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

№ 7 (липень)

Київ – 2019

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., 2019. – № 7 (липень) . – 64 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

«Комітет з цифрових технологій в освіті при Міністерстві освіти та науки розробив та доопрацював більше 20 документів в напрямку цифровізації загальної середньої освіти в Україні…

Протягом 2018-2019 навчального року комітет вніс пропозиції до Закону "Про повну загальну середню освіту", в Концепцію розвитку педагогічної освіти, до конкурсного відбору електронних підручників, стандартів цифрової компетентності учнів і педагогічних працівників, тощо.

"Якщо створюються цифрові сервіси в галузі електронного врядування, охорони здоров'я та загалом цифрової економіки, необхідно, щоб суспільство, учні, випускники впевнено володіли цифровими навичками", — говорить Тетяна Нанаєва.

Крім того, експерти комітету доклали зусиль для створення та отримання грифів МОН на два курси програм академій Cisco — "Вступ до кібербезпеки" (17 годин) та "Основи кібербезпеки" (35 годин). Безкоштовне тренінгове навчання з цих курсів на базі Тернопільського національного технічного університету пройшли понад 250 вчителів та викладачів ВНЗ.

Зі свого боку засновник STEM-центру "Сократ" та експерт комітету Сергій Дзюба повідомив, що наразі в рамках громадського проекту розробляються матеріали для вчителів початкової школи з основ кібербезпеки на 16 годин: "Очікується, що навчальні тренінги з кібербезпеки пройдуть близько 550 вчителів міста Київ. Крім того, ці методичні матеріали будуть доступні для всіх охочих онлайн"…» ***(Петро Івасюк. Комітет з цифрових технологій при МОН хоче навчати школярів і вчителів кібербезпеці // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1810543-komitet-z-tsifrovikh-tekhnologiy-pri-mon-khoche-navchati-shkolyariv-i-vchiteliv-kiberbezpetsi). 02.07.2019).***

***

Національна система кібербезпеки

«Государственная служба специальной связи и защиты информации предлагает создать при участии Интернет Ассоциации Украины организационно-технический комплекс по вопросам кибербезопасности в области телекоммуникаций и, в качестве первого шага, – отраслевой центр реагирования на киберугрозы (CSIRT – Computer Security Incident Response Team).

Об этом говорится в письме Госспецсвязи к Интернет Ассоциации Украины…

– Госспецсвязи подчеркивает необходимость создания отраслевых центров реагирования на киберугрозы (центров компетенции по кибербезопасности) и предлагает рассмотреть вопрос создания при участии ИнАУ и ее членов

организационно-технического комплекса по вопросам киберзащиты в отрасли телекоммуникаций. Первым шагом, по нашему мнению, было бы целесообразно создать отраслевой CSIRT, который станет отраслевой разветвленной платформой в для обмена информацией в сфере киберзащиты, - говорится в письме. - Кроме того, с учетом требований Директивы ЕС 2016/1148 «О мерах по высокому общему уровню безопасности сетевых и информационных систем на территории Союза», предлагаем рассмотреть вопрос о принятии мер по защите от киберугроз на объектах тех операторов (провайдеров) и других субъектов ведения хозяйства, которые выполняют функции точек обмена трафиком и предоставляют услуги DNS.

Для решения этих вопросов Госспецсвязи предлагает организовать рабочую встречу по обсуждению сотрудничества в сфере кибербезопасности.

– Совместная реализация указанных проектов в рамках государственно-частного партнертсва позволит эффективно решать вопросы киберзащиты в целом, – подчеркивается в письме ГСССЗИ.

Как сообщил нашему изданию Председатель Правления Интернет Ассоциации Украины Александр Федиенко, в ИнАУ на данный момент готовят официальный ответ на предложение ГСССЗИ, но саму идею восприняли позитивно: идея создания киберцентра на базе крупнейшей телеком-ассоциации страны уже давно витала в воздухе и письмо Госспецсвязи стало своеобразным толчком к его реализации.

– Все більше операторів зв'язку і телекомунікацій беруть активну участь у наданні послуг кібербезпеки. Продаж виключно доступу до мережі Інтернет, без сервісів з аналітики кіберзагроз, на мій погляд, у подальшому буде питанням не цікавим. Наприклад, асоціація ETIS, яка вважає BT, Telefonica і Deutsche Telekom своїми клієнтами, виступила з новою ініціативою щодо підтримки обміну інформацією про кіберзагрози між провайдерами. А вже далі, цією інформацією можна ділитися з CERT. На мій погляд, саме на базі ІнАУ можна створити відповідний CSIRT як пілотний проект, що являє собою технічну платформу, яка дозволить автоматизувати обмін інформацією щодо інцидентів у режимі реального часу.

Александр Федиенко отмечает: телеком-бизнес в Украине уже не хочет быть просто «трубой», провайдеры становятся сервисными компаниями, и создание CSIRT – вполне логичный шаг на этом пути…

Александр Федиенко также подчеркивает: то, что предложение поступило от ГСССЗИ не значит, что центр будет строится на базе госучреждения…

В целом позитивно оценивают идею создания отраслевого центр реагирования на киберугрозы и опрошенные нами эксперты по кибербезопасности. Единственное, что их смущает – роль, собственно Госспецсвязи в этом процессе…

Более категоричен в отношении Госспецсвязи участник группировки RUH8, известный в сети под ником Шон Таунсенд:

– Очень специальная в своих представлениях о реальности Государственная служба специальной связи и защиты информации в очередной раз решила кого-нибудь осчастливить частно-государственным партнерством. В этот раз – провайдеров. Я вам очень коротко скажу про партнерство. У госорганов есть три

предложения для бизнеса – «мы вам дадим контракты» (в случае провайдеров – куда вы денетесь с подводной лодки, сами приползёте), «мы вам дадим информацию», которая иначе осталась бы секретной (это больше интересует ИБ компании) и «мы вас не будем задалбывать регуляцией». Дело в том, что телеком – одна из самых защищенных отраслей, у них есть опыт и квалифицированные сотрудники, а ГСССЗИ – кровоточащая дыра в безопасности. Эта нищая и дырявая «госуха» просит у телекома построить себе за свои деньги «вундервафлю» для защиты того, что не сломано, и которая им не нужна. Зачем? Чтобы подобраться поближе к частной информации и инфраструктуре. А взамен что? Просто ничего. «Чудесное» предложение, я считаю.» ***(Владимир Кондрашов. Госспецсвязи предлагает создать всеукраинский центр кибербезопасности при поддержке ИнАУ // Internetua (http://internetua.com/gosspecsvyazi-predlagaet-sozdat-vseukrainskii-centr-kiberbezopasnosti-pri-podderjke-inau). 16.07.2019).***

***

«Урочистий захід відбувся за участі першого заступника Голови Національної поліції України В'ячеслава Аброськіна та начальника Департаменту кіберполіції Сергія Демедюка. До привітань приєдналися міжнародні партнери та колеги інших правоохоронних органів. Роботу кращих поліцейських підрозділу було відзначено подяками, подарунками та черговими званнями.

«Кіберполіція стала новим підрозділом у складі Національної поліції України та почала стрімко нарощувати свій потенціал, результатами якого ми можемо пишатися на міжнародній арені», – звернувся з вітальним словом до присутніх В'ячеслав Аброськін.

Він висловив подяку за сумлінність й самовіддачу та від імені керівництва Нацполіції привітав співробітників підрозділу.

Сергій Демедюк подякував поліцейським за службу та відзначив вагомий внесок міжнародних партнерів у розвиток Кіберполіції.

«Упродовж цих років роботи кіберполіції, нам вдалося провести більше 70 міжнародних спецоперацій та викрити більше 45 тисяч злочинів, які відносяться до нашої компетенції» , – зауважив він.

З-поміж усіх спецоперацій підрозділу Сергій Демедюк відзначив найбільш резонансні: припинення діяльності піратських онлайн ресурсів fs.to та ex.ua, викриття шахрайської фінансової біржі «trade12», закриття злочинної бот-мережі АВАЛАНШ, затримання злочинців за розбещення неповнолітніх та поширення ними відповідного контенту в закритій мережі інтернет, ліквідація найбільшого у дарк неті майданчику з продажу персональних даних – xDedic тощо…» ***(Кіберполіція відзначає свій перший ювілей: 10 років боротьби з кіберзлочинністю // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vidznachaje-svij-pershij-yuvilej-10-rokiv-borotbi-z-kiberzlochinnistyu/). 27.07.2019).***

***

«Наблюдатели от Всемирного конгресса украинцев зафиксировали попытки России сорвать внеочередные парламентские выборы в Украине, распространяя.дезинформацию о кандидатах. Об этом сообщил президент общественной организации Евгений Чолий.

Он также констатировал, что аналогичным образом россияне действовали и во время президентских выборов в Украине в марте.

«Во время президентских выборов наша команда была представлена 122 наблюдателями, которые делали медиа-мониторинг для 30 стран мира, на 20 языках и зафиксировали попытки дезинформировать западный мир об избирательном процессе в Украине, а также пытались очернить каждого из кандидатов. В своем отчете мы еще раз подчеркиваем, что Российская Федерация пыталась сорвать процесс выборов во время президентской кампании в Украине», — заявил Евгений Чолий.

Тем не менее в МВД Украины данных о серьезных кибератаках во время выборов в Верховную Раду не зафиксировали, заявил министр Арсен Аваков.

«В отличие от президентской кампании, во время парламентской мы не фиксировали серьезных кибератак. Мы постоянно сотрудничаем с британскими, канадскими и американскими и европейскими коллегами, а также с офисами Facebook, Google, Twitter», — сказал министр…» ***(Стало известно о попытках России сорвать выборы в Раду // Факты и комментарии® (https://fakty.ua/312316-stalo-izvestno-o-popytkah-rossii-sorvat-vybory-v-radu). 21.07.2019).***

***

«Одна из самых надёжных и безопасных электронных почтовых служб в мире оказалась объектом изощренной кибератаки, направленной против экспертов и журналистов, ведущих расследования деятельности российских разведслужб.

Пострадавшие от кибератаки использовали электронную почту ProtonMail, серверы которой находятся в Швейцарии, для обмена секретной информацией, связанной с расследованиями деятельности Главного управления Генерального штаба Вооружённых сил Российской Федерации (ГРУ). Сотрудникам ГРУ были предъявлены обвинения в причастности к катастрофе малазийского рейса MH17 над Украиной в 2014 году и в покушении на убийство Сергея Скрипаля и его дочери в Великобритании в прошлом году.

Компания ProtonMail, созданная в 2014 году группой бывших научных сотрудников Европейской организации по ядерным исследованиям (CERNВнешняя ссылка), позиционирует себя в качестве самого безопасного почтового сервиса, благодаря использованию передовых технологий шифрования и защиты от хакерских атак.

В среду в компании стало известно о предпринятой попытке скомпрометировать ее пользователей. Компания связалась со швейцарскими властями с целью помочь закрыть домены, использовавшиеся для обмана клиентов,

и предприняла меры по блокировке фишинговых электронных сообщений. В компании отметили, что её собственные системы и ПК-серверы не пострадали.

Исполнительный директор ProtonMail Энди Йен (Andy Yen) заявил Financial Times: «Начавшаяся [в среду] кампания с точки зрения сложности действительно относится к 1-2% кибератак самого высокого уровня сложности. Они заблаговременно знали, кто именно должен стать объектом этой атаки. Наши научные исследования говорят о том, что это была целенаправленная операция».

По словам Энди Йена, швейцарские домены были зарегистрированы для имитации пользовательского интерфейса ProtonMail, оплачиваемого через посредников с использованием анонимных биткоин-трансакций. Поддельные порталы входа в систему в этих доменах были затем синхронизированы с реальным процессом входа в ProtonMail для одновременного входа в систему, чтобы обманным путем заставить и пользователей отказаться от двухфакторных кодов аутентификации.

Письма, отправленные пользователям, были тщательно зашифрованы, но одновременно содержали редкую неисправленную ошибку программного кода в широко используемом открытом ПО, которую под силу обнаружить только хакерам, обеспеченным наиболее современными ресурсами…

Учетные записи, которые хакеры пытались взломать, принадлежали членам команды интернет-издания «Бэллингкэт» (Bellingcat), общедоступном сайте, публикующем результаты журналистских расследований, и некой фирме по корпоративной разведке, сотрудники которой, а среди них есть и бывшие сотрудники разведки, используют ProtonMail для конфиденциальной работы по расследованию деятельности России…

Однако, конкретных доказательств, указывающих на причастность Москвы к хакерской атаке на ProtonMail, не так уж много. По словам К. Грозева, вполне вероятно, что кибератака была хакерской операцией самого ГРУ. Подразделение, известное на западе под никами Fancy Bear и APT28, несет ответственность за взлом переписки Хиллари Клинтон и членов Национального комитета Демократической партии в ходе президентской кампании в США в 2016 году…

По словам Мейерса, Fancy Bear последнее время не заявлял о себе, но судя по предварительным данным, его активность за последнее время как, например, атаки на ProtonMail, стала носить более тщательный и целенаправленный характер…

«Выбор целей действительно дает основания утверждать, что это атака была осуществлена при поддержке государства. И тому есть многочисленные подтверждения, в особенности, уровень сложности исполнения хакерской операции». Энди Йен отмечает, что учетные записи пользователей электронной почты ProtonMail полностью зашифрованы, поэтому им не о чем беспокоиться, если только они случайно не выдали свои пароли.» ***(Сэм Джонс. Что стоит за атакой на швейцарский почтовый домен? // SWI swissinfo.ch (http://www.swissinfo.ch/rus/%D1%81%D0%BF%D0%B5%D1%86%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D1%8B-%D0%B8-%D1%88%D0%BF%D0%B8%D0%BE%D0%BD%D0%B0%D0%B6_%D1%87%D1%82%D0%BE-%D1%81%D1%82%D0%BE%D0%B8%D1%82-%D0%B7%D0%B0-%D0%B0%D1%82%D0%B0%D0%BA%D0%BE%D0%B9-%D0%BD%D0%B0-***

%D1%88%D0%B2%D0%B5%D0%B9%D1%86%D0%B0%D1%80%D1%81%D0%BA%D0%B8%D0%B9-%D0%BF%D0%BE%D1%87%D1%82%D0%BE%D0%B2%D1%8B%D0%B9-%D0%B4%D0%BE%D0%BC%D0%B5%D0%BD-/45129406?utm_source=multiple&utm_campaign=swi-rss&utm_medium=rss&utm_content=o). 30.07.2019).

***

«Партия "Голос" заявляет, что на их сервер была совершена кибератака.

Об этом сообщает пресс-служба партии в Facebook.

"Мы подтверждаем, что на CRM-сервер, которым пользуется партия "Голос", произошла кибератака. Наши IT-специалисты выясняют ее последствия и причины", – сказазано в сообщении.

В то же время в политсиле уточнили, что финансово чувствительной информации на сервере не было.

Позже, в партии сообщили, что атака была отражена.

"С наибольшей вероятностью, данные волонтеров не вышли за пределы системы. Спасибо волонтерам Киберальянса за то, что помогли выявить проблемное место в защите", – сообщили в пресс-службе партии.» ***(Партия Голос заявляет о кибератаке // ФОКУС (https://focus.ua/ukraine/435774-partiia_golos_zaiavliaet_o_kiberatake). 25.078.2019).***

***

Боротьба з кіберзлочинністю в Україні

«Киберполиция вышла на след двух украинских хакеров, которые, по версии следствия, на протяжении двух лет занимались взломом и последующей продажей доступов к серверам, расположенным на территории Украины, Европы и США. Продавали свой специфический товар злоумышленники на хакерских форумах и через собственный интернет-сайт…

Согласно материалам дела, неустановленные лица по предварительному сговору в группе в течение 2018-2019 годов на территории Украины систематически осуществляют незаконное вмешательство в работу электронно-вычислительных машин, систем и компьютерных сетей, что приводит к утечке информации. В рамках досудебного расследования уголовного производства были установлены два лица, которые «систематически в течение 2018-2019 лет осуществляют несанкционированное вмешательство в работу электронно-вычислительных машин, автоматизированных систем и компьютерных сетей, путем взломов и в дальнейшем продажей доступов к серверам, расположенным на территории Украины, Европы и США». Для реализации преступной цели указанные лица используют объявления на хакерских форумах и собственный сайт по продаже взломанных серверов.

В конце мая полицейские провели так называемую «контролируемую закупку», во время которой установили, что хакеры «осуществили несанкционированное вмешательство в работу электронно-вычислительных машин и автоматизированных систем» предприятий различных форм собственности, в том числе государственной и коммунальной, расположенных на территории разных регионов Украины, в том числе и реализовали их правоохранителям по заранее оговоренной цене.

В средине июня по месту жительства одного из подозреваемых хакеров прошел обыск. От обычного обыска с изъятием он отличился тем, что полицейским пришлось собирать технику на улице – мать подозреваемого выбросила системный блок и мобильный телефон сына из окна квартиры на десятом этаже.

