атакующий сможет нарушить аутентификацию даже на устройствах Bluetooth Classic, работающих в режиме надежной аутентификации. То есть для полной безопасности необходимы патчи для обеих проблем.

Ожидается, что в ближайшие месяцы производители Bluetooth-устройств выпустят обновления своих прошивок, устраняющие проблему. Однако статус и доступность этих патчей в настоящее время неясны даже для самих представителей исследовательской группы». ***(Мария Нефёдова. Bluetooth-атака BIAS угрожает устройствам с прошивками Apple, Broadcom, Cypress, Intel, Samsung // Xakep (https://xakep.ru/2020/05/19/bias/). 19.05.2020).***

***

«Аналитики ФБР и Агентства по кибербезопасности и защите инфраструктуры, организованного при Министерстве внутренней безопасности США (DHS CISA), подготовили список самых эксплуатируемых уязвимостей за период с 2016 по 2019 год.

Исследователи в очередной раз призвали организации в государственном и частном секторах своевременно устанавливать необходимые патчи для предотвращения наиболее распространенных форм атак. Дело в том, что власти США уверены: массовая установка исправлений может больно ударить киберарсеналу иностранных хакеров, нацеленных на американские компании, ведь тогда взломщикам придется тратить ресурсы на разработку новых эксплоитов.

«Эксплуатация этих уязвимостей, как правило, требует намного меньше ресурсов по сравнению с эксплоитами для 0-day уязвимостей, для которых нет доступных патчей», — пишут эксперты в своем докладе.

Также аналитики CISA и ФБР отмечают следующие тенденции:

- чаще всего атакам подвергается технология Microsoft's Object Linking and Embedding (OLE), позволяющая встраивать контент из других приложений в документы Office;
- уязвимости OLE, такие как CVE-2017-11882, CVE-2017-0199 и CVE-2012-0158, чаще всего используются «правительственными» хакерами Китая, Ирана, Северной Кореи и России;
- второй наиболее уязвимой технологией был назван Apache Struts;
- наиболее используемыми уязвимостями в 2020 году стали CVE-2019-19781 (баг в Citrix VPN) и CVE-2019-11510 (баг в серверах Pulse Secure VPN);
- из-за пандемии коронавируса многие организации перешли на удаленную работу и неправильно настроили развертывание Office 365.

Что до списка 10 наиболее используемых уязвимостей 2016-2019 годов, в него вошли следующие баги: CVE-2017-11882, CVE-2017-0199, CVE-2017-5638,

CVE-2012-0158, CVE-2019-0604, CVE-2017-0143, CVE-2018-4878, CVE-2017 -8759, CVE-2015-1641 и CVE-2018-7600…» ***(Мария Нефёдова. Власти США опубликовали список самых эксплуатируемых уязвимостей // Xakep (https://xakep.ru/2020/05/14/most-targeted-cve/). 14.05.2020).***

***

«**ИБ-специалисты Алекс Ионеску и Ярден Шафир опубликовали информацию об уязвимости PrintDemon, которая связана со службой печати в Windows. По словам исследователей, эта проблема затрагивает все версии ОС, начиная с Windows NT 4, выпущенной в далеком 1996 году.** На GitHub уже доступен PoC-эксплоит для PrintDemon.

Корень проблемы PrintDemon кроется в компоненте Windows Print Spooler, который управляет операциями печати в Windows. Служба используется для отправки данных для печати на USB или параллельный порт (для физически подключенных принтеров), на порт TCP (для принтеров, находящихся в локальной сети или в интернете), или в локальный файл (в тех редких случаях, когда пользователь хочет сохранить задание на печать на будущее).

Эксперты пишут, что обнаруженную ими ошибку можно использовать для компрометации механизма Printer Spooler. По сути, PrintDemon представляет собой уязвимость локального повышения привилегий (LPE). То есть проблему нельзя использовать для удаленной компрометации через интернет, а значит, к счастью, можно не опасаться волны удаленных атак на Windows-системы.

Эксплуатация PrintDemon позволяет атакующему, который ранее имел хоть какую-то «точку опоры» в системе, получить привилегии администратора. Поскольку служба Print Spooler доступна любому приложению, которое хочет напечатать файл, она доступна для всех приложений, работающих в системе, без ограничений.