Обыск у второго подозреваемого прошел без эксцессов.

В начале июля суд арестовал изъятое у подозреваемых оборудование.

Подозреваемым грозит от трех до шести лет лишения свободы.» ***(Владимир Кондрашов. Украинские хакеры продавали доступ к взломанным серверам в Европе и США // Internetua (http://internetua.com/ukrainskie-hakery-prodavali-dostup-k-vzlomannym-serveram-v-evrope-i-ssha). 12.07.2019).***

***

«К штрафу в восемь с половиной тысяч гривен приговорен ранее несудимый гражданин Украины, который встроил в сайт о медицине скрипт для майнинга криптовалюты Monero. Следствие квалифицировало его действия как создание с целью использования, распространения вредоносных программных средств, предназначенных для несанкционированного вмешательства в работу электронно-вычислительных машин…

По версии следствия (то что удалось понять из бездарно составленного текста приговора), мужчина в августе 2018 года, действуя умышленно и из корыстных побуждений, то есть с целью получения дохода от так называемого «скрытого майнинга» криптовалюты «Monero» встроил в программный код Интернет - ресурса http://diagnoz.net.ua/ скрипт «Coinhive».

– После запуска зараженного файла на компьютере пользователя, создается дополнительный файл и процессы, содержащие исполняемый код со ссылкой на загрузку скрытого от пользователя запуска в операционной системе программы для использования вычислительных возможностей процессора его компьютера для осуществления алгоритмических расчетов с целью майнинга (добычи) криптовалюты, – объясняется версия следствия в приговоре. – Согласно разработанного обвиняемым плана преступления, после запуска зараженного файла на компьютере пользователя создаются дополнительные файлы и процессы, содержащие исполняемый код со ссылкой на загрузку скрытого от пользователя запуска в операционной системе программы для использования вычислительных возможностей процессора его компьютера для осуществления алгоритмических расчетов с целью майнинга (добычи) криптовалюты «Monero Blockchain», так называемого «скрытого майнинга». Указанный процесс приводит к чрезмерной загрузке работы процессора компьютера, в результате чего пользователь в процессе

обработки информации получает лишь часть тех результатов, которые можно было бы получить до запуска указанного процесса.

Эксперты МВД Украины установили, что файл «coinhive.min.js.» антивирусным программным обеспечением определяется как вредоносное программное обеспечение и относится к типу «Coinminer» (майнер криптовалют). Далее документация на сайте https://coinhive.com/ помогла экспертам понять, что файл «coinhive .min.js.» предназначен для майнинга криптовалюты «Monero Blockchain» в скрытом режиме путем установления данного майнера на сайте и использования ресурсов компьютера пользователя, который открывает сайт в браузере.

30 мая 2019 года между прокурором и обвиняемым было заключено соглашение о признании виновности. По условиям соглашения мужчина признал себя виновным в совершении уголовного преступления, предусмотренного ч.1 ст.361-1КК Украины.

Сторонами также согласовано, что при утверждении соглашения обвиняемому за совершение уголовного преступления, предусмотренного ч.1 ст.361-1КК Украины, будет назначено наказание в виде штрафа в размере пятисот необлагаемых минимумов доходов граждан, что составляет 8500 грн. Суд соглашение сторон утвердил.» ***(Владимир Кондрашов. За встраивание скрипта для майнинга криптовалют в чужой сайт, выписали большой штраф // Internetua (http://internetua.com/za-vstraivanie-skripta-dlya-maininga-kriptovaluat-v-csujoi-sait-vypisali-bolshoi-shtraf). 10.07.2019).***

***

«Ранее несудимого безработного украинца засудили за распространение вредоносного программного обеспечения. Передача файла с помощью мессенджера Telegram стоила мужчине восемь с половиной тысяч гривен…

Согласно приговору, примерно в августе - сентябре 2018 года, у обвиняемого «возник умысел на распространение вредоносного программного средства, предназначенного для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров)». Для этого он решил использовать ранее приобретенное им у неустановленного следствием лица вредоносное программное обеспечение – «Azorult 3.2». «Azorult 3.2», как установило следствие – вирус класса «стиллер», обладающий функционалом для получения логинов и паролей, сохраненных пользователем удаленного компьютера в браузерах, мессенджерах и кошельках криптовалют.

18 февраля, в ходе общения с пользователем «е» с помощью мессенджера Telegram» из своего аккаунта «@N3V3RM0R3Z», обвиняемый передал файл с вирусом пользователю с никнеймом «RedCliff».

Действия обвиняемого квалифицированы по ч. 1 ст. 361-1 УК Украины, как распространение вредных программных средств, предназначенных для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров).

После завершения досудебного расследования между прокурором и подозреваемым было заключено соглашение о признании виновности. Исходя из

содержания данного соглашения, подозреваемый безоговорочно полностью признал свою виновность в совершении указанного преступления и обязался безоговорочно признать обвинения в объеме подозрения в судебном производстве. Стороны также согласовали наказание в виде штрафа в размере 500 необлагаемых минимумов доходов граждан (8 тысяч 500 гривен).

Суд сделку утвердил…» ***(Владимир Кондрашов. Украинца осудили за передачу вируса через Telegram // Internetua (http://internetua.com/ukrainca-osudili-za-peredacsu-virusa-cserez-telegram). 08.07.2019).***

***

«Четыре года лишения свободы с испытательным сроком в два года получил безработный украинец за «угон» и продажу чужих аккаунтов в сервисе дистрибуции игр Steam. Это уже второй осужденный за продажу чужих «учеток» в этом сервисе за последние три месяца. При этом приговор обеим продавцам вынес один и тот же судья…

Первого июля в Едином государственном реестре судебных решений был опубликован приговор безработному уроженцу Чернигова. Согласно документу, мужчина, с конца ноября 2018 года по начало января 2019 года «угнал» три аккаунта в сервисе Steam, изменил идентификационные данные и с помощью мессенджера Telegram продал их неизвестному лицу.

Кроме продажи аккаунтов, мужчина также через Telegram бесплатно передал лицу с никнеймом «Ивангай» текстовый файл с названием «Отработка.txt» объемом 228 КБ, в котором находилась информация о номерах 1820 банковских карт, их CVV-кодах, датах окончания действия, назначении, виде банковской карты, IP-адресах, фамилиях и именах владельцев. Чуть позже этому же пользователю мужчина бесплатно отправил аналогичные данные ещё о 32 банковских карточках. Откуда мужчина получил эту информацию, следствию установить не удалось. Не выяснили следователи и причины такой щедрости обвиняемого по отношению к «Ивангаю».

В судебном заседании обвиняемый свою вину по предъявленному ему обвинению по ч.1 ст. 361 («Несанкционированное вмешательство в работу электронно-вычислительных машин»), ч.2 ст. 361 («Несанкционированное вмешательство в работу электронно-вычислительных машин, совершенное повторно»), ч. 1 ст. 361-2 («Несанкционированные сбыт или распространение информации с ограниченным доступом»), ч. 2 ст. 361-2 УК Украины («Несанкционированные сбыт или распространение информации с ограниченным доступом, совершенные повторно») признал полностью, подтвердив обстоятельства, изложенные в обвинительном акте, и отметил, что в содеянном искренне раскаивается.

В результате суд признал уроженца Чернигова виновным в предъявленном ему обвинении и назначил ему наказание:

– по ч.1 ст. 361 УК Украины - штраф в размере шестисот необлагаемых минимумов доходов граждан, что составляет десять тысяч двести гривен;

– по ч.2 ст. 361 УК Украины – четыре года лишения свободы;

– по ч.1 ст. 361-2 УК Украины – штраф в размере пятиста необлагаемых минимумов доходов граждан, что составляет восемь тысяч пятьсот гривен;

– по ч.2 ст. 361-2 УК Украины – два года лишения свободы.

На основании ч.1 ст.70 УК Украины по совокупности преступлений путем поглощения менее строгого наказания более строгим суд окончательно назначил наказание в виде четырех лет лишения свободы. Кроме этого, мужчина оплатит судебные издержки на экспертизу в размере 3432 гривны.» ***(Владимир Кондрашов. Украинца осудили за продажу ворованных аккаунтов в Steam // Internetua (http://internetua.com/ukrainca-osudili-za-prodaju-vorovannyh-akkauntov-v-steam). 05.07.2019).***

***

«Співробітники Служби безпеки України спільно з партнерами із США припинили діяльність потужного хакерського угруповання. Про це на брифінгу повідомив т.в.о. Голови СБУ Іван Баканов.

Оперативники спецслужби встановили, що учасники угруповання на території України організували і тривалий час (з 2007 року) надавали віртуальні послуги хакерам та іншим злочинцям, створюючи їм умови для безперешкодного здійснення протиправної діяльності в мережі Інтернет. Зловмисники використовували Dark Net – приховану від звичайних користувачів частину інтернет-мережі, де можливо анонімно придбати зброю, наркотики тощо.

На відміну від пересічних громадян, правоохоронці зазвичай мають право та багато можливостей деанонімізувати особу, що вчиняє злочин, запитавши необхідні відомості у провайдера або оператора зв’язку. Але не в Dark Net, бо він базується на так званому «абузостійкому» хостингу, тобто хостингу, що не відповідає ні на запити правоохоронців, ні на скарги правовласників, який майже неможливо знайти через складні технології маскування (і фізичного, і віртуального) та особливості самого Інтернету…

Оперативники спецслужби встановили, що організатором угруповання є громадянин України, який свій перший хакерський досвід здобував у Москві в середині 2000-х. Вже у 2007 році він розпочав надавати свої послуги хакерам всього світу через українські мережі, ретельно приховуючи фактичне місцезнаходження свого обладнання від правоохоронців та спецслужб будь-якої країни. Обладнання періодично знаходили українські, російські, американські правоохоронці, вилучали його, тимчасово припиняли діяльність, але хакерська група невдовзі продовжувала діяти.

На сьогодні угруповання нараховує близько десяти основних учасників та десятки пособників, посередників у низці країн світу, а також тисячі клієнтів. «Вони занепокоєні тим, що у руках спецслужб опинились сотні терабайт даних, які можуть стати доказами у сотнях кримінальних справ по всьому світу. За нашими оцінками, мова може йти про 40% російськомовного сегменту Dark Net», - підкреслив т.в.о Голови СБУ.

Лише в США відносно цього громадянина України висунуто обвинувачень загалом на п’ятдесят років ув’язнення. Він звинувачується у шахрайстві,

несанкціонованому втручанні, крадіжці персональних даних та низці інших злочинів за американським кримінальним законодавством.

В Україні організатору та ще одному учаснику угруповання оголошено підозру у вчиненні кримінальних правопорушень, передбачених за ч. 2 ст. 361 та ч. 3 ст. 301 Кримінального України, та обрано запобіжний захід - домашній арешт.

Незважаючи на складний механізм документування, пов'язаний із недосконалим вітчизняним законодавством у кіберсфері, оперативникам СБУ спільно зі слідчими Державного бюро розслідування та прокурорами Генеральної Прокуратури України вдалося зібрати необхідні докази щодо причетності фігурантів провадження до вчинення тяжких злочинів.

Під час санкціонованих слідчих дій на території приватного будинку поблизу Одеси було віднайдено справжній дата-центр з резервним автономним джерелом електроживлення, охороною, потужними каналами доступу до інтернету, який було ретельно приховано. «З нього вилучено майже півтори сотні серверів, на яких розміщувались тисячі хакерських ресурсів, деякі з них залишились зашифрованими, тобто були налаштовані таких чином, щоб не зберігати слідів злочинної діяльності», - повідомив т.в.о начальника Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Микола Кулешов.

Попереднє дослідження мережевого обладнання та оцінка діапазонів IP-адрес, що використовувались угрупованням, вказує на мінімум три автономні системи, зарезервовані за підприємствами Російської Федерації. Враховуючи контррозвідувальний режим, наявний в РФ, а також технологічні особливості організації та побудови СОРМ-3, володіння та керування цим номерним ресурсом з боку угруповання не могло відбутись без контролю та прикриття російських спецслужб. Ця інформація дозволяє СБУ отримати більш чітке уявлення про схеми кібератак на українські об'єкти критичної інфраструктури, про роль російських спецслужб в кібератаках на інші країни…» ***(СБУ спільно з іноземними партнерами припинили діяльність потужного хакерського угруповання (відео) // СБ України (https://ssu.gov.ua/ua/news/1/category/21/view/6281#.Lnc4lYFH.dpbs). 16.07.2019).***

***

«…Сотрудники Службы безопасности Украины разоблачили и блокировали в Хмельницкой области механизм продажи информации с ограниченным доступом из государственных автоматизированных информационных систем…

"Оперативники спецслужбы установили, что бывший пограничник наладил противоправный механизм получения и сбыта сведений с ограниченным доступом, в частности относительно въезда-выезда граждан за границу, наличии запрета въезда в Украину для иностранцев и тому подобное", – сказано в сообщении.

Злоумышленника задержали в Хмельницком после попытки очередной передачи данных.

Задержанному сообщено о подозрении в совершении преступления по статье о несанкционированном вмешательстве в работу компьютеров,

автоматизированных систем и сетей.» (ч.2 ст.361-2 УК Украины). ***(Бывший пограничник торговал секретной информацией, – СБУ // ФОКУС (https://focus.ua/ukraine/434214-byvshii_pogranichnik_torgoval_sekretnoi_informatsiei__sbu). 10.07.2019).***

***

«…Працівники Київського управління кіберполіції спільно зі слідчими поліції Черкащини викрили 30-річного мешканця Черкас у використанні викрадених реквізитів банківських карток та персональних даних громадян.

Працівники кіберполіції провели обшук у квартирі зловмисника. У його помешканні виявили велику кількість цифрової техніки, яка призначалася для продажу, комп'ютерну техніку, а також сканкопії документів підставних осіб, на ім'я яких надсилалися міжнародні бандеролі.

Встановлено, що за час таких оборудок чоловік отримав близько 200 міжнародних посилок на одному поштовому відділенні. Під час проведення подальших слідчих дій буде встановлено усіх осіб, які стали його жертвами. Враховуючи те, що серед потерпілих були не тільки громадяни України, а і іноземці, наразі працівники кіберполіції надсилають міжнародні запити до різних країн, аби встановити усіх потерпілих.

Кримінальне провадження відкрито за ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України…» ***(Кіберполіція викрила чоловіка у використанні викрадених баз даних для здійснення онлайн-покупок // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-cholovika-u-vikoristanni-vikradenix-baz-danix-dlya-zdijsnennya-onlajn-pokupok/). 22.07.2019).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Секретар Ради національної безпеки і оборони України Олександр Данилюк провів зустріч із делегацією НАТО під керівництвом Голови Представництва НАТО в Україні Александером Вінніковим…

Сторони обговорили перспективи євроатлантичної інтеграції України, виконані завдання в рамках річної програми Україна-НАТО та стратегічні плани.

"Александер Вінніков був поінформований про пріоритетні напрями роботи РНБО України, серед яких, зокрема, кібербезпека та реформа оборонно-промислового комплексу, а також позитивно оцінив початок роботи над Стратегією національної безпеки України. Олександр Данилюк зазначив, що для реалізації визначених планів першочерговим завданням є реформування законодавства у цих сферах, над удосконаленням якого зараз працює РНБО України", — вказано у повідомленні.

Водночас Голова Представництва НАТО зауважив, що реформування сектору безпеки позитивно вплине на процес євроатлантичної інтеграції України та запевнив у підтримці НАТО у впровадженні реформ…» ***(Олексій Супрун. Данилюк провів зустріч із делегацією Представництва НАТО в Україні // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1811989-danilyuk-proviv-zustrich-iz-delegatsiyeyu-predstavnitstva-nato-v-ukrayini). 09.07.2019).***

***

«Напередодні парламентських виборів у Києві відбулися міжнародні кібернавчання, організовані для отримання новітнього європейського досвіду безпеки виборчих процесів в інформаційному та кібернетичному просторі…

Другі навчання побудовані за більш складною технологією та передбачають відпрацювання складніших завдань. На технічному рівні вони відбуваються у межах проекту ЄС "Посилення кібербезпеки в Україні перед виборами" за підтримки Естонського центру Східного партнерства та компанії CybExer Technologies.

У кібернавчаннях, окрім європейських фахівців, беруть участь спеціалісти СБУ, Державної служби спеціального зв'язку та захисту інформації, кіберполіції, ЦВК, які вдосконалять унікальний досвід протидії хакерам в умовах максимально наближених до реальних за рахунок повністю віртуалізованої інфраструктури.

За сценарієм кібернавчань усі учасники діляться на дві групи команд: хакерів та кібербезпеки. Команди з першої групи, що сформовані за участі представників CybExer Technologies, здійснюють атаки на інформаційні ресурси "умовної ЦВК". Інші, сформовані з фахівців СБУ, ЦВК, Держспецзв'язку та Кіберполіції, їм протидіють. Паралельно з навчаннями технічних команд фахівців відбулись тренінги зі стратегічних комунікацій, до яких залучались менеджери та представники пресслужб українських відомств…» ***(Роман Рудський. Перед виборами пройшли міжнародні навчання із забезпечення кібербезпеки систем ЦВК // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1811019-pered-viborami-proyshli-mizhnarodni-navchannya-iz-zabezpechennya-kiberbezpeki-sistem-tsvk). 04.07.2019).***

***

Світові тенденції в галузі кібербезпеки

«…Только 25% ведущих IT-компаний по региону EMEA (Европа, Ближний Восток, Африка) уверены в надежности своей системы информационной безопасности, сообщается в отчете компании VMware.

70% IT-специалистов считают, что их организации используют устаревшие технологии защиты. Только 42% респондентов отметили обновление инструментов защиты в компаниях за прошлый год. 75% респондентов планируют увеличить расходы на обнаружение и идентификацию атак. По словам 20% участников исследования, их организация уже применяет более 26 решений для безопасности.

Несмотря на увеличение инвестиций в кибербезопасность, только 13% IT-компаний решают такие проблемы менее чем за одну неделю. Большинство компаний сталкиваются с парадоксом продуктивности, когда расходы на информационную безопасность растут, а эффективность остается прежней. 96% российских организаций планируют внедрить новые технологии кибербезопасности в течение трех ближайших лет.

Только 26,6% респондентов полностью уверены в надежности своих облачных развертываний. И лишь 23,3% опрошенных уверены в готовности своих сотрудников разрешать проблемы кибербезопасности.

Руководители компаний и их команды по безопасности совершенно по-разному представляют совместную работу в сфере борьбы с киберугрозами. Всего 36% IT-специалистов считают руководителей достаточно отзывчивыми и активно участвующими в разрешении проблем. В то же время 27% руководителей уверены, что уделяют достаточно внимания совместной работе в области обеспечения кибербезопасности, но с этим утверждением согласны всего 16% опрошенных IT-специалистов.» ***(75% IT-компаний не уверены в своей кибербезопасности // SecurityLab.ru (https://www.securitylab.ru/news/499977.php). 17.07.2019).***

***

«…68% компаний пострадали от кибератак в 2018 году, несмотря на все попытки предотвратить их. При этом 91% IT-специалистов признались, что атаки были успешными, несмотря на использование современных методов защиты. Такие данные приводятся в отчете компании Sophos, сформированном по итогам опроса, в котором приняли участие 3100 IT-специалистов из 12 стран.

Согласно результатам опроса, в числе наиболее популярных векторов атак респонденты называют электронную почту (33%), интернет (30%), уязвимости в программном обеспечении (23%), а также использование несанкционированных USB-накопителей или других внешних устройств (14%). 20% IT-специалистов признались, что не знали, каким образом были скомпрометированы сети их организаций.

53% из успешных атак были фишинговыми, 35% задействовали вредоносное ПО, 35% — эксплоиты, а 30% — программы-вымогатели. Наиболее значительными рисками респонденты называют фишинговые письма (50% опрошенных), эксплоиты (45%), а также человеческий фактор (сотрудники, подрядчики и клиенты).

Опрошенные IT-специалисты также упомянули о нехватке ключевых навыков у персонала, что значительно усложняет отслеживание количества инцидентов и оценку масштабов рисков. Две трети респондентов сообщили о слишком низких бюджетах для найма персонала и закупки технологий.» ***(68% IT-специалистов не могут защититься от кибератак // SecurityLab.ru (https://www.securitylab.ru/news/499965.php). 16.07.2019).***

***

«Малый и средний бизнес (МСБ) плохо справляется с защитой своего периметра безопасности, позволяя злоумышленникам оставаться в

инфраструктуре по два года и более, считают аналитики Infocyte. По их данным, только 28% таких организаций справились бы с присутствующей угрозой менее чем за три месяца, у остальных бы на это ушло намного больше времени.

Таковы результаты исследования, в котором приняли участие компании с численностью сотрудников от 100 до 5000 человек и годовой выручкой до $1 млрд. Аналитики собрали информацию с 339 тыс. аккаунтов и логов вредоносной активности.

Быстрее всего МСБ обнаруживает атаки вымогателей — на это у компаний уходит в среднем 43 дня. Остальные зловреды обычно выявляются через 798 дней (2 года и 2 месяца). В случае веб-трекеров, рекламных приложений и прочих неявных угроз средний период обнаружения и вовсе составил 869 дней (2 года и 4 месяца).

Корни этой ситуации эксперты видят в общей низкой защищенности МСБ. Чем сложнее зловред, чем лучше он скрывает свою активность, тем меньше у компании шансов заблокировать его. Поэтому быстро проявляющий себя шифровальщик удается обнаружить через полтора месяца, а если вредоносные функции ПО не предполагают явных действий, оно может оставаться в сети сколько угодно.

С другой стороны, специалистам таких компаний зачастую не под силу и зачистить инфраструктуру от обнаруженного зловреда — будь то из-за технической отсталости ИБ-систем или неграмотности самих сотрудников…

Специалисты рекомендуют компаниям развернуть системы ИБ-мониторинга, которые смогут в реальном времени отслеживать нежелательную активность. Если такое решение организации не по карману, следует хотя бы раз в год приглашать сторонних специалистов для проверки защищенности. Оценка существующих уязвимостей и тесты на проникновение также составляют обязательную часть ИБ-профилактики…» ***(Egor Nashilov. Кибератаки могут оставаться незамеченными по два года // Threatpost (https://threatpost.ru/cyberattacks-can-be-unnoticed-for-years/33479/). 15.07.2019).***

***

«Ирландская глобальная транснациональная компания по управлению рисками, страховыми брокерами и консалтингу Willis Towers Watson провела опрос крупнейших 467 компаний мира. В результате было выяснено, что 12% из них планируют увеличить финансирование кибербезопасности.

На основе опроса несколько мировых специалистов в сфере кибернетической безопасности совместно с Willis Towers Watson (WTW) подготовили спецотчет о перспективах финансирования мировыми компаниями защиты своих информационных систем.

Согласно отчету, 12% респондентов на 50% увеличат свои инвестиции для защиты информационного пространства. Участники исследования планируют нарастить на 34% свои инвестиции в кибернетический защиту, что в два раза больше, чем годом ранее.

Выросла озабоченность специалистов и по поводу увеличения рисков для бизнеса от таких угроз. Если в 2017 году только 57% из них считали эти угрозы значительными, то сейчас их 71%.

В Willis Towers Watson прокомментировали это так: “Компании испытывают все возрастающее воздействие со стороны ключевых противников, включая киберпреступников, злоумышленников и спонсируемых государством хакеров, часто из юрисдикций, выходящих за рамки местного законодательства”.» ***(Исследование: Компании больше инвестируют в кибербезопасность // Олфин (https://allfin.com.ua/news/issledovanie-kompanii-bolshe-investirujut-v-kiberbezopasnost/). 20.07.2019).***

***

«Лишь четверть ведущих компаний по региону EMEA уверены в надежности своей системы информационной безопасности. Эти данные были получены VMware в рамках совместного исследования с Forbes Insights.

Почти 70% специалистов по информационной безопасности считают, что решения, которые их организация применяет для защиты своих систем, устарели. При этом 42% опрошенных отмечают, что за прошлый год их компания приобрела новые инструменты, направленные на борьбу с потенциальными угрозами. Около 75% респондентов планируют увеличить расходы на обнаружение и идентификацию атак. При этом 20% участников исследования сообщили, что их организация уже применяет 26 и более решений для безопасности.

Несмотря на то, что компании продолжают наращивать инвестиции в защиту систем, всего 13% ИТ-специалистов утверждают, что разрешение проблем, связанных с кибербезопасностью, занимает менее одной недели. В современном мире, где обработка данных производится в режиме реального времени, число интернет-пользователей ежедневно увеличивается более чем на миллион человек[i], а большая часть операций проходит через приложения в считанные секунды, такой медленный отклик представляет серьезную опасность.

Особенно драматично то, что многие компании сталкиваются с парадоксом продуктивности, когда расходы на ИБ растут, а эффективность — нет.

Исследование, в котором приняли участие 650 компаний Европы, Ближнего Востока и Африки, позволило выявить опасную тенденцию: для борьбы с новейшими киберугрозами предприятия используют медленные и неэффективные методы. При этом, по данным Европейского союза, масштабы экономических последствий киберпреступности увеличились в пять раз по сравнению с 2013 годом.

Сложившийся подход к безопасности привел к тому, что организации все чаще считают себя незащищенными перед лицом киберугроз. Только четверть (26,6%) респондентов заявили, что полностью уверены в надежности своих облачных развертываний. И лишь 23,3% опрошенных уверены в готовности своих сотрудников разрешать проблемы, связанные с безопасностью.

Руководители компаний и их команды по безопасности совершенно по-разному представляют себе прогресс и совместную работу в сфере борьбы с киберугрозами. Всего 36% ИТ-специалистов считают, что руководители высшего

звена их предприятий достаточно отзывчивы и активно участвуют в разрешении проблем такого рода. В то же время 27% руководителей заявляют, что уделяют значительное внимание совместной работе в области обеспечения кибербезопасности. С этим утверждением согласно всего 16% опрошенных профессионалов в области информационной безопасности.» ***(VMware: лишь 25% компаний уверены в эффективности своей системы кибербезопасности // Компьютерное Обозрение (https://ko.com.ua/vmware_lish_25_kompanij_uvereny_v_jeffektivnosti_svoej_sistemy_kiberbezopasnosti_129468). 17.07.2019).***

***

Сполучені Штати Америки

«Microsoft представил первую систему для голосования на выборах с технологией ElectionGuard, специально разработанную для обезопасить проведение выборв от внешнего вмешательства…

Аппаратная сторона системы включает в себя планшетный компьютер Surface, принтер и адаптивный контроллер Xbox, позволяющий сделать голосование более доступным для всех людей.

Такая система является уникальной, поскольку она доказывает, что для проведения голосования могут использоваться обычные аппаратные компоненты, объединённые между собой программным обеспечением.

После того, как избиратель проголосовал с помощью планшета или контроллера, система ElectionGuard подсчитывает голоса с использованием гомоморфного шифрования, сохраняя при этом данные в зашифрованном виде.

Система предоставляет каждому избирателю индивидуальный код, позволяющий проверить с помощью сети Интернет, был ли голос засчитан корректно. Дополнительным уровнем проверки является бумажный бюллетень, который распечатывается на принтере. Избиратель может оставить соответствующую отметку в нём и поместить его в специальную урну.

После того, как избиратель проголосует, его ответ будет зашифрован, а пользователю выдадут код отслеживания. Так избиратель сможет следить, что его голос учли и не изменили в процессе. С помощью принтера можно будет дополнительно опустить бюллетень в ящик для голосования.

ПО будет бесплатным и будет доступно в США и других странах по всему миру.

В Microsoft сообщили, что «пилотная» версия безопасной системы для голосования будет использоваться на выборах в США в следующем году. Хотя разработчики считают, что систему ElectionGuard следует начать использовать как можно раньше…» ***(Николай Загорский. В Microsoft разработали систему ElectionGuard для предотвращения махинаций с голосами избирателей (ФОТО) // (https://golos.ua/i/694625). 19.07.2019).***

***

«Посол Великої Британії в ЄС поскаржився на те, що британські чиновники були "відсторонені" від засідання ЄС з кібербезпеки, яке стосувалося ризиків китайського виробника обладнання Huawei…

Британія має вийти з ЄС 31 жовтня, але до того часу країна залишається повноправним членом з правом бути присутньою на засіданнях, які не включають обговорення Brexit.

На порядку денному засідання з кібербезпеки, яке відбулося 25 червня, були кіберстандарти і захист мереж 5G в контексті потенційних ризиків безпеки від присутності Huawei в Європі.

Посол Британії в ЄС Тім Барроу стверджував, що участь Британії в таких зустрічах не загрожує інтересам безпеки ЄС. Він висловив жаль з приводу того, що немає жодної чіткої причини для виключення.

Лондон ще не визначився з питанням, чи обмежувати використання обладнання Huawei. Раніше британський парламентський комітет з науки і технологій порадив уряду заборонити обладнання Huawei в так званих основних частинах телекомунікаційних мереж, зберігаючи при цьому решту ринку для китайських виробників телекомунікаційного обладнання…» ***(Британію "відсторонили" від зустрічі ЄС з кібербезпеки – ЗМІ // "Європейська правда" (https://www.eurointegration.com.ua/news/2019/07/22/7098746/). 22.07.2019).***

***

«Евросоюз намерен до конца года завершить разработку общеевропейских мер по снижению рисков и повышению безопасности систем мобильной связи пятого поколения (5G).

Об этом сообщил в пятницу на брифинге в Брюсселе еврокомиссар по вопросам безопасности Джулиан Кинг.

"Сегодня мы завершили первый этап этой работы - 24 (из 28) государства ЕС предоставили национальные оценки угроз и рисков, которые существуют для систем 5G. Мы переходим к следующему этапу - анализу этих оценок и определению на европейском уровне ключевых структур, которые будут иметь влияние на функционирование систем 5G, степень уязвимости ключевых компонентов этих сетей. Эта работа должна быть завершена к октябрю, чтобы к концу года мы разработали набор пропорциональных и эффективных общеевропейских мер для контроля рисков и стандартов безопасности систем 5G", - отметил он…» ***(ЕС намерен к концу года разработать меры по обеспечению безопасности сетей 5G // IKSMEDIA.RU (http://www.iksmedia.ru/news/5599204-ES-nameren-k-konczu-goda-razrabotat.html). 22.07.2019).***

***

«Китайская телекоммуникационная компания ZTE открыла в Брюсселе лабораторию кибербезопасности…

Первоначальное намерение создать лабораторию заключалось в предоставлении максимально прозрачной кибербезопасности клиентам со всего мира, контролирующим органам и всем заинтересованным сторонам путем личной проверки и общения, заявил представитель ZTE Чжун Хун на церемонии открытия.

По его словам, в Брюсселе расположены многие административные органы Европейского союза, поэтому создание здесь лаборатории является важной мерой по повышению уровня прозрачности и направлено на выполнение обязательств ZTE по повышению безопасности в информационной и коммуникационной отрасли.

Лаборатория будет предоставлять более масштабную внешнюю проверку безопасности продукции, услуг и технологических процессов компании ZTE, а также содействовать развитию сотрудничества между ZTE и всеми заинтересованными сторонами в сфере безопасности.

В церемонии открытия приняли участие представители Еврокомиссии и Европейского совета, а также компаний мобильной связи…» ***(ZTE открыла в Европе лабораторию кибербезопасности // ООО «Файненс.юа» (https://news.finance.ua/ru/news/-/452509/zte-otkryla-v-evrope-laboratoriyu-kiberbezopasnosti). 12.07.2019).***

***

«Петропавловск-Камчатский городской суд в конце мая текущего года закрыл уголовное дело против сотрудника Института вулканологии и сейсмологии, устроившего две DDoS-атаки на сайты Роскомнадзора из-за блокировки мессенджера Telegram…

Мужчине инкриминировалась ч. 1 ст. 274.1 УК РФ (Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации).

«Весной прошлого года он, посредством своего рабочего компьютера, не желая блокировки мессенджера Telegram государственными органами РФ, использовал компьютерное программное обеспечение «LOIC», <…> заведомо для него предназначенное для неправомерного воздействия на критическую информационную структуру Российской Федерации, для блокирования информации, содержащейся на сайтах «rkn.gov.ru», «vigruzki.rkn.gov.ru», — также указано в судебном решении.

Обвиняемый и его защитник ходатайствовали о прекращении уголовного преследования в связи с деятельным раскаянием обвиняемого, поскольку он свою вину в совершении преступления признал, обратился с явкой с повинной, способствовал раскрытию и расследованию преступления: «Согласно ст. 75 УК РФ

лицо, впервые совершившее преступление небольшой или средней тяжести, может быть освобождено от уголовной ответственности, если после совершения преступления добровольно явилось с повинной, способствовало раскрытию преступления, возместило причинённый ущерб или иным образом загладило вред, причинённый в результате преступления, и вследствие деятельного раскаяния перестало быть общественно опасным».

Помощник прокурора не возражал против удовлетворения этого ходатайства. Суд уголовное дело прекратил…» ***(DDoS протеста // РосКомСвобода (https://roskomsvoboda.org/47977/). 04.07.2019).***

***

«Телеком-операторы Казахстана начали уведомлять клиентов о необходимости установить специальный сертификат безопасности Qaznet на все абонентские устройства с доступом в интернет.

…SMS-сообщения с соответствующим уведомлением получили некоторые абоненты Tele2 и Beeline. Операторы Kcell и Activ разместили сообщения аналогичного содержания и инструкции по установке сертификата на своих официальных сайтах.