Злоумышленник может создать задание на печать, которое печатает «в файл», например, локальный DLL, используемый ОС или другим приложением. В итоге получится инициировать операцию печати, «уронить» при этом Print Spooler, а затем возобновить работу, но теперь операция печати будет выполняться с привилегиями SYSTEM и позволит перезаписывать любые файлы в произвольном месте.

Ионеску отмечает у себя в Twitter, что для эксплуатации бага в текущих версиях Windows требуется всего одна строка PowerShell. В более старых версиях ОС атака может потребовать чуть больших усилий.

«В непропатченной системе это позволит установить устойчивый бэкдор, который не исчезнет *даже после установки патча*», — подчеркивает эксперт.

Как можно понять по сообщению исследователя, исправление для этой проблемы уже доступно. Патч для уязвимости PrintDemon вошел в состав майского «вторника обновлений» от Microsoft, а сама уязвимость получила идентификатор CVE-2020-1048.

Стоит отметить, что первыми этот баг заметили эксперты компании SafeBreach Labs, и они же сообщили о ней в Microsoft. Исследователи представят собственный доклад по этому вопросу на конференции Black Hat, которая

состоится в августе текущего года». ***(Мария Нефёдова. Уязвимость PrintDemon опасна для всех версий Windows, выпущенных после 1996 года // Xakep (https://xakep.ru/2020/05/14/printdemon/). 14.05.2020).***

***

«Майский «вторник обновлений» стал третьим по объему за все время, так как в его рамках было исправлено 111 уязвимостей (13 из которых были критическими и еще 91 баг получил статус важного) в различных продуктах, от Edge до Windows, от Visual Studio до .NET Framework.

Напомню, что предыдущие «рекорды» тоже зафиксированы в этом году: 115 ошибок были устранены в марте 2020 года, а в апреле 2020 года инженеры компании исправили 113 багов.

Если в последние месяцы Microsoft регулярно выпускала обновления для уязвимостей нулевого дня, уже находившихся под атаками, в этом месяце обошлось без подобных проблем. Тем не менее, откладывать обновления на абстрактное «потом» все же не стоит, так как майский набор патчей содержит исправления для весьма серьезных багов. Так, наиболее опасными из них можно назвать:

CVE-2020-1023, CVE-2020-1024 и CVE-2020-1102: RCE-уязвимости в Microsoft SharePoint;

CVE-2020-1067: RCE-уязвимость в Windows;

CVE-2020-1064: RCE-уязвимость в движке MSHTML;

CVE-2020-1096: RCE-уязвимость в Microsoft Edge PDF Reader;

CVE-2020-1051, CVE-2020-1174, CVE-2020-1175 и CVE-2020-1176: RCE-уязвимости в движке Jet Database;

CVE-2020-1056: эскалация привилегий в Edge.

Патчи для своих продуктов недавно представили и другие компании, включая Adobe (патчи вышли для Acrobat, Reader и DNG SDK), SAP (6 уязвимостей, набравшие 9 и более баллов по шкале CVSS), VMWare (обновление VMware vRealize Operations Manager).

Также стоит отметить, что майские обновления для Android начали распространяться на устройства пользователей еще на прошлой неделе, и тогда же был выпущен обновленный Firefox 76 и обновления безопасности для Google Chrome.» ***(Мария Нефёдова. Microsoft исправила 111 уязвимостей в своих продуктах // Xakep (https://xakep.ru/2020/05/13/may-paches/). 13.05.2020).***

***

«Тайваньский исследователь безопасности Генри Хуань опубликовал подробности о трех уязвимостях (CVE-2019-7192, CVE-2019-7194 и CVE-2019-7195) в прошивке сетевых хранилищ (NAS) QNAP. Проблемы содержатся в приложении для создания фотоальбомов Photo Station, которое поставляется со всеми последними версиями систем QNAP. Эксплуатация уязвимостей позволяет злоумышленнику перехватить контроль над устройствами.

Как сообщил специалист, приложение Photo Station установлено примерно на 80% всех сетевых хранилищ QNAP, что по результатам поисковых запросов Shodan составляет примерно 450 тыс. устройств.

Хуань опубликовал технические сведения о трех из четырех уязвимостей, обнаруженных им в устройствах QNAP. Три из них затрагивают приложение Photo Station, а четвертая (CVE-2019-7193) — приложение файлового менеджера QTS. Все проблемы получили оценку в 9,8 балла по шкале CVSS.