Рекомендованный к установке сертификат «разработан в Казахстане и предоставлен уполномоченным государственным органом» и «позволит оградить казахстанских пользователей интернета от хакерских атак и просмотра противоправного контента», говорится в сообщении на сайте провайдера Kcell.

Загрузить сертификат пользователям предлагается с сайта qca.kz. Эта доменное имя зарегистрировано на частное лицо – некоего Аскара Дюссекеева (Askar Dyussekeyev) из города Нур-Султана (бывшая Астана). Адрес владельца совпадает с адресом Министерства цифрового развития, инноваций и аэрокосмической промышленности Казахстана.

Оператор Kcell также предупреждает, что в случае отсутствия сертификата пользователи могут столкнуться с проблемами доступа к отдельным интернет-ресурсам. Действительно, по свидетельству некоторых пользователей из столицы Казахстана, без установки сертификата невозможно зайти на сайты, которые форсируют использование безопасного протокола HTTPS с помощью механизма HSTS. Таких сайтов сейчас большинство. Вместо запрашиваемого сайта провайдеры выдают страницу-заглушку с призывом установить сертификат.

По словам вице-министра цифрового развития, инноваций и аэрокосмической промышленности Казахстана Аблайхана Оспанова, жители республики не обязаны устанавливать сертификаты, им всего лишь предоставляется подобная возможность, положенная по закону.

Установка национального корневого сертификата безопасности на устройства жителей Казахстана позволит владельцу этого сертификата перехватывать, расшифровывать и модифицировать защищенный с помощью средств криптографии HTTPS-трафик пользователей перед дальнейшей отправкой к узлу назначения, то есть осуществлять так называемую атаку посредника – MITM (Man in the middle, «человек посередине»).

Принимая во внимание заявление оператора KCell о том, что сертификат разработан «уполномоченным государственным органом», можно предположить, что такие возможности могут быть использованы властями Казахстана для получения доступа к информации, которой граждане обмениваются через интернет.

Впрочем, слежкой за пользователями смогут заниматься не только государственные структуры, но и злоумышленники, к ним отношения не имеющие. По мнению президента интернет-ассоциации Казахстана Шаквата Сабирова, слова которого цитирует Tengrinews.kz, «если по какой-либо причине, неважно технической или из-за человеческого фактора, этот сертификат будет украден или взломан, то злоумышленникам достанется абсолютно вся информация о пользователях и данных, которые используют этот сертификат».

В настоящее время на базе багтрекера (системы отслеживания ошибок) браузера Mozilla Firefox представителями интернет-сообщества и разработчиками ведется обсуждение возможности добавления сертификата в «черный список» и введения запрета на его установку вручную, чтобы таким образом защитить пользователей из Казахстана от слежки со стороны властей…» ***(В Казахстане перекроют интернет всем, кто не подключит государственное шпионское ПО // IKSMEDIA.RU (http://www.iksmedia.ru/news/5599043-V-Kazaxstane-perekroyut-internet.html). 19.07.2019).***

***

Інші країни

«…Уже почти год бразильские пользователи страдают от кибератак, нигде больше в мире не встречающихся. Атаки проходят почти незаметно и могут привести к прямым финансовым потерям.

То, что происходит сейчас в Бразилии, должно стать предупреждающим сигналом для интернет-провайдеров и пользователей по всему миру, уверены эксперты. По их мнению, провайдеры и пользователи должны успеть принять соответствующие меры предосторожности, пока атаки не вышли за пределы Бразилии.

Вышеупомянутые атаки впервые были зафиксированы летом прошлого года специалистами компании Radware. По словам ИБ-экспертов, на то время неизвестные киберпреступники взломали порядка 100 тыс. домашних маршрутизаторов и модифицировали настройки DNS таким образом, чтобы при попытке воспользоваться сервисом online-банкинга жертва перенаправлялась на точную копию настоящего сайта.

По данным исследователей из Ixia, злоумышленники использовали не только копии сайтов бразильских банков, но также подделывали такие ресурсы, как Netflix, Google и PayPal, с целью похищения учетных данных пользователей.

Прошел год, но атаки не прекратились, отмечают эксперты Avast. Напротив, в первой половине 2019 года злоумышленники взломали около 18 тыс. маршрутизаторов в Бразилии и изменили их настройки DNS. Более того, методы

атаки усложнились, а количество причастных к ним киберпреступников увеличилось.

По данным Avast, чаще всего пользователи становятся жертвами злоумышленников при посещении, спортивных сайтов, стриминговых видеосервисов и порталов «для взрослых». Размещенная на таких ресурсов реклама содержит вредоносный код, способный определять IP-адрес и модель маршрутизатора и подбирать к ним учетные данные по умолчанию из прилагающегося списка. Этот процесс занимает некоторое время, но пользователи обычно ничего не замечают, поскольку заняты просмотром видео.

Если взлом прошел успешно, вредоносная реклама внедряет дополнительный код, меняющий IP-адреса легитимных DNS-серверов на IP-адреса серверов, подконтрольных киберпреступникам. Когда в следующий раз устройство пользователя подключится к маршрутизатору, вместо полученных от провайдера IP-адресов нужных DNS-серверов оно получит IP-адреса серверов киберпреступников.» ***(Бразильские пользователи становятся жертвами необычных кибератак // SecurityLab.ru (https://www.securitylab.ru/news/499963.php). 15.07.2019).***

***

«Первый в своем роде учебный курс по кибербезопасности для людей с ограниченными возможностями был открыт в Израиле в целях расширения кадрового потенциала в отрасли.

В первую группу курса войдут 16 студентов с аутистическим спектром в возрасте от 21 года и старше. Курс является инициативой Рама Леви (Ram Levy), исполнительного директора компании по кибербезопасности "Konfidas", которая стремится помочь людям с ограниченными возможностями интегрироваться в ту область, в которой высок спрос на квалифицированных работников.

Программа обучения продлится около двух месяцев и будет включать около 250 часов теоретического обучения, а также практические занятия. Теоретические занятия будут проводиться в колледже безопасности "Зее", а практические занятия будут проводиться профессиональными наставниками из фирм, присоединившихся к этой инициативе. К ним относятся "Израильская электрическая корпорация", "Facebook Israel", "Bank Hapoalim" и "Israel Discount Bank".» ***(В Израиле запускается курс по кибербезопасности для аутистов // ISRAland Online Ltd (http://www.isra.com/news/232692). 22.07.2019).***

***

«На прошлой неделе израильское управление по защите личной информации обнародовало данные, согласно которым информация о примерно трети серьезных кибератак против израильских целей не была передана властям, как предписывают новые правила раскрытия информации.

Согласно финансовому изданию "Calcalist", опубликованы данные, свидетельствующие о том, что правительственное агентство имело дело со 146 серьезными инцидентами, но только о 103 из них ему сообщили целевые организации. Правила, вступившие в силу в мае прошлого года, требуют от

местных компаний и некоммерческих организаций, которые ведут базы данных личной информации, сообщать о любых нарушениях и взломах…» ***(В Израиле власти не в курсе о трети нарушений конфиденциальности // ISRAland Online Ltd (http://www.isra.com/news/232958). 29.07.2019).***

***

Протидія зовнішній кібернетичній агресії

«Спецслужби Китаю встановлюють шпигунське програмне забезпечення на смартфони туристів, яке витягує їх електронні листи, тексти, контакти і може використовуватися для відстеження переміщень…

Розслідування, проведене Guardian і міжнародними партнерами, показало, що мандрівники стають жертвами нападів при спробі в'їзду в Китай з сусідньої Киргизії. Зокрема, китайські прикордонники беруть телефони туристів і таємно встановлюють додаток, яке отримує електронні листи, тексти та контакти, а також інформацію про самому телефоні.

За словами туристів, вони не були заздалегідь проінформовані про встановлення будь-яких додатків і використанні особистих даних без їх згоди…» ***(Китай встановлює шпигунські програми на смартфони туристів, - ЗМІ // Espreso.tv (https://espreso.tv/news/2019/07/04/kytay_vstanovlyuye_shpygunski_programy_na_smartfony_turystiv_zmi). 04.07.2019).***

***

«Компанія Microsoft за рік повідомила близько 10 тисяч клієнтів про загрозу кібератак за підтримки різних держав, йдеться в повідомленні корпорації.

«Активність» переважно йшла з боку Ірану, Північної Кореї і Росії.

Більше 80% атак було направлено проти компаній, близько 16% – на особисті облікові записи користувачів. Кібератаки, за даними Microsoft, були організовані іранськими групами Holmium і Mercury, північнокорейської групою Thallium і двома російськими групами Yttrium і Strontium (вона ж Fancy Bear і ATP28)…» ***(Тисячі клієнтів Microsoft опинилися під загрозою кібератак – корпорація // Радіо Свобода (https://www.radiosvoboda.org/a/news-microsoft-hackers/30062771.html). 18.07.2019).***

***

«В начале лета 2019 года США, вместо того чтобы отомстить авианалетом Ирану за сбитый беспилотник, совершили кибератаку на пусковые установки иранских ракет. Это дало новый толчок разговорам о возможностях кибервойны и о том, кто может использовать эту тактику. Неожиданно оказалось, что США могут пострадать от несанкционированного вмешательства в управление их спутниковыми сетями.

БУДЕТ ХАОС. Согласно отчету аналитического центра Chatham House, последствием кибератаки на американские спутники станут «хаос и смятение» в системах управления стратегическим вооружением. Опасность кибератак сложно переоценить, ведь они происходят быстро, о них не предупреждают.

Поймать автора кибератаки и адекватно ответить на нападение – сложно. От спутников на поле боя зависит многое: система связи, ПВО, управление беспилотниками, обнаружение целей и командование боем. Учитывая то, насколько важны спутниковые данные для ведения боевых действий в современном мире, логично предположить, что враги уже проникли в сети.

КТО ТАМ? Иран не имеет никакого отношения к кибератакам на спутники – у него нет таких технологий. Но Россия и Китай вполне способны осуществить подобные нападения. Пребывая в условиях торговой войны с США, Китай одобрил наступательную кибернетическую стратегию и финансирует собственных хакеров.

Если РФ или Китай предпримут такую атаку, то последствия для военных миссий США будут катастрофическими. На фоне ухудшения отношений между Вашингтоном, Пекином и Москвой кибератаки составляют угрозу американской нацбезопасности.

ОПАСНЫЕ СЕТИ. Китай и Россия сосредоточились в кибератаках именно на американские спутники, поскольку их эффективность может угрожать китайским и российским военным операциям.

«В случае возобновления боев на Востоке Украины, на Ближнем Востоке или в Южноазиатском регионе ожидается, что спутниковая связь обеспечит надлежащую работу оборонительных систем. Нельзя воспринимать это, как нечто, само собой разумеющееся. Для любой миссии НАТО критически важными будут управление и защита космических возможностей», – уверены эксперты Chatham House.

В ЗОНЕ РИСКА. Для передачи данных и получения нужной информации военные США используют коммерческие спутники. Если эти устройства подвергнутся вражеской атаке, то возможна утечка стратегически важных данных. Это касается не только военной сферы, но и любой другой, где не обойтись без спутниковой связи.» ***(Гарченко. Хакеры России и Китая могут устроить кибератаку на военные спутники США. Это правда? // ETCETERA.MEDIA (https://etcetera.media/hakeryi-rossii-i-kitaya-mogut-ustroit-kiberataku-na-voennyie-sputniki-ssha-eto-pravda.html). 17.07.2019).***

***

«Первый канал Общественного вещателя Грузии сообщил о кибератаке, совершенной в пятницу на его сайт с IP-адреса, зарегистрированного у одного из российских провайдеров.

"За последние 20-30 минут на веб-портале фиксировалась аномальная нагрузка. Как установили специалисты, выявлен один IP-адрес, с которого, предположительно, сканировался сайт или была попытка атаки с одного конкретного адреса", — говорится в сообщении телеканала.

Также указано, что подозрительный адрес уже заблокирован…» ***(Грузинский телеканал сообщил об атаке на свой сайт с российского IP-адреса //***

Каспаров.ru (http://www.kasparov.ru/material.php?id=5D2888BC0CE73). 12.07.2019).

***

«Британский журналист Элиот Хиггинс, основавший исследовательскую группу Bellingcat, заявил, что проект стал мишенью для хакеров. Он связал кибератаки с резонансными расследованиями, касающимися России.

«Bellingcat считает себя мишенью кибератак, и, скорее всего, они связаны с нашей работой по России. Я полагаю, один из способов оценить наше влияние — посмотреть, как часто российские агенты пытаются атаковать нас, будь то хакеры, тролли или СМИ», — написал Хиггинс вTwitter. В недавнем интервью Forbes USA Хиггинс заявил, что история Bellingcat началась с катастрофы малазийского Boeing в Донбассе, унесшей жизни 298 человек. Исследовательская группа использовала находящиеся в открытом доступе фотографии и видеозаписи, чтобы отследить передвижения зенитно-ракетного комплекса «Бук« к месту пуска ракеты, которая сбила самолет Boeing 777. Затем команда Bellingcat воспользовалась онлайн-источниками и установила, что данный ЗРК «Бук» принадлежал 53-й бригаде ПВО Вооруженных сил Российской Федерации. Российские власти причастность к авиакатастрофе отрицают.» ***(Основатель Bellingcat заявил об атаках российских хакеров // Новости Великобритании на русском языке (https://theuk.one/osnovatel-bellingcat-zayavil-ob-atakax-rossijskix-xakerov/). 29.07.2019).***

***

«Комитет по разведке Сената США опубликовал в четверг отредактированную первую часть отчета, в котором содержатся некоторые итоги расследования о вмешательстве России в выборы 2016 года…

По мнению сенаторов, избирательная система США по-прежнему уязвима перед возможными кибератаками.

В частности, сенаторы выяснили, что Россия начала подготовку к вмешательству в президентские выборы как минимум в 2014 году, и эти попытки продолжались вплоть до 2017 года. Авторы отчета соглашаются с выводом, к которому пришел спецпрокурор Роберт Мюллер: факт вмешательства неоспорим, однако злоумышленникам не удалось повлиять на исход голосования или помешать работе избирательных комиссий.

При этом сенаторы считают, что федеральное правительство недостаточно тесно контактировало с властями штатов и не сообщало на места о реальном масштабе угрозы со стороны России. Авторы отчета рекомендуют Министерству внутренней безопасности улучшить процесс координации работы с властями штатов…» ***(Сенаторы США предупредили, что Россия снова попробует вмешаться в выборы // mediahouse.com.ua (http://mediahouse.com.ua/senatory-ssha-predupredili-chto-rossiya/). 26.07.2019).***

***

«…Береговая охрана США предупредила о кибератаке, направленной на компьютерную систему одного из судов, и рекомендовала судовладельцам принять эффективные меры по обеспечению кибербезопасности сети и важных систем управления на своих кораблях.

Инцидент произошел в феврале 2019 года, когда одно из суден подверглось атаке с использованием вредоносного ПО, «значительно ухудшившего функциональность бортовой компьютерной системы». Хотя основные системы управления судна не пострадали от хакерской атаки, она является примером того, что судовладельцы не заботятся должным образом об обеспечении безопасности своего транспорта.

В пресс-службе не уточнили, против какого именно судна была проведена хакерская атака и какое вредоносное ПО для этого использовалось.

В качестве превентивных мер Береговая охрана порекомендовала операторам и владельцам судов сегментировать свою сеть для того, чтобы усложнить злоумышленникам доступ к критическим системам и оборудованию, исключить использование одинаковых учетных данных несколькими сотрудниками, установить антивирусное программное обеспечение и регулярно обновлять его, ограничить уровень прав для пользователей, которым не нужен доступ администратора, проверять внешние носители (USB-накопители и пр.) перед их подключением к сети судна и устанавливать патчи и обновления ОС и приложений.» ***(Береговая охрана США сообщила о хакерской атаке на один из коммерческих кораблей // SecurityLab.ru (https://www.securitylab.ru/news/499865.php). 09.07.2019).***

***

«…Ответственная за электроснабжение финансовой столицы Южной Африки Йоханнесбурга компания City Power заявила в своем аккаунте в Twitter о совершенной на нее масштабной кибератаке. Злоумышленники использовали вымогательское ПО, которое зашифровало базы данных, приложения и сеть City Power.

Произошедшая 25 июня 2019 года кибератака привела к тому, что многие жители Йоханнесбурга, пользующиеся тарифом с предоплатой остались без электроэнергии. Жители города продолжают звонить на местные радиостанции и жаловаться на проблему. Клиенты City Power до сих пор не могут зайти на web-сайт компании, просмотреть и оплатить счета.

В настоящее время сотрудники IT-отдела продолжают бороться с последствиями заражения. О каком именно вредоносном ПО идет речь, компания не сообщает…» ***(Из-за кибератаки жители Йоханнесбурга остались без электричества // SecurityLab.ru (https://www.securitylab.ru/news/500167.php). 26.07.2019).***

***

«24 июля 2019 года Федеральная торговая комиссия (FTC) объявила о наложении на Facebook штрафа в размере $5 млрд за то, что социальная сеть потеряла контроль над пользовательскими данными, а также продавала их рекламодателям и другим компаниям.

Как отмечает CNN, $5 млрд — это самый крупный штраф от FTC, он в 20 раз больше прежде рекордного взыскания и примерно соответствует месячной выручке Facebook. Ранее интернет-компания заложила в список возможных трат «непредвиденные расходы» в $3–5 млрд из-за расследования властей США.

Facebook согласилась на сделку после многолетних нарушений своей политики конфиденциальности. Последней каплей стал скандал, когда аналитическая компания Cambridge Analytica получила данные 87 млн пользователей Facebook и использовала их для изучения политических предпочтений избирателей и демонстрировала им соответствующую рекламу.

«Facebook выплатит рекордный штраф в размере $5 млрд и введёт новые ограничения и изменения в свою корпоративную структуру, что возложит на компанию ответственность за решения, которые она принимает в отношении конфиденциальности данных своих пользователей», — говорится в сообщении FTC от 24 июля 2019 года.

По данным регулятора, Facebook нарушила законодательство, злоупотребив телефонными номерами, которые должны были применяться только для безопасности учётных записей, но в конечном итоге использовались в рекламных целях.

Кроме того, компания обманула «десятки миллионов пользователей», заявляя, что функция распознавания лиц в сервисе не была включена по умолчанию. На самом деле она была активна, говорят в FTC.

Председатель Федеральной торговой комиссии США Джозеф Симонс (Joseph Simons) отметил, что этот штраф наложен не только для того, чтобы показать, как будут наказывать за подобное в будущем, но и для изменения «всей культуры конфиденциальности Facebook, чтобы уменьшить вероятность новых нарушений». ***(Facebook оштрафовали на рекордные $5 млрд // IKSMEDIA.RU (http://www.iksmedia.ru/news/5599785-Facebook-oshtrafovali-na-rekordnye.html). 24.07.2019).***

***

«Управление комиссара по информации Великобритании (ICO) оштрафовало British Airways (BA) и его материнскую компанию International Airlines Group (IAG) на рекордную сумму — 183,39 млн фунтов стерлингов (230 млн долларов) — в связи с произошедшим в прошлом году инцидентом, который затронул более 500 тысяч клиентов.

В сентябре 2018 г. BA сообщила, что хакеры украли данные около 380 000 клиентов за две недели с сайта и мобильного приложения авиакомпании. Данные клиентов (имена, адреса электронной почты, за исключением паспортных данных)

хакеры украли в разгар сезона летних каникул, с 21 августа по 5 сентября. В октябре того же года авиакомпания заявила, что помимо этого хакеры получили данные кредитных карт 185 000 клиентов. Речь идет о номерах карт, сроках истечения их действия и трехзначном коде CVV, указанном на обороте карт.

Максимально возможный штраф в Великобритании за утечку данных составляет 4% от оборота компании, а наложенный на British Airways составил 1,5% от мирового оборота, став самым большим, который был когда-то вынесен.

Важность такого прецедента профильное издание Techcrunch видит в следующем:

«…это показывает, что утечка данных может быть не просто обязанностью, в случае ошибки приводящей к репутационным рискам, но и финансовой ответственностью».

Степень ответственности, которую компании будут нести за эти виды нарушений, станет гораздо более прозрачной в будущем: объявление ICO является частью новой директивы по раскрытию подробностей о её штрафах и расследованиях для общественности.

«Личные данные людей — это просто личные данные, — заявила комиссар по информации Элизабет Денхем. — Когда организация не может защитить ее от потери, повреждения или кражи, это больше, чем неудобство. Вот почему закон гласит — когда вам доверяют личные данные, вы должны следить за ними».

В заявлении ICO говорится, что штраф связан с нарушениями Общего регламента защиты данных (GDPR), который вступил в силу в прошлом году до нарушения, допущенного BA.

«Мы удивлены и разочарованы решением ICO. British Airways быстро отреагировала на преступное деяние с целью кражи данных клиентов. Мы не нашли никаких доказательств мошенничества со счетами, связанными с кражей данных», – заявил председатель правления и главный исполнительный директор British Airways Алекс Круз.

В свою очередь, исполнительный директор International Airlines Group Вилли Уолш сообщил, что компания собирается оспорить штраф. На подачу апелляции у British Airways будет 28 дней, отметил он.» ***(British Airways оштрафовали на £183 млн за утечку данных клиентов // РосКомСвобода (https://roskomsvoboda.org/48083/). 08.07.2019).***

***

«…Учетные данные пользователей крупного российского интернет-магазина Ozon оказались в открытом доступе. Обнаруженная база включала информацию об адресах электронной почты и паролях, связанных с более чем 450 тыс. учетных записей. На утечку обратили внимание журналисты РБК.

Издание выборочно проверило часть электронных адресов и выяснило, что все они актуальны, однако содержащие в базе пароли уже не действительны. Как полагают эксперты, утечка могла произойти около полугода назад, а база была сформирована из двух других БД, которые в ноябре 2018 года были замечены на одном из хакерских форумов.

Как заявили в Ozon, из 450 тыс. обнаруженных РБК логинов и паролей пользователям интернет-магазина принадлежит «не больше нескольких процентов» записей, а остальная информация относится к клиентам других сервисов. По данным компании, большая часть учетных записей являются неактивными. Представители Ozon отметили, что пристально следят за активностью таких профилей.

В компании также сообщили, что сбросили скомпрометированные пароли после сообщения об утечке и уведомили пользователей об инциденте.» ***(Логины и пароли пользователей Ozon обнаружены в открытом доступе // SecurityLab.ru (https://www.securitylab.ru/news/499918.php). 11 07.2019).***

***

«Самую крупную в мире гостиничную сеть Marriott International оштрафуют на сумму в £99 млн за утечку данных с 2014 года.

Управление уполномоченного по вопросам информации Великобритании (Information Commissioner's Office, ICO) оштрафует гостиничную сеть Mariott International на сумму в размере £99 млн ($123 млн) за нарушение Общего регламента по защите данных (GDPR).

Речь идет об утечке данных, обнаруженной в ноябре 2018 года, когда компания выявила компрометацию базы данных ее дочернего предприятия Starwood Hotels. В руки злоумышленников попала личная информация примерно 339 млн постояльцев. База данных включала имена гостей, почтовые адреса, номера телефонов, адреса электронной почты, даты рождения, информацию о поле, прибытии и отъезде, даты бронирования и пр. Атакующие заполучили 5,25 млн незашифрованных и 20,3 млн зашифрованных паролей, а также незашифрованные данные 8,6 млн банковских карт.

Как показало внутреннее расследование, у злоумышленников был доступ к системе еще с 2014 года. Расследование ICO выявило, что Mariott провела недостаточную проверку при покупке компании Starwood и не защитила свою систему должным образом…» ***(Вслед за British Airways за утечку данных оштрафуют Marriott International) // SecurityLab.ru (https://www.securitylab.ru/news/499905.php). 10.07.2019).***

***

«У країні з 7-мільйонним населенням були викрадені дані 5 млн болгар, - практично всіх дорослих жителів країни…

Урядові бази даних містять величезну кількість інформації, яка може бути «корисною» на довгі роки, вважають експерти.

Болгарська комісія із захисту персональних даних заявила, що почне розслідування злому.

Представник Національного податкового управління не повідомила, чи були дані належним чином захищені. У зв'язку зі зломом болгарська поліція заарештувала 20-річного працівника служби кібербезпеки.

За даними софійській прокуратури, комп'ютер і програмне забезпечення, використані при зломі, поліцію до підозрюваного привели.

Чоловік був затриманий, і поліція конфіскувала його обладнання, включаючи мобільні телефони, комп'ютери та диски, йдеться в заяві прокуратури.» ***(У Болгарії хакери зламали урядову базу з даними на все доросле населення // Чорноморські новини (https://www.blackseanews.net/read/152991). 22.07.2019).***

***

«У Болгарії відпустили на свободу 20-річного чоловіка, затриманого раніше за підозрою в скоєнні хакерської атаки на Національне податкове управління, в ході якої були викрадені особисті та фінансові дані мільйонів мешканців країни…

Прокуратура Софії звільнила затриманого днями раніше болгарина Крістіана Бойкова під підписку про невиїзд.

Звинувачення проти Бойкова перекваліфікували: замість кібератаки на критично важливий об'єкт інфраструктури йому закидають звичайний злом інформаційної системи. IT-фахівець знову повернувся на роботу, його начальство вважає його невинним. Слідство у справі про кібератаку триває…

Міністр внутрішніх справ Младен Маринов повідомив, що вкрадені дані хакери надіслали болгарським ЗМІ електронною поштою, зареєстрованою на російському сервері.

Він сказав, що кібератаки, ймовірно, мотивовані кроком Болгарії з метою купити вісім нових винищувачів Lockheed Martin F-16 за $ 1,256 мільярда у Сполучених Штатів. Це найбільша військова покупка Софії після падіння комунізму.» ***(Підозрюваний у кібератаці на податкове відомство Болгарії вийшов на свободу // Чорноморські новини (https://www.blackseanews.net/read/152969). 19.07.2019).***

***

«Компания Canonical, куратор проекта Ubuntu Linux, столкнулась с неприятным киберинцидентом. Неизвестные лица получили доступ к ее учетной записи на GitHub и создали 11 новых репозиториев, которые оставили пустыми.

Согласно заявлению в Twitter, стороннее вмешательство было обнаружено 6 июля; злоумышленникам удалось каким-то образом заполучить регистрационные данные Canonical на GitHub.

Взломанный аккаунт уже удален, ведется расследование. Признаков компрометации исходных кодов или информации личного характера на настоящий момент не выявлено.

Поскольку разработка и корректировка дистрибутивов Ubuntu осуществляется на хостинг-платформе Launchpad, не связанной с Github, пользователей заверили, что Ubuntu-инфраструктура не пострадала. В настоящее время Canonical проверяет хранимые на GitHub исходники, чтобы оценить размеры ущерба, и обещает обнародовать результаты по завершении расследования…» ***(Maxim Zaitsev. Взлом GitHub-аккаунта Canonical не затронул Ubuntu // Threatpost (https://threatpost.ru/canonical-github-account-hacked-ubuntu-unaffected/33392/). 09.07.2019).***

***

«Специалисты исследовательской группы vpnMentor обнаружили в открытом доступе базу данных, содержащую конфиденциальные данные пользователей умных приборов китайского вендора Orvibo. По словам аналитиков, любой желающий может получить сведения из более чем 2 млрд логов, сформированных IoT-устройствами, в частности логины, пароли, и их местоположение.

ИБ-эксперты проинформировали производителя об утечке еще 16 июня по электронной почте и, не получив ответа в течение нескольких дней, написали на официальный Twitter-аккаунт компании. Попытки связаться с производителем также предпринимали журналисты портала BleepingComputer, однако ни в одном случае реакции вендора не последовало.

Orvibo выпускает около 100 моделей оборудования для умных домов, которые устанавливают как частные пользователи, так и организации. Список доступных устройств включает электронные замки, камеры видеонаблюдения и системы управления освещением. Как заявили специалисты vpnMentor, в обнаруженных ими базах данных хранятся:

- адреса электронной почты;
- пароли;
- коды для сброса аккаунта;
- точные координаты устройств;
- IP-адреса;
- имена и идентификаторы пользователей;
- фамилии владельцев оборудования;
- семейные идентификаторы;
- название IoT-приборов;
- данные о других подключенных устройствах;
- календарь пользователя.

Эксперты отмечают, что анализ логов показал избыточность сведений, собираемых оборудованием Orvibo о владельце. Так, местоположение устройства определяется не по IP-адресу, а хранится в виде точных географических координат.

Обладая скомпрометированными данными, злоумышленники способны организовать широкий спектр атак, включая проникновение в жилище жертвы. Как утверждают ИБ-специалисты, при помощи кода для сброса аккаунта киберпреступники могут поменять не только пароль, но и электронный адрес пользователя, полностью перехватив управление устройством. Через взломанный профиль нападающие получат возможность манипулировать видеокамерами, электронными замками, освещением и розетками…» ***(Egor Nashilov. Миллионы IoT-устройств Orvibo под угрозой взлома // Threatpost (https://threatpost.ru/orvibo-leaks-pretty-much-everything/33330/). 02.07.2019).***

***

«Исследователь в сфере кибербезопасности Сэм Джидали (Sam Jidali) недавно обнаружил огромную утечку данных, раскрывающую личную

информацию миллионов людей и 45 крупных компаний. Названная «DataSpii» Джидали и его командой, утечка была вызвана совершенно неприметными на первый взгляд расширениями для браузеров Chrome и Firefox, которые собирали и распределяли данные о действиях пользователей в сети — URL-адреса, которые раскрывали личную информацию о пользователях, а также длинный список компаний, включающий Apple, Walmart , Amazon, 23AndMe, SpaceX, Skype и многие другие. (Полный список можно посмотреть в отчете Джидали).

Восемь опасных расширений для браузеров

Вот восемь расширений, используемых для слежки за пользователями:

Branded Surveys (Chrome)

FairShare Unlock (Chrome and Firefox)

HoverZoom (Chrome)

Panel Community Surveys (Chrome)

PanelMeasurement (Chrome)

SaveFrom.net Helper (Firefox)

SpeakIt! (Chrome)

SuperZoom (Chrome and Firefox)

Исследователь сообщил об обнаруженной утечке компаниям Chrome и Mozilla, которые ответили удаленным отключением расширений и удалением их из своих специализированных онлайн-магазинов. Тем не менее, Джидали продолжал следить за активностью этих отключенных браузерных расширений, впоследствии обнаружив, что они по-прежнему отслеживают пользовательские данные, хотя их основные функции и были отключены.

Другими словами, лучше удалите все расширения, приведённые выше, если используете какое-либо из них. В то время как некоторые из этих расширений имели не более 10 пользователей, другие обладали пользовательской базой, состоящей из нескольких сотен тысяч (и иногда свыше миллиона) человек.

Каждое из этих расширений отслеживало данные по-разному и использовало собственную хитрую тактику — например, ожидало до 24 дней после установки, и только потом активировалось и начинало процесс слежки, тем самым запутывая процесс сбора данных...

Джидали также предупредил компании, чья информация также была раскрыта, и они смогли подтвердить выводы Джидали. Утечка данных включала в себя конфиденциальную корпоративную информацию и компрометирующие пользовательские данные, такие как имена сотрудников, адреса, данные кредитных карт, пароли и ПИН-коды, хранимые в облаке файлы и многое другое — в некоторых случаях даже документы из налоговой, генетическую информацию и историю болезни…» ***(Браузерные расширения крадут данные // Український телекомунікаційний портал (https://portaltele.com.ua/news/events/brauzernye-rasshireniya-kradut-dannye.html). 21.07.2019).***

***

«…Разработчики браузера Pale Moon сообщили о взломе неизвестными злоумышленниками их архивного сервера, в результате чего хранящиеся на нем файлы были заражены вредоносным ПО.

Pale Moon – браузер с открытым исходным кодом, ориентированный на кастомизацию и повышение производительности. Браузер базируется на коде Firefox, но использует собственный движок Goanna. В прошлом году число пользователей Pale Moon колебалось в пределах от 750 тыс. до 1,25 млн.

По словам разработчиков, архивный сервер archive.palemoon.org был взломан, и в хранящиеся на нем исполняемые файлы, в том числе установщики и PE-файлы, был внедрен загрузчик вредоносного ПО, детектируемый решениями ESET как Win32/ClipBanker.DY. Когда жертва запускает зараженный файл, на ее систему устанавливается бэкдор.

Инцидент был обнаружен 9 июля, и разработчики незамедлительно отключили скомпрометированный сервер. Тем не менее, как показывают временные метки в файлах, злоумышленники получили к нему доступ еще в декабре 2017 года. Киберпреступники могли подделать временные метки, однако, судя по резервным копиям файлов, даты являются достоверными. Похоже, злоумышленники внедряли загрузчик не удаленно, а локально, добавив в каждый файл по 3 дополнительных мегабайта.

Расследование инцидента затруднено отсутствием достаточного количества данных, уничтоженных в результате отключения сервера в мае нынешнего года. Неожиданно сервер вышел из строя, и все записи реестра пропали, поэтому сложно установить, каким образом злоумышленникам удалось в него поникнуть.

По мнению разработчиков браузера, взлом стал возможным из-за недостаточной защиты сервера со стороны хостинг-провайдера. По этой причине команда Pale Moon сменила хостинг-провайдера.