Три уязвимости в Photo Station можно объединить в цепочку с целью обойти аутентификацию, внедрить вредоносный код в PHP-сессию приложения, а затем установить web-оболочку на уязвимых устройствах. Поскольку Photo Station работает с привилегиями суперпользователя, злоумышленники могут использовать данные уязвимости для перехвата контроля над сетевыми хранилищами QNAP.

Эксперт сообщил о своих находках QNAP в июне прошлого года, и в ноябре компания выпустила исправления, устраняющие уязвимости». ***(Около 450 тыс. сетевых хранилищ QNAP уязвимы ко взлому // SecurityLab.ru (https://www.securitylab.ru/news/508502.php). 20.05.2020).***

***

«Сотрудники норвежской фирмы кибербезопасности Promon нашли в системе Androis уязвимость, позволяющую похищать пользовательские данные — логины/пароли, файлы, журналы текстовых чатов и пр., путём создания вредоносной надстройки над нормальными приложениями, перехватывающей входящую информацию от пользователя.

Подробные сведения об этой недоработке, получившей название StrandHogg 2.0, фирма Promon опубликовала через две недели, после того, как Google выпустила соответствующий патч, включив его в состав планового майского обновления для Android.

Предыдущая уязвимость Android от которой унаследовано имя StrandHogg, была замечена в прошлом году. «Версия 2.0» считается более опасной, поскольку, в отличие от тёзки, она может эксплуатироваться хакерским приложением без получения каких-либо разрешений от операционной системы. Кроме того её труднее выявить средствами безопасности.

StrandHogg 2.0 представляет опасность для Android Pie 2018 года выпуска и всех предыдущих версий, которые в настоящее время работают примерно на 90% всех мобильных устройств на базе Android. Исследователи не располагают свидетельствами того, что StrandHogg 2.0 кем-либо использовалась в преступных целях, но теперь, после раскрытия информации о ней, рекомендуют всем затронутым данной угрозой как можно скорее установить майский патч Google». ***(StrandHogg 2.0 позволяет похищать данные, вводимые в Android-приложения // Компьютерное Обозрение (https://ko.com.ua/strandhogg_2_0_pozvolyaet_pohishhat_dannye_vvodimye_v_android-prilozheniya_133166). 27.05.2020).***

***

«Пакет экспертизы для выявления сетевых аномалий при удаленной работе получил второе обновление. Теперь он покрывает еще пять сценариев, среди которых случаи подозрительной активности в сети при организации удаленного доступа с помощью межсетевого экрана Palo Alto Networks.

По результатам опроса специалистов по ИТ и ИБ, проведенного Positive Technologies , межсетевой экран Palo Alto Networks входит в пятерку наиболее популярных способов организации удаленного доступа в крупных компаниях. Поэтому специалисты Positive Technologies разработали правила обнаружения угроз, актуальные для такой системы, и загрузили их в MaxPatrol SIEM.

Теперь MaxPatrol SIEM выявляет атаки методом перебора на подсистему VPN межсетевого экрана Palo Alto (это может помешать злоумышленникам завладеть паролем для подключения в корпоративную сеть) и обнаруживает дублирующиеся VPN-подключения к межсетевому экрану, что свидетельствует о нелегитимном доступе.

Для тех компаний, в которых удаленный доступ организован с помощью межсетевого экрана Palo Alto или других популярных firewall, актуален сценарий выявления прямых VPN-подключений между двумя клиентскими узлами. Такая подозрительная активность в числе прочего свидетельствует о том, что устройство сотрудника скомпрометировано из внешней сети.

«За месяц нам удалось собрать набор правил для выявления аномалий в работе самых популярных систем для организации удаленного доступа: OpenVPN, RDG, межсетевые экраны Cisco ASA, Check Point и Palo Alto, — комментирует Михаил Помзов, директор департамента базы знаний и экспертизы Positive Technologies. — С учетом двух обновлений пакет экспертизы покрывает 16 сценариев».

Обновление пакета экспертизы также актуально для компаний, в которых удаленный доступ организован с помощью Remote Desktop Gateway. Теперь MaxPatrol SIEM выявляет случаи, когда злоумышленники перемещаются внутри сети по RDP: продукт обнаруживает подключения через RDG к сетевому узлу, от которого есть RDP-соединения на другие узлы. Оперативное реагирование на такую активность позволит предотвратить развитие атаки внутри сети.