Злоумышленники заразили исполняемые файлы для версии Pale Moon 27.6.2 и более ранних. Файлы, хранящиеся за пределами архивного сервера, не были затронуты атакой. Пользователям, загрузившим браузер не с archive.palemoon.org, опасаться нечего. Тем же, кто мог получить зараженную версию Pale Moon, рекомендуется провести полное сканирование системы на наличие вредоносного ПО.» ***(Взломанный сервер Pale Moon распространял зараженные версии браузера // SecurityLab.ru (https://www.securitylab.ru/news/499942.php). 12.07.2019).***

***

«Американські компанії у 2018 році зазнали збитків на 45 мільярдів доларів через кібератаки. Згідно дослідження Online Trust Alliance, хакери провели 2 мільйони нападів.

«Фінансові наслідки кіберзлочинності значно збільшуються, а кібер-злочинці стають більш кваліфікованими. Таким чином, кількість кібер-інцидентів та фінансових втрат є набагато більшими, ніж ми фіксували до цього», – пояснює Джеф Уілбур, технічний директор інтернет-асоціації.

Із 2 млн випадків атак у минулому році, 95% можна було уникнути за допомогою поліпшення безпеки. Також асоціація назвала найпопулярніші види кібератак:

– напади на ланцюги постачання товарів
– атаки на електронну пошту
– криптовалютні кібератаки
– напади на органи влади

зламування хмарних сервісів і доступ до облікових записів…» ***(Кібератаки завдали США збитків на десятки мільярдів // UA.NEWS (https://ua.news/ua/kiberataky-zavdaly-ssha-zbytkiv-na-desyatky-milyardiv/). 10.07.2019).***

***

«Операторы вредоносных кампаний фокусируются на незащищенных подключениях удаленного доступа, отказываясь от массированных email-рассылок и других методов доставки полезной нагрузки. В сегодняшних реалиях онлайн-сканеры мгновенно обнаруживают уязвимый сервер, после чего он оказывается под постоянной атакой.

К таким выводам пришли ИБ-эксперты, которые в течение месяца наблюдали за попытками взломать 10 ханипотов с доступом по RDP (Remote Desktop Protocol, протокол удаленного доступа). В качестве приманок выступали виртуальные машины Amazon под управлением Windows Server 2019. Их базовая конфигурация допускает RDP-подключение, что делает такие хосты желанной целью для операторов зловредов, таких как шифровальщики SamSam, Dharma, Scarabey.

В ходе исследования первая попытка неправомерного доступа произошла менее чем через полторы минуты после запуска виртуальных машин. В последующие 15 часов онлайн-сканеры нашли все созданные ханипоты. После обнаружения приманки попытки взломать ее происходили в среднем каждые шесть секунд. Всего же за период исследования системы зарегистрировали 4,3 млн таких инцидентов…» ***(Egor Nashilov. Взломщики находят уязвимый RDP-хост за 90 секунд // Threatpost (https://threatpost.ru/number-of-rdp-attacks-increased-300-times/33532/). 18.07.2019).***

***

«ИБ-специалисты обнаружили и пресекли вредоносную кампанию в Facebook, построенную вокруг темы гражданской войны в Ливии. Организатор атак использовал актуальную новостную повестку, чтобы красть конфиденциальные материалы и заражать пользователей зловредным ПО.

Расследование началось, когда эксперты обнаружили в социальной сети поддельный профиль генерала Халифы Хафтара, одного из главных участников ливийских событий последних лет. С момента создания страницы в апреле 2019 года на нее подписались более 11 тыс. пользователей. Владелец профиля публиковал записи на политические темы, прикрепляя к ним ссылки, которые якобы ведут на секретные материалы спецслужб. На самом деле по этим адресам находились вредоносные программы для Windows и Android.

Исследователи назвали в их числе системы скрытного доступа Remcos, SpyNote и Houdini, исходники которых размещены в хранилищах Google Drive, Dropbox и Box. Злоумышленнику также удалось скомпрометировать несколько легитимных ресурсов, включая сайт одного из крупнейших ливийских мобильных операторов Libyana.

Характерные опечатки в тексте постов и адресе профиля позволили экспертам составить карту более чем 30 вредоносных страниц, используемых в обнаруженных атаках. Некоторые из них украдены у реальных пользователей, другие созданы специально для проведения атак.

По словам специалистов, фальшивых профилей оказалось множество, и все они находились под контролем одного человека, который запустил кампанию еще в 2014 году. За это время он собрал свыше 100 тыс. подписчиков. Злоумышленник не поддерживал какую-либо сторону ливийского противостояния, используя общественно-политическую повестку исключительно для привлечения потенциальных жертв.

В некоторых случаях он и вовсе отходил от основной темы, чтобы сыграть на других громких событиях. Так, в 2018 году один из зловредов продвигался как средство бесплатного просмотра матчей Чемпионата мира по футболу. В другой раз преступник распространял троян под видом VPN-клиента.

Поскольку мошенник маскировал вредоносные URL с помощью укороченных ссылок, эксперты смогли изучить статистику переходов и сделать вывод об успешности выбранной злоумышленником стратегии — большинство записей собирали тысячи кликов.

После изучения всех деталей кампании исследователи определили Facebook-профиль человека, который с высокой долей вероятности стоит за всеми этими атаками. Им оказался некий Декстер Ли (Dexter Ly) — житель Ливии, который регулярно размещал материалы по теме киберпреступности. В них эксперты обнаружили, помимо прочего, скриншоты онлайн-панелей, обеспечивающих управление вредоносными кампаниями.

Пользователь также выкладывал секретную информацию, до которой ему удалось добраться. Среди этих данных были документы ливийского правительства, электронная переписка и телефоны чиновников, фотокопии их паспортов. В итоге исследователи отследили деятельность Ли до участия в группировке OpSyria, подразделении Anonymous, которое объявило своей целью борьбу с сирийским правительством.

Эксперты передали материалы расследования представителям Facebook, которые заблокировали все уличенные в нежелательной деятельности страницы…» ***(Egor Nashilov. Хактивист организовал многолетнюю кибератаку в Facebook // Threatpost (https://threatpost.ru/operation-tripoli-deconstructed/33349/). 05.07.2019).***

***

«Эксперты «Лаборатории Касперского» зафиксировали серию целевых атак на российские организации из сферы здравоохранения. Инциденты произошли весной и в начале лета этого года, жертвами злоумышленников стали несколько учреждений в южных регионах России.

Как выяснили аналитики, атакующие свободно говорят на русском языке, однако территориально находятся за пределами России. Основной целью злоумышленников был сбор данных финансового характера.

Заражение компьютеров в организациях, работающих в сфере здравоохранения, осуществлялось с помощью неизвестной ранее программы-шпиона CloudMid. Зловред рассылался по электронной почте и маскировался под VPN-клиент известной российской компании. Однако эта рассылка не была массовой: почтовые сообщения, содержащие программу-шпиона, получили лишь некоторые организации отдельных регионов, а это говорит о целевом характере атаки.

После установки в системе CloudMid приступал к сбору документов, хранящихся на заражённом компьютере. Для этого, в частности, зловред делал снимки экрана несколько раз в минуту. Эксперты «Лаборатории Касперского» обнаружили что атакующие собирают с зараженных машин информацию финансового характера: контракты, направления на дорогостоящее лечение, счета-фактуры и другие документы, которые так или иначе относятся к финансовой деятельности организаций здравоохранения…». ***(Российские организации из сферы здравоохранения столкнулись с целенаправленным кибершпионажем // IKSMEDIA.RU (http://www.iksmedia.ru/news/5599022-Rossijskie-organizacii-iz-sfery-zdr.html). 19.07.2019).***

***

«Министерство внутренних дел Беларуси заявляет о волне кибератак на белорусские предприятия разных форм собственности.

"Мошенники атакуют белорусские предприятия!!! Волна кибервирусов прокатилась по белорусским предприятиям всех форм собственности!" – сообщила в телеграм-канале пресс-секретарь МВД Ольга Чемоданова.

"Сотрудниками УРПСВТ МВД уже зафиксировано более 10 подобных кибератак. Последний случай списания средств произошел в столице, где фирма лишилась 14 тысяч рублей", - сообщила пресс-секретарь.

"В то время, когда сотрудники фирмы не предпринимают действий, запускается вредоносный процесс. Формируется фиктивное платежное поручение на перевод финансовых средств на расчетный счет мошенникам", - поясняется в сообщении.

Пресс-секретарь подчеркивает, что в целях безопасности не следует активировать прикрепленные к электронному письму файлы, если нет уверенности в отправителе. Также не следует оставлять в компьютере электронный ключ - вирусный алгоритм использует его при генерировании платежного поручения…» ***(МВД Беларуси заявило о волне кибератак на предприятия // ua-ru.info (http://ua-ru.info/news/142081-mvd-belarusi-zayavilo-o-volne-kiberatak-na-predpriyatiya.html). 25.07.2019).***

***

«В 2018 г. FinCERT Банка России (центр мониторинга и реагирования на компьютерные атаки) получил сведения о 687 кибератаках на банки, говорится в отчете организации. Из них 177 атак были целевыми атаками на кредитно-финансовые организации ради финансовой выгоды.

Также FinCERT насчитал 97 DDoS-атак на финансовые организации.

В прошлом году FinCERT зафиксировал 375 кампаний по распространению вредоносного ПО, из которых 71 была нацелена на кредитно-финансовые организации и их клиентов.

Множество таких атак на банки организация приписывает двум хакерским группировкам: Cobalt (также известна как Carbanak и FIN7) и Silence. По данным FinCERT, Cobalt нанесла ущерб российской финансовой сфере минимум на 44 млн руб., а Silence – на 14,4 млн руб. Впрочем, это во много раз меньше, чем в 2017 г., отмечается в отчете. В 2017 г. ущерб от атак с использованием программ Cobalt Strike превысил 1 млрд руб.

Несмотря на арест в марте 2018 г. в Испании одного из лидеров Cobalt и задержание в Европе еще нескольких ее членов, группа свою деятельность не прекратила, а лишь снизила активность на некоторое время, говорится в отчете.

Также FinCERT выявил более 540 ресурсов в интернете, которые распространяют вирусное ПО или управляют серверами, отвечающими за использование вредоносного софта. Более 500 подобных ресурсов зарегистрированы за пределами России. Эти доменные зоны неподконтрольны FinCERT, что затрудняет возможность остановить их деятельность, отмечается в докладе. Сейчас прорабатывается законопроект, который позволит Банку России блокировать такие ресурсы до суда на территории России вне зависимости от географической привязки доменного имени…

FinCERT также приводит наблюдения компаний в области кибербезопаности. Так, например, эксперты лаборатории компьютерной криминалистики Group-IB пришли к выводу, что в 2018 г. на финансовый сектор пришлось около 70% всей хакерской активности. При этом 74% банков были не готовы к атакам, отмечает Group-IB: более чем у половины банков были выявлены следы совершения атак в прошлом, они не смогли централизованно управлять сетью для локализации атаки, а также тратили на согласование работ по ликвидации атаки более четырех часов.

Эксперты Group-IB также проанализировали атаки на клиентов банков: более 80% случаев похищения у них денег происходит с использованием методов социальной инженерии. Мошенники звонят жертвам и представляются сотрудниками банка, предлагая услуги, или представителями службы безопасности, которая якобы обнаружила подозрительную активность. В 2018 г. банки ежемесячно сталкивались в среднем с 3000 атак с использованием таких методов.

За прошлый год мошенникам удалось похитить почти в 1,5 раза больше денег с карт россиян – 1,4 млрд руб., по данным ЦБ, это на 44% больше, чем годом ранее. До этого улов мошенников снижался три года подряд. Большинство случаев хищения денег связано с социальной инженерией, говорилось в отчете FinCERT за

2018 г.» ***(Алена Сухаревская. ЦБ зафиксировал почти 700 кибератак на банки в прошлом году // АО Бизнес Ньюс Медиа (https://www.vedomosti.ru/finance/articles/2019/07/05/805928-bank-rossii). 05.07.2019).***

***

«…Киберпреступная группировка Sea Turtle атаковала организацию ICS-Forth, управляющую греческими доменами верхнего уровня .gr и .el.

О группировке Sea Turtle специалисты Cisco Talos впервые рассказали в апреле нынешнего года. Злоумышленники используют весьма необычную технику взлома – вместо того, чтобы атаковать непосредственно жертву, они получают доступ к учетным записям регистратора домена и провайдеров управляемого DNS и меняют настройки DNS компании.

Путем модификации записей DNS внутренних серверов злоумышленники перенаправляют трафик, предназначенный для легитимных приложений и почтовых серверов компании, на подконтрольные им серверы, осуществляют атаку «человек посередине» и перехватывают учетные данные.

Вышеописанные атаки являются непродолжительными (длятся от нескольких часов до нескольких дней) и незаметными (большинство компаний не проверяют настройки DNS на предмет изменений). По данным FireEye, группировка действует в интересах правительства Ирана.

Для того чтобы добраться до жертвы, Sea Turtle не гнушается взламывать сети провайдера целиком. Как сообщалось в первом отчете Cisco Talos, группировка взломала шведскую организацию NetNod, управляющую точкой обмена трафиком. Атака позволила злоумышленникам манипулировать записями DNS для sa1[.]dnsnode[.]net и получить доступ к учетным данным администратора доменов верхнего уровня Саудовской Аравии (.sa)

В новом отчете Cisco Talos сообщает об аналогичной атаке на греческую организацию ICS-Forth. На данный момент исследователи затрудняются сказать, что атакующие делали в сетях ICS-Forth после взлома. Неизвестно также, для каких доменов злоумышленники поменяли настройки DNS. После того, как организация уведомила общественность о взломе, Sea Turtle оставалась в ее сетях еще пять дней.» ***(Киберпреступники атакуют компании через их DNS-провайдеров // SecurityLab.ru (https://www.securitylab.ru/news/499907.php).10.07.2019).***

***

«Хакери зламали сервери компанії-підрядника SyTech, вкрали 7,5 терабайта даних Федеральної служби безпеки Росії та передали інформацію для оприлюднення.

Про це повідомила російська служба BBC. Злом стався 13 липня 2019 року. Замість головної сторінки сайту московської IT-компанії SyTech з'явилося зображення відомого мему з широкою посмішкою і самовдоволено примруженими очима.

Заміна головної сторінки сайту є поширеною тактикою хакерів і демонстрацією того, що їм вдалося отримати доступ до даних жертви.

Знімок головної сторінки ФСБ РФ з'явився у твіттер-акаунті 0v1ru$, зареєстрованому в день атаки. Там же з'явилися скріншоти папки «Комп'ютер», яка ймовірно належала жертві. На одному знімку видно загальний обсяг інформації – 7,5 терабайта. На іншому знімку видно, що більша частина цих даних вже видалена.

Зазначається, що хакери відправили документи журналістам кількох видань та групі Digital Revolution, яка відома спробами попередніх хакерських нападів на ФСБ.

У документах начебто містяться описи десятків непублічних проєктів в області інтернету: від деанонімізація користувачів браузера Tor до дослідження уразливості торрентів. Хакери також оприлюднили назви таємних проектів: «Аріон», «Надія», «Відносини», «Гривня», а також імена деяких співробітників SyTech.

З архіву, з яким змогла ознайомитися Російська служба BBC, вихожить, що SyTech виконувала роботи у щонайменше 20 непублічних IT-проектах, замовлених російськими спецслужбами і відомствами. Ці папери не містять позначок про державну таємницю або секретність.» ***(Хакери вкрали 7,5 терабайта даних ФСБ – ЗМІ // MediaSapiens (https://ms.detector.media/web/cybersecurity/khakeri_vkrali_75_terabayta_danikh_fsb_zmi/). 21.07.2019).***

***

«Хакери зламали сайт, пошту і Twitter Служби столичної поліції Лондона (Скотленд-Ярд) в п'ятницю ввечері…

Зловмисники заповнили Twitter відомства образливими висловлюваннями на адресу поліції і жартівливими новинами, а також опублікували фальшиві заяви на офіційному сайті.

Прес-секретар Скотлен-Ярду Рой Сміт написав в своєму Twitter, що поліція працює над відновленням контролю над своїми обліковими записами.» ***(Ілля Нежигай. Хакери зламали сайт, пошту та Twitter Скотленд-Ярду // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1814216-khakeri-zlamali-sayt-poshtu-ta-twitter-skotlend-yardu). 20.07.2019).***

***

«Экперты центра безопасности Positive Technologies (PT Expert Security Center) исследуют активность злоумышленников из RTM с 2018 года. Интересы кибергруппы шире, чем только финансовые компании: например, их атаки затрагивают также сферу промышленности. При этом, вместе с известными группировками Cobalt и Silence, RTM входит в тройку самых активных кибергруппировок, атакующих российских финансовый сектор. Преступники стремятся получить контроль над счетами атакуемых организаций и похитить находящиеся на них средства.

Для получения доступа в корпоративную сеть группировка использует фишинговые рассылки. По данным PT Expert Security Center, за 2018 год

группировка провела 59 атак. С начала 2019 года было зафиксировано еще 45 атак. Эксперты PT Expert Security Center изучили формат фишинговых рассылок кибергруппировки RTM и выяснили, что в качестве одного из центров управления злоумышленники использовали домены в зоне .bit. Это специальная зона, созданная на базе блокчейна Namecoin, выступающего в роли альтернативного регистратора имен DNS.

Изучив особенности архитектуры блокчейна, эксперты PT Expert Security Center сумели разработать алгоритм отслеживания регистрации новых доменов группировки и смены их IP-адресов. Это позволило уведомлять кредитно-финансовые организации о новых управляющих серверах с небольшой задержкой после начала их использования злоумышленниками. «Проведенное исследование позволило нам выявлять признаки планируемой атаки до фишинговой рассылки, — говорит директор экспертного центра безопасности PT Expert Security Center Алексей Новиков. — Этого достаточно, чтобы заблокировать обновившиеся IP-адреса группировки. Даже если рассылаемое в письмах вредоносное ПО попадет в сеть организации, злоумышленники не смогут с ним связаться и контролировать его»…» ***(Эксперты PT Expert Security Center предсказывают атаки кибергруппировки RTM // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/eksperty-pt-expert-security-center-predskazyvayut-ataki-kibergruppirovki-rtm/). 22.07.2019).***

***

«По данным ИБ-экспертов, злоумышленники из группировки Magecart внедрили код скиммера в JavaScript-файлы более 17 тыс. сайтов, использующих облачные хранилища Amazon S3. Некоторые из атакованных веб-ресурсов входят в список 2000 самых посещаемых сайтов в рейтинге Alexa.

Как отмечают исследователи, киберпреступники начали сканировать Интернет в поисках доступных на запись контейнеров Amazon S3 в начале апреля этого года. В плохо защищенных корзинах они находили JavaScript-файлы и добавляли в них вредоносный код из коммерческого набора Inter Skimmer Kit. Последний почти год рекламировался на мошеннических площадках, и теперь им пользуются многие преступные группы.

«Злоумышленники использовали эту технику для создания как можно более широкой сети зараженных сайтов, но многие из скомпрометированных скриптов не загружаются на страницах оплаты. Тем не менее, простота атаки через общедоступные контейнеры S3 позволяет мошенникам окупить вложения даже в том случае, если платежную информацию похитит лишь часть внедренных ими онлайн-скиммеров», — пояснил журналистам исследователь Йонатан Клинсма (Yonathan Klijnsma).

По его словам, эта кампания демонстрирует, насколько легко злоумышленники могут скомпрометировать огромное количество сайтов, внедряя на них вредоносные скрипты через неправильно настроенные контейнеры S3. Администраторам веб-ресурсов Клинсма посоветовал использовать белые списки и отключить возможность чтения и редактирования документов посторонними на

серверах Amazon. Также, чтобы убедиться, что сайт не был скомпрометирован ранее, можно проверить логи и даты изменения файлов в контейнерах.

Это вторая кампания группировки Magecart за неделю: ранее эксперты обнаружили, что злоумышленникам удалось за сутки взломать 962 торговые площадки на базе CMS Magento. В ходе атак злоумышленники также внедряли на сайты скиммер.» ***(Egor Nashilov. Группировка Magecart внедрила скиммер на 17 тысяч веб-сайтов // Threatpost (https://threatpost.ru/magecart-implants-skimmer-to-17k-sites-via-aws-buckets/33463/). 12.07.2019).***

***

«…с электронного адреса лондонской полиции началась массовая рассылка писем странного содержания, затем серия «несанкционированных» сообщений появилась в Twitter-аккаунте ведомства.

В собщениях, которые впоследствии были удалены, содержались оскорбительные выражения и упоминались имена нескольких человек, передаёт BBC. В полиции Лондона сообщили, что пытаются установить причины произошедшего. Между тем, в адрес Скотленд-Ярда уже поступает критика с призывом усилить кибербезопасность. В противном случае скомпрометированными могут оказаться любые сообщения полиции. В частности, пресса и общественность могут усомниться, стоит ли полагаться на уведомления, которые могут быть разосланы в ходе вероятных террористических атак. В полиции пообещали выполнить эти требования…» ***(Британская полиция усилит кибербезопасность после атаки хакеров // Новости Великобритании на русском языке (https://theuk.one/britanskaya-policiya-usilit-kiberbezopasnost-posle-ataki-xakerov/). 21.07.2019).***

***

«…Хакеры рыщут по интернету в поисках фото, видео и другой информации, чтобы с ее помощью лучше спланировать атаку на вашу фирму. Об этом предупреждает Стефани Каррутерс (Stephanie Carruthers), известная в киберсообществе под псевдонимом Snow. Вместе с другими коллегами по “хакерскому цеху” она входит в команду X-Force Red подразделения IBM Security, специализирующегося на вопросах информационной безопасности…

Социальные сети и опубликованные в них фотографии – настоящая “золотая жила” для получения такой информации. Чего только не рассмотришь на заднем фоне снимков, сделанных в компаниях – от пропусков сотрудников в офис до незаблокированных экранов ноутбуков и приклеенных листочков-напоминалок с записанными на них паролями к Wi-Fi…

Не секрет, что самое слабое звено в системе кибербезопасности организаций – это сотрудники. За технической или программной уязвимостью нередко стоит человеческий фактор. Особенно это касается молодых специалистов и новичков, проходящих в компании стажировку или недавно занявших должность. По словам Каррутерс, в 75 процентах случаев нужную ей информацию она получает именно от таких сотрудников.

Молодые люди, приходящие сегодня в компании, выросли на соцсетях и привыкли выкладывать в интернет буквально все. А уж стажировка или новая работа – такая замечательная новость, чтобы ею поделиться. Ситуацию усугубляет то, что компании нередко проводят тренинги по кибербезопасности с новым персоналом лишь недели, а то и месяцы спустя после приема на работу. Вот вам и готовый рецепт уязвимости.

Зная это слабое место и несколько расхожих хэштегов, таких как #firstday, #newjob или #intern + [#companyname] (#первыйденьнаработе, #новаяработа, #стажировка + [#названиекомпании]), Каррутерс всего за несколько часов может найти в соцсетях массу полезной для хакера информации.

Многие не задумываются, что публикуя собственные и коллективные фотографии на рабочем месте, во время перерыва и какого-то корпоративного мероприятия, они раскрывают о себе больше информации, чем планировали. На фото могут случайно попасть различные детали, например, постеры и офисные доски с записями, которые хакер может использовать в своих интересах. Например, заметив на снимке постер с объявлением о скором проведении командного турнира по софтболу, киберзлоумышленник может отправить сотруднику электронное письмо со ссылкой якобы на расписание игр. Скорее всего, сотрудник не заподозрит ничего плохого и кликнет по линку… на самом деле вредоносному.

Также Каррутерс множество раз находила в соцсетях снимки, на которых крупном планом видны бейджи сотрудников, служащие пропуском в офис. Такие фото чаще всего публикуют новички и стажеры, когда выкладывают свои селфи в первый рабочий день. Зная, как выглядит бейдж, нетрудно изготовить дубликат и с его помощью проникнуть в офис…

Но настоящая находка для хакеров – это сотрудник-видеоблогер, решивший опубликовать ролик на тему “день в офисе”. По записи можно узнать и планировку здания, и места, где действует пропускная система. По схемам на офисных досках, которые случайно окажутся в кадре, можно изучить и планы компании. В общем, попадись такой ролик злоумышленнику – и считай, он сам побывал в офисе.

Кроме того, по изображениям на экранах офисных компьютеров можно понять, какой антивирус и другое программное обеспечение используются в компании. Зная это, хакер может изготовить персонализированное вредоносное ПО, замаскированное под обновление для одного из офисных приложений. Киберпреступники также могут воспользоваться информацией об имеющихся в компании проблемах. Выяснить, чем недовольны сотрудники, позволяют такие онлайн ресурсы, как Glassdoor, сайты поиска работы и, конечно, обсуждения в соцсетях.

Каррутерс с помощью таких сведений однажды устроила успешную фишинговую рассылку. В одной из компаний, киберзащиту которой тестировала команда X-Force Red, многие работники жаловались онлайн на нехватку парковочных мест. Каррутерс написала электронное письмо, в котором компания якобы разъясняла новую политику паркинга и предупреждала, что автомобили, оставленные не на своих местах, будут эвакуироваться. Метод социальной инженерии сработал на ура: взволнованные новостью о выделении мест для стоянки и напуганные тем, что машину может забрать эвакуатор, многие

сотрудники открывали вредоносное вложение к письму, выполненное в виде схемы парковки…» ***(Любители соцсетей – находка для хакеров // Український телекомунікаційний портал (https://portaltele.com.ua/news/internet/lyubiteli-sotssetej-nahodka-dlya-hakerov.html). 12.07.2019).***

***

«…По оценкам Европола, преступная группа Cobalt похитила около €100 млрд у банков из 40 стран, в том числе России, Беларуси, Малайзии, Испании, Великобритании.

Эксперты Всемирного экономического форума поставили кибератаки на третье место в рейтинге глобальных рисков по вероятности проявления и на шестое — по разрушительному воздействию. Государства не могут в одиночку противостоять киберугрозам: сказываются и масштабность проблемы, и различия в правовом регулировании. Мировой опыт борьбы с правонарушениями в основном связан с финансовыми расследованиями (форензик) и выявлением киберпреступлений как факта.» ***(Банкиры против хакеров. Какие технологии будут защищать клиентов от киберугроз // Новости Великобритании на русском языке (https://theuk.one/bankiry-protiv-xakerov-kakie-texnologii-budut-zashhishhat-klientov-ot-kiberugroz/). 15.07.2019).***

***

«…Десятый по размеру банк в США Capital One стал жертвой атаки хакеров. Злоумышленники украли личную информацию более 100 миллионов людей, имевших счета или кредиты в банке…

Отмечается, что финучреждение узнало об этом 19 июля, но сообщило только через полторы недели, когда ФБР арестовало в Сиэтле подозреваемую Пейдж Томпсон.

Ранее она разрабатывала программное обеспечение в компании Amazon Web Services, которая борется за контракт в размере $10 миллиардов на создание "облачного" сервиса для Пентагона. Банк уже подал иск против Томпсон в суд.

Кроме американцев, от хакерской атаки пострадали канадские вкладчики банка.

Злоумышленники украли информацию о датах рождения, доходах, номерах банковских счетов и карт, а также номерах социального страхования.

В Capital One убеждают, что эти данные не успели использовать с преступной целью. Банк обещает усилить меры кибербезопасности и потратить на это дополнительно $100-150 миллионов.» ***(Более 100 миллионов человек пострадали в результате хакерской атаки на банк в США // Телеграф (https://telegraf.com.ua/mir/usa/5110517-bolee-100-millionov-chelovek-postradali-v-rezultate-hakerskoy-ataki-na-bank-v-ssha.html). 31.07.2019).***

***

«…Эксперты в области безопасности продемонстрировали новую атаку по сторонним каналам, позволяющую вредоносным приложениям перехватывать голосовые данные, исходящие с динамиков смартфона без какого-либо разрешения.

Новый метод, получивший название Spearphone, задействует акселерометр, встроенный в большинство Android-устройств. Доступ к этому датчику может получить любое приложение, включая программы, не имеющие никаких разрешений.

Акселерометр – прибор, с помощью которого измеряется кажущееся ускорение. Он призван помочь программному обеспечению смартфона определить положение, а также расстояние перемещения мобильного устройства в пространстве.

Данная атака срабатывает в случае, когда жертва активирует режим громкоговорителя в телефоне или при видео-звонке, прослушивает медиафайлы или взаимодействует с виртуальным помощником на смартфоне.

Исследователи разработали вредоносное Android-приложение, которое записывает реверберации с помощью акселерометра и отправляет полученные данные на сервер атакующих. По словам исследователей, злоумышленник может проанализировать данные и с помощью технологий цифровой обработки сигналов и машинного обучения воссоздать произнесенные слова и извлечь нужную информацию о жертве.

Атака Spearphone может использоваться для определения содержимого проигранного жертвой аудио или голосовых заметок, полученных через мессенджеры, такие как WhatsApp, персональной информации (номеров социального страхования, дат рождения, возраста, данных платежных карт, банковских счетов и т.д.). Более подробно новый метод описан в работе исследователей.» ***(Представлен метод перехвата данных с динамиков смартфона // SecurityLab.ru (https://www.securitylab.ru/news/499988.php). 18.07.2019).***

***

«Вредонос «Topinambour» из семейства дропперов стал имплантом первой стадии атаки, распространяя шпионский троян.

Киберпреступная группировка Turla обновила свой арсенал набором инструментов для атак на правительственные структуры. В частности, злоумышленники используют дроппер под названием «Topinambour», используемый на первой стадии атак. После установки он загружает на систему другие вредоносные программы, используемые Turla для доступа к целевым сетям и извлечения данных.

По информации «Лаборатории Касперского», для распространения новых модулей преступники используют легитимные установщики ПО, зараженные дроппером «Topinambour». Это могут быть инструменты для обхода интернет-цензуры, такие как Softether VPN 4.12 и psiphon3, или активаторы Microsoft Office.

Последние используются пиратами для активации пакета Microsoft Office без необходимости покупать ключ.

Русскоговорящая хакерская группировка Turla (Snake, Venomous Bear, Waterbug и Uroboros) известна своими атаками на западные правительства, а также посольства и консульства в странах постсоветского пространства.

«Topinambour» содержит «крошечный .NET шелл», который ожидает команды от C&C-сервера и выполняет их. Сама C&C-инфраструктура размещена на скомпрометированных сайтах на WordPress и облачных сервисах. С помощью команд «net use» и «copy» операторы кампании распространяют вредоносные модули следующего этапа — инструмент KopiLuwak, а также новые трояны MiamiBeach и RocketMan!, написанные на языках PowerShell и .NET.

MiamiBeach и RocketMan! загружают, скачивают и исполняют файлы, а также собирают информацию о системе. Кроме того, PowerShell-версия также способна делать снимки экрана. Также они загружают конечный более сложный вредоносный модуль, который может выполнять команды, полученные с C&C-сервера.

По мнению исследователей, создание похожих по функционалу троянов на разных языках может быть связано с защитой от обнаружения. Если на компьютере будет обнаружена одна версия, то операторы могут прибегнуть к аналогу на другом языке. Причиной разработки аналогов KopiLuwak может быть минимизация рисков обнаружения известных JavaScript-версий троянов.» ***(Turla вооружилась новым вредоносным ПО // SecurityLab.ru (https://www.securitylab.ru/news/499968.php). 16.07.2019).***

***

«…Специалисты Check Point обнаружили новый вид вредоносного ПО для Android, успевшего заразить более 25 млн устройств. Вредонос, окрещенный «Agent Smith», незаметно для пользователя заражает устройство и заменяет официальные приложения клонами, показывающими большое количество рекламы. В основном жертвами кампании стали пользователи в Индии (15,2 млн), Бангладеш (2,5 млн) и Пакистане (1,7 млн).

Исследователям удалось отследить оператора вредоносного ПО, им оказалась некая китайская технологическая компания. Фирма специализируется на помощи китайским разработчикам в продвижении своих Android-приложений, однако, помимо этого, занимается и иной деятельностью. В частности, эксперты обнаружили на китайских сайтах по поиску работы вакансии, указывающие на связь компании с вредоносным ПО «Agent Smith».

Злоумышленники начали распространять вредоносное ПО в 2018 году через 9Apps — независимый магазин приложений от разработчика мобильного браузера UC Browser.

В последние месяцы приложения, зараженные вредоносным ПО «Agent Smith», начали появляться в магазине Google Play. Специалисты обнаружили 11 инфицированных приложений, что говорит о готовящейся кампании по распространению вредоноса через официальный магазин Google. После сообщения в службу безопасности Google зараженные приложения были удалены.

Инфицированные приложения содержали вредоносный компонент, замаскированный под SDK, который загружал и устанавливал другой пакет приложений с вредоносным ПО «Agent Smith». Оказавшись на зараженном телефоне, он сканировал установленные приложения и на основании встроенного списка целей заменял их клонами с рекламой. Список включает 16 приложений, в частности, WhatsApp, Lenovo AnyShare, Opera Mini, Flipkart и TrueCaller, а также программы, в основном популярные на индийском рынке, такие как Jio и Hotstar.