Еще один новый сценарий, требующий оперативного реагирования и выявляемый с помощью пакета экспертизы, — обнаружение повторных подключений от одного имени пользователя к серверу VPN на базе ОС Windows Server.

28 мая специалисты Positive Technologies расскажут, как правильно настроить пакет экспертизы для безопасной удаленной работы, разберут сценарии выявления аномалий и реагирования на них. Для участия в вебинаре зарегистрируйтесь по ссылке .

[1] В MaxPatrol SIEM доступны 17 пакетов экспертизы, которые содержат 370 правил обнаружения атак. Поставка пакетов экспертизы в MaxPatrol SIEM —

это регулярная автоматизированная передача знаний в области обнаружения инцидентов ИБ в виде алгоритмов, позволяющих выявлять даже сложные нетиповые атаки. Соответствующие наборы правил и рекомендаций формируют эксперты Positive Technologies (R&D и PT Expert Security Center), которые непрерывно анализируют актуальные угрозы, исследуют полный цикл атак и разрабатывают способы их обнаружения. Эти наборы объединяются в пакеты и передаются в базу знаний Positive Technologies Knowledge Base (PT KB), которая входит в состав MaxPatrol SIEM. Далее пользователь может в интерфейсе PT KB выбрать интересующие его пакеты и применить их в рамках своей инсталляции продукта». ***(Пакет экспертизы для безопасной удаленной работы в MaxPatrol SIEM пополнился новыми сценариями // SecurityLab.ru (https://www.securitylab.ru/news/508154.php). 08.05.2020).***

***

«Швейцарская ИБ-компания ImmuniWeb обновила платформу ImmuniWeb Community Edition, позволяющую организациям и предприятиям бесплатно тестировать безопасность своих web-ресурсов, доменов и мобильных приложений. Отныне с помощью сервиса ImmuniWeb Domain Security Test безопасники также могут проверять наличие данных своих компаний в даркнете.

ImmuniWeb Domain Security Test позволяет:

- Осуществлять мониторинг даркнета на предмет наличия в нем данных предприятия;
- Осуществлять мониторинг фишинговых кампаний;
- Осуществлять мониторинг кибersквоттинга;
- Осуществлять мониторинг незаконного использования торговых марок;
- Осуществлять мониторинг поддельных учетных записей в соцсетях.

Для того чтобы проверить упоминание предприятия в даркнете, достаточно лишь ввести основной URL-адрес его сайта в строку поиска ImmuniWeb Domain Security Test и подождать несколько минут. Сервис осуществляет мониторинг постоянно растущих киберпреступных форумов и подпольных торговых площадок, тематических IRC-каналов и Telegram-чатов, paste-сайтов и других ресурсов в так называемой «Глубокой паутине», даркнете и общедоступном интернете, занимающихся рекламой и куплей-продажей похищенных данных.

Чаще всего к таким данным относятся логины и пароли для авторизации на взломанных сайтах, серверах и SaaS-платформах, а также базы данных, исходные коды и документы.

Киберсквоттинг – регистрация доменных имен, содержащих торговую марку, принадлежащую другому лицу с целью их дальнейшей перепродажи или недобросовестного использования». ***(Выпущен бесплатный инструмент для мониторинга наличия данных предприятия в даркнете // SecurityLab.ru (https://www.securitylab.ru/news/508503.php). 20.05.2020).***

***

«Шифрование информации на жестких дисках и облачных хранилищах, веб-трафика, сообщений и паролей позволит обезопасить данные от несанкционированного доступа.

Специалисты международного разработчика антивирусного программного обеспечения, эксперта в области киберзащиты – компании ESET рассказали, как сохранить конфиденциальную информацию от несанкционированного доступа с помощью шифрования. Соответствующая информация содержится на сайте ESET. «Большинство людей хранит на своем персональном компьютере, смартфоне или в облаке все виды конфиденциальной информации. Опытные пользователи, как правило, устанавливают пароль или биометрическую аутентификацию, или даже комбинацию обоих видов защиты учетных записей. Такие меры безопасности являются правильными, однако, их может быть недостаточно в случае потери или кражи устройств. Чтобы быть уверенными, что ваши данные не попадут к посторонним лицам, используйте шифрование», - сообщила пресс-служба компании. Согласно сообщению, значительная часть пользователей все еще использует сменные жесткие диски как дополнительное хранилище. Поэтому шифрование диска — это необходимый уровень безопасности.

«Если вы потеряете свой жесткий диск или его украдут, никто не сможет получить доступ к информации на нем. Диск будет полностью зашифрован, включая все данные, программное обеспечение и операционную систему. Шифрование также доступно на большинстве современных смартфонов Android или iOS и часто является уже встроенной функцией, которую нужно только настроить», - отметили в компании ESET. Также, по данным IT-специалистов, важно шифровать данные перед их загрузкой на облачные хранилища. Таким образом без ключа расшифровки никто не сможет получить доступ к этой информации. «На рынке существует множество, как платных, так и бесплатных программ, однако для более высокого уровня защиты выбирайте программы хотя бы с алгоритмом шифрования AES», - добавили эксперты по кибербезопасности. Пресс-служба сообщила, что в случае шифрования веб-трафика одним из самых простых способов является виртуальная частная сеть (VPN), которая работает как зашифрованный туннель. Для защиты конфиденциальности можно использовать специальные программы, которые позволяют устанавливать анонимное сетевое подключение, например, Tor. Сеть Tor направляет трафик через добровольную сеть ретрансляции и обвертывает ее в несколько уровней шифрования. Кроме этого, следует всегда следить за тем, чтобы веб-сайт, на который вы переходите, использовал протокол HTTPS. Буква S означает, что вся коммуникация между посетителем и веб-сервером зашифрована. Поэтому большинство мировых веб-сайтов сейчас используют HTTPS по умолчанию. Также важным элементов защиты конфиденциальной информации является шифрование сообщений и паролей. Большинство приложений для обмена сообщениями имеют встроенное сквозное шифрование, однако оно не всегда включено по умолчанию. Например, чтобы включить его в Facebook Messenger, нужно начать секретную переписку. В WhatsApp эта функция включена по умолчанию, а в Telegram сквозным шифрованием также защищены только «секретные чаты», в которых можно установить таймер самоуничтожения для сообщений и файлов. Таким образом все

отправленные сообщения будут сами удаляться через определенный промежуток времени. Однако, одним из самых защищенных мессенджеров и дальше считается Signal. Благодаря тому, что он имеет открытый исходный код, ведущие специалисты имели возможность проверить Signal и подтвердить высокий уровень защиты. По данным ESET, шифровать можно также сообщения электронной почты, чтобы защитить их от перехватывания. Смысл такого шифрования заключается в том, что письмо зашифровывается у отправителя, а расшифровывается у получателя. Большинство клиентов электронной почты поддерживают различные стандарты шифрования, например, TSL и S/MIME. В компании добавили, что популярным способом шифрования паролей является менеджер паролей. Эти программы выполняют функцию хранилища, где можно сохранять все данные для входа. Большинство облачных сервисов имеют копию хранилищ пользователей на своих серверах, надежно защищенных несколькими уровнями шифрования. Для дополнительного уровня безопасности пользователи могут использовать многофакторную аутентификацию (MFA). «Ответственный подход к хранению конфиденциальных файлов и данных поможет заблаговременно предупредить утечки важных данных, которые могут вызвать много проблем. Решение ESET Endpoint Encryption обеспечивает надежное шифрование сменных медиа носителей, файлов и папок, а также электронной почты с возможностью управления устройствами из любой точки мира», - подытожили в компании ESET. …ранее специалисты ESET рассказали об обнаруженных уязвимостях в умных устройствах, которые ставят под угрозу безопасность конфиденциальных данных их владельцев. По данным ESET, в Украине ежедневно фиксируется около 300 тыс. новых киберугроз для информационной безопасности. При этом, найти хакеров-злоумышленников крайне сложно, компаниям остается лишь проводить ежеминутные мониторинги на предмет выявления киберугроз с целью их дальнейшего блокирования. Компания ESET – ведущий разработчик решений в области компьютерной безопасности и эксперт в сфере IT-безопасности. Компания была основана в 1992 году в Словакии и на сегодня представлена более, чем в 180 странах мира…» ***(Специалисты по кибербезопасности рассказали, как защитить конфиденциальную информацию от хакеров // УНИАН (https://www.unian.net/science/specialisty-po-kiberbezopasnosti-rasskazali-kak-zashchitit-konfidencialnuyu-informaciyu-ot-hakerov-novosti-11012297.html). 26.05.2020).***

***

«Компания Smarsh, специализирующаяся на облачной архивации данных, за необъявленную сумму купила фирму Endreda, расширив с её помощью свою компетенцию на кибербезопасность и оценку информационных рисков.

Основанная в 2010 г. Entreda среди прочего предлагает удалённый десктоп, автоматические виртуальные приватные сети, мониторинг утечек данных и паролевых политик, антивирусные средства и шифрование устройства. Её платформа кибер-рисков Unity предназначена для оказания помощи регулируемым

отраслям в контроле и защите клиентской информации и активов с обеспечением высокого уровня безопасности.

В число почти 300 клиентов компании входят зарегистрированные инвестиционные консультанты и брокер-дилеры, такие как Advisor Group, компания по управлению активами, насчитывающую в штате более 11 000 финансовых консультантов.

После поглощения, Entreda сохранит свой брэнд и продолжит работу под руководством сооснователь и нынешнего исполнительного директора, Сида Йенамандры (Sid Yenamandra)…». ***(Облачный архиватор Smarsh приобрёл фирму кибербезопасности Entreda // Компьютерное Обозрение (https://ko.com.ua/oblachnyj_arhivator_smarsh_priobryol_firmu_kiberbezopasnosti_entreda_133129). 25.05.2020).***

***

«Компания Citrix Systems анонсировала инструмент App Protection, который позволяет защитить приложения и данные на неуправляемых оконечных устройствах и обеспечить безопасность корпоративных систем и информации.

«Оконечные точки — предпоследний рубеж для защиты устройств, данных и приложений. Ускорение перехода на удаленную работу, вызванное пандемией COVID-19, наряду с быстрым ростом числа неуправляемых персональных устройств, используемых в служебных целях, создали специфическую проблему, ведь децентрализация не дружит с информационной безопасностью, — сказал Фрэнк Диксон (Frank Dickson), вице-президент компании IDC по проектам в сфере безопасности. — И для решения этой проблемы нужны комплексные инструменты».

С ним согласен Дион Хинчклифф (Dion Hinchcliffe), вице-президент и главный аналитик Constellation Research, приглашенный профессор центра цифровых стратегий Школы бизнеса им. Амоса Така: «Недавний массовый переход к удаленной работе частично был реализован благодаря возможности использовать доступные устройства, в том числе неуправляемые. В то же время, открылась новая обширная поверхность для атак на системы кибербезопасности и, соответственно, добавилась нагрузка на сотрудников, адаптирующихся к новым условиям, — отмечает он. — App Protection обеспечивает неоценимую защиту, работники и работодатели могут быть уверены, что удаленные устройства безопасны с точки зрения утечек критичной информации. Каждый может сосредоточиться на главном, выполняя работу на своем безопасном, защищенном цифровом рабочем месте».

Адаптируясь к новым нормам работы из дома, многие работники в разных странах используют любые устройства, которые упрощают им доступ к необходимым для работы ресурсам. Обычно это ноутбуки, планшеты и телефоны. «На таких устройствах распространены вредоносные программы, которые перехватывают клавиатурный ввод и делают снимки экрана, давая злоумышленникам возможность войти в корпоративную сеть и получить ценную информацию», — сказал Эрик Кенни (Eric Kenney), старший менеджер Citrix по маркетингу продуктов.

Установленные на устройстве вредоносные программы перехвата клавиатуры записывают все нажатия на клавиши, включая имена пользователей и их пароли. Программы захвата изображения экрана периодически делают снимки экрана, сохраняя их в скрытой папке на устройстве или сразу передавая на сервер атакующей стороны, где происходит обработка информации. Сервис App Protection позволяет это предотвратить.

App Protection защищает от программ перехвата клавиатуры и снимков экрана, кодируя нажатия клавиш на устройстве и передавая атакующим бессмысленный набор символов, а вместо снимков экрана злоумышленники получают пустые изображения.

После активации App Protection сотрудники могут использовать свои персональные, неуправляемые оконечные устройства, не подвергая риску информационную безопасность компании.» ***(Citrix представила App Protection — инструмент для защиты данных на персональных устройствах // Компьютерное Обозрение (https://ko.com.ua/citrix_predstavila_app_protection_instrument_dlya_zashhity_dannyh_na_personalnyh_ustrojstvah_133123). 25.05.2020).***

***