По словам исследователей, «подмена» приложений — сам по себе сложный процесс. Для внедрения вредоносного кода внутри легитимной программы эксплуатируется уязвимость Janus (CVE-2017-13156) в Android, позволяющая добавить контент в APK, не нарушая целостности цифровой подписи. В случае успеха «Agent Smith» инициирует обновление целевого приложения, а затем блокирует будущие обновления для предотвращения удаления вредоносного кода при следующем апдейте.» ***(Вредонос «Agent Smith» заразил 25 миллионов Android-устройств // SecurityLab.ru (https://www.securitylab.ru/news/499924.php). 11.07.2019).***

***

«Шкідливі програми під назвою «Агент Сміт» були завантажені на 25 мільйонів пристроїв Android, свідчить нове дослідження компанії з кібербезпеки Check Point…

Виявлена нещодавно програма, що отримала назву «Агент Сміт» (на ім'я головного антигероя трилогії «Матриця»), показувала користувачам небажані оголошення. За словами фахівців з Check Point, найчастіше шкідливе ПО потрапляло на пристрій через популярні додатки, більшість з яких були іграми. Всі вони були завантажені через сторонні магазини додатків китайської компанії.

Шкідлива програма змогла скопіювати популярні додатки на телефоні, включаючи WhatsApp і веб-браузер Opera, впровадити власний шкідливий код і замінити початковий додаток своєю версією, використовуючи уразливість в оновленні Google. «Захоплені» додатки не перестають працювати нормально, що приховує шкідливе ПЗ від користувачів.

Отримавши необхідні дозволи, які користувачі надали реальним додатками, «Агент Сміт» зміг захопити інші програми для відображення небажаних оголошень господареві гаджета. Це може здатися незначною проблемою, але ті ж недоліки в безпеці можуть бути використані для захоплення банківських, торгових та інших додатків, а також крадіжки даних…» ***(25 мільйонів пристроїв Android виявилися заражені шкідливим вірусом // UkrMedia інтернет-газета (https://ukr.media/science/396517/). 13.07.2019).***

***

«В ходе одной из текущих TrickBot-кампаний исследователи обнаружили вариант зловреда, загружающий новый компонент. Анализ показал, что этот модуль предназначен для сбора учетных данных электронной почты и контактов из ящиков жертвы, а также для рассылки вредоносного спама с ее адреса.

Windows-троян TrickBot появился на интернет-арене в 2016 году и с тех пор постоянно совершенствуется, расширяя свою функциональность за счет добавления новых модулей. Изначально он был нацелен только на кражу финансовых данных, к 2018 году список мишеней TrickBot пополнился криптобиржами, а более современные версии зловреда умеют воровать учетные данные пользователей служб удаленного доступа и куки-файлы, а также перехватывать трафик жертвы с целью фишинга.

Модификация TrickBot, обнаруженная экспертами Deep Instinct, по команде загружает с американского или румынского сервера модуль, которому было присвоено кодовое имя TrickBooster. Основной функцией этого компонента, по словам исследователей, является сбор учетных данных и email-адресов на машине жертвы; для этого TrickBooster запускает процесс OUTLOOK.exe и взаимодействует с ним, используя Microsoft Outlook Messaging API (MAPI).

Собранную информацию бот отправляет на свой сервер (выявлены два: один прописан в США, другой — в Румынии), а затем получает из центра управления (с московским IP-адресом) команду на рассылку спама. Примечательно, что отправленные от имени жертвы письма зловред удаляет из ее ящика, чтобы скрыть несанкционированные рассылки.

Исследователям удалось проникнуть на серверы, используемые TrickBooster. Как оказалось, операторы трояна собрали с помощью нового модуля базу из 250 млн email-адресов. Основную массу похищенного составили частные ящики на Gmail, Yahoo, Hotmail, MSN и AOL; в этом дампе также числились госструктуры США и Великобритании, британские и канадские ВУЗы, региональные органы исполнительной власти Канады. Сверка нескольких тысяч адресов со списками жертв известных утечек показала, что это новая массовая компрометация email.

Код всех найденных образцов TrickBooster был подписан действующим сертификатом — их оказалось несколько, и все выданы на имя разных мелких британских компаний, в том числе даже не связанных с разработкой ПО. Эксперты связались с УЦ Thawte (собственность DigiCert) и сообщили о злоупотреблении; скомпрометированные сертификаты уже отозваны…» ***(Maxim Zaitsev. TrickBot получил модуль для рассылки спама // Threatpost (https://threatpost.ru/trickbot-trojan-gets-a-spam-mailer-module/33487/). 16.07.2019).***

***

«Исследователи обнаружили вымогательскую кампанию, направленную на сетевые хранилища QNAP. Злоумышленники взламывают серверы со слабыми паролями и требуют выкуп в 0,05–0,06 BTC (36–43 тыс. рублей по курсу на день публикации).

По сообщениям экспертов, новый шифровальщик eCh0raix — это компактная программа на языке Go (код занимает не более 400 строк). В настоящий момент известно об атаках на NAS-устройства QNAP TS-251, QNAP TS-451, QNAP TS-459 Pro II и QNAP TS 253B. Злоумышленники подбирали пароли к ним через брутфорс.

Связь с управляющим сервером eCh0raix поддерживает с помощью прокси SOCKS5. Вымогатель отправляет на управляющий узел информацию о

пораженном хосте, скачивает требование о выкупе и публичный RSA-ключ, которым позже будет защищать ключи шифрования пользовательских данных.

Эксперты уточняют, что зловред не передает операторам системную информацию, чтобы в дальнейшем различать жертвы. По мнению исследователей, этой цели служит отдельный API, который позволяет обрабатывать запросы на получение специфических данных. В частности, с его помощью зловред получил порядковый номер — идентификатор кампании.

Эксперты отмечают, что операторы eCh0raix научили его прекращать активность при попадании на хосты в России, Белоруссии или на Украине. Географическую принадлежность зараженного устройства зловред определяет по раскладке клавиатуры.

Если пораженный NAS находится вне перечисленных стран, зловред завершает ряд процессов, связанных с взаимодействием с базами данных: apache2, nginx, mysqld, php-fpm и другие. Далее он определяет интересующие его файлы и шифрует их с помощью алгоритма AES.

Вымогателя интересуют документы Microsoft Office и OpenOffice, архивы, базы данных, PDF- и мультимедийные файлы. После преобразования они сохраняют название и получают расширение *.encrypt.

Создатели зловреда воспользовались тем, что на хранилищах QNAP нет нативных антивирусных систем. Эксперты также отмечают, что многие защитные средства пока не распознают новую угрозу — по данным VirusTotal, лишь 3 движка из 55 определяют eCh0raix как вредоносное ПО.

Исследователи утверждают, что создать декриптор к новому шифровальщику будет несложно: разработчики зловреда создают секретный ключ не на истинно случайной основе, а по определенному математическому алгоритму. Со своей стороны, компания QNAP подготовила рекомендации по защите от вымогателей.

В конце 2018 года пользователи NAS-устройств QNAP попали под атаку зловредного bash-сценария — скрипт проникал на хранилища, чтобы похитить администраторские пароли.» ***(Egor Nashilov. Шифровальщик eCh0raix прицельно атакует NAS-хранилища QNAP // Threatpost (https://threatpost.ru/ech0raix-ransomware-targets-nas-storages/33441/). 12.07.2019).***

***

«ИБ-эксперты предупредили об очередной кампании операторов шпионского трояна Astaroth, который скрывается от программ безопасности с помощью техники «подножного корма» (living-off-the-land), то есть использует инструменты атакуемой системы. По словам исследователей, защитить от зловреда могут только продвинутые антивирусные средства, заточенные под такой класс ПО.

Обнаружить нынешнюю атаку удалось по подозрительной активности легитимной утилиты для управления Windows (Windows Management Instrumentation Command, WMIC). Она позволяет вызывать соответствующие инструменты прямо из командной строки, при этом все выполняемые сценарии абсолютно легитимны. Эти факторы делают WMIC интересной целью для взломщиков.

Как выяснилось, первоначальное проникновение произошло через письмо с вредоносным URL. Ссылка вела на ZIP-архив, замаскированный под HTM-страницу. Внутри находился LNK-ярлык, в чьем наименовании использован тот же прием. Открытие этого файла запускает WMIC.

Консольная утилита начинает работу с включенным параметром /Format, что позволяет ей скачивать и запускать JavaScript-код. Именно это и происходит на следующем этапе, когда на компьютер последовательно загружаются несколько файлов с обфусцированным содержимым.

Эти компоненты, в свою очередь, обеспечивают запуск легитимных утилит, которые скачивают и приводят в рабочее состояние полезную нагрузку — DLL-библиотеки в открытом и зашифрованном виде. Одна из них встраивает Astaroth в процесс Userinit. Он обеспечивает авторизацию пользователя при запуске системы, что позволяет трояну закрепиться на машине.

Подобные бесфайловые зловреды, которые действуют непосредственно в памяти и используют легитимные сервисы Windows, стоят за многими крупными кибератаками. Например, к этой категории относится червь Stuxnet, который вывел из строя иранские АЭС и все еще циркулирует в Сети. Другой пример — зловред группировки Fin7, предназначенный для взлома банкоматов и платежных систем.

Особенность подобных программ в том, что их сложно пробить по антивирусным базам. Специалисты призывают администраторов обращать внимание на косвенные признаки вторжения, как это было с подозрительной активностью WMIC в нынешней атаке Astaroth.» ***(Egor Nashilov. Троян Astaroth работает на «подножном корме» // Threatpost (https://threatpost.ru/astaroth-gets-by-living-off-the-land/33395/). 09.07.2019).***

***

«Специалисты по кибербезопасности от антивирусной компании ESET сделали тревожное заявление. Им удалось зафиксировать распространение ряда мошеннических схем, рассчитанных на пользователей популярного приложения FaceApp.

Согласно опубликованным данным, как правило, злоумышленники распространяют в сети поддельные версии приложения, которые пользователи скачивают с фальшивых сайтов…

У жертв при попытке установить приложение появляется на экране большое количество всплывающих окон. Также они получают запросы на уведомление, которые являются очередной мошеннической схемой.

Более того, даже в магазине Google Play оказалось одно из таких приложений, которое ведет непосредственно на файлообменный сервис mediafire.com, с которого скачивается вредоносное программное обеспечение.

Фальшивый клон данного приложения также располагался на YouTube в виде ссылок на скачивание.

Чтобы избежать подобных ловушек, и не распрощаться со своими конфиденциальными данными, специалисты советуют скачивать приложение только из официальных магазинов - Google Play и App Store…» ***(Будь на чеку! Пользователей FaceApp атакуют мошенники // Ukrainianwall.com***

(https://ukrainianwall.com/society/9386-bud-na-cheku-polzovateley-faceapp-atakuyut-moshenniki). 22.07.2019).

***

«…Компании QNAP и Synology предупредили пользователей о текущих атаках с использованием вымогательского ПО eCh0raix на сетевые накопители.

Согласно предупреждению Synology, несколько пользователей уже пострадали от атак, в рамках которых злоумышленники похитили учетные данные администратора и с их помощью получили доступ к устройствам и зашифровали хранящуюся на них информацию. Согласно сообщениям пострадавших, за восстановление файлов атакующие требовали 0,06 биткойна (примерно $587).

«Мы считаем, что это организованная атака. После тщательного расследования мы выяснили, что атакующие использовали ботнет для сокрытия IP-адреса, с которого исходили атаки. Злоумышленники получили учетные данные администратора с помощью брутфорса, атака была осуществлена 19 июля», - отмечается в сообщении Synology…» ***(QNAP и Synology предупредили об атаках шифровальщика на NAS-устройства // SecurityLab.ru (https://www.securitylab.ru/news/500176.php). 27.07.2019).***

***

«…Злоумышленники распространяют по электронной почте программу-вымогатель Sodinokibi (также известный как REvil и Sodin), выдавая себя за сотрудников немецкого Федерального управления по информационной безопасности (Bundesamt für Sicherheit in der Informationstechnik). Используя в качестве темы сообщения «Предупреждение о скомпрометированных пользовательских данных» («Warnmeldung kompromittierter Benutzerdaten»), злоумышленники побуждают своих жертв открыть вложение с вредоносным PDF документом, говорится в сообщении BSI.

После открытия документа на системе запускается hta-файл с помощью легитимной утилиты mshta.exe, далее на систему загружается вымогательское ПО Sodinokibi.

Инфицировав систему, вредонос удаляет теневые копии файлов и отключает восстановление при загрузке Windows. Затем Sodinokibi шифрует файлы на системе и за их восстановление требует $2500 в биткойнах, по прошествии указанного срока сумма возрастает до $5000.

Ранее стало известно об атаках, в рамках которых операторы Sodinokibi взламывали провайдеров управляемых услуг через Webroot SecureAnywhere и заражали системы их клиентов вымогательским ПО. В июне компания Oracle исправила уязвимость десериализации в WebLogic Server, используемую ранее для распространения вымогательского ПО Sodinokibi и майнеров криптовалют.» ***(Злоумышленники распространяют вымогатель Sodinokibi от имени немецкой спецслужбы // SecurityLab.ru (https://www.securitylab.ru/news/500173.php). 26.07.2019).***

***

«…Национальная полиция Испании (Policía Nacional) задержала в ходе операций в Барселоне две киберпреступные группировки. В общей сложности в интернет-мошенничестве подозреваются 25 злоумышленников, 12 из которых оказались несовершеннолетними, сообщается в пресс-релизе полиции.

Преступники получали доступ к банковским счетам, используя такие методы мошенничества как фишинг и кардинг, чтобы потом заказывать и перепродавать электронную технику. Число пострадавших от их деятельности насчитывает 69 человек.

Первая группа киберпреступников орудовала в провинции Барселоны Матаро с помощью интернет-рассылок. Они отправляли письма от имени банков, в которых сообщали о проблемах со счетами. Для их решения злоумышленники предлагали перейти на поддельную web-страницу и ввести пароль доступа. По словам полиции, преступникам удалось похитить с банковских счетов жертв 48 тыс. евро. В группировку входили 10 человек, в том числе граждане Испании и Марокко.

Вторая группировка, состоявшая из 15 человек (12 несовершеннолетних), вела преступную деятельность в Маресме и Вальес-Орьенталь (провинция Барселона). Каждый член группировки выполнял отдельную задачу. Одни отвечали за нумерацию кредитных карт путем фишинга и кардинга для последующей перепродажи сообщникам. Другие покупали электронную технику с помощью украденных карт, а затем перепродавали ее. Третьи отправляли интернет-покупки в автоматизированные пункты приема курьерских компаний. Среди задержанных были уроженцы разных стран, однако полиция не уточнила национальности.

Злоумышленники использовали украденные удостоверения личности для создания профилей и идентификации получателей мошеннических покупок, системы защиты против отслеживания IP-адресов используемых ими терминалов, а также сеть Tor для сохранения анонимности.» ***(Испанская полиция задержала киберпреступников, промышлявших кардингом и фишингом // SecurityLab.ru (https://www.securitylab.ru/news/499990.php). 18.07.2019).***

***

«…Сотрудники правоохранительных органов Болгарии взяли под стражу подозреваемого в кибератаке на сервер Национального агентства по доходам (Националната агенция за приходите), которая привела к утечке персональных данных более половины жителей страны…

Подозреваемым является Кристиан Бойков (Кристиян Бойков), 20-летний компьютерный специалист из города София. Он обвиняется в незаконном копировании данных с серверов НАП.

Ранее на серверы НАП была совершена кибератака, в ходе которой преступник похитил 110 баз данных с паролями, именами, адресами и информацией о доходах миллионов болгар. Позже злоумышленник отправил в СМИ 57 папок с персональной информацией жителей, сообщив что это только половина украденных данных.

Главная дирекция «Борьба с организованной преступностью» (ГДБОП) и Информационная служба АД совместно проанализировали загруженные данные более чем 5 миллионов граждан Болгарии. Они обнаружили файл с данными, указывающими на конкретного пользователя, конфигурацию компьютера, дату, время и программное обеспечение для чтения файлов. Таким образом была установлена личность злоумышленника.

Бойкова задержали на рабочем месте в офисе одной из столичных компаний, занимающейся вопросами кибербезопасности. Молодой человек остается под стражей в течении 72 часов, ему грозит заключение сроком от 5 до 8 лет и штраф в размере 10 000 левов (примерно 360 000 рублей).» ***(Задержан подозреваемый в утечке данных миллионов жителей Болгарии // SecurityLab.ru (https://www.securitylab.ru/news/499984.php). 17.07.2019).***

***

«DerpTrolling, введший в моду «рождественские» DDoS-атаки на игровые сервисы, приговорен к 27 месяцам лишения свободы.

23-летний житель штата Юта был приговорен к 27 месяцам лишения свободы за осуществление DDoS-атак на такие сервисы, как Sony PlayStation Network, Valve Steam, Microsoft Xbox, EA, Riot Games, Nintendo, Quake Live, DOTA2 и League of Legends.

Остин Томпсон (Austin Thompson), известный в Сети как DerpTrolling, является первым, кто ввел в моду выведение из строя перед Рождеством игровых сервисов с помощью DDoS-атак. Томпсон начал свою деятельность в 2011 году, но пик его активности пришелся на период с декабря 2013 года по январь 2014-го, когда DDoS-атаки были чрезвычайно успешными, поскольку на то время у многих компаний не было мощных средств защиты от них.

Злоумышленник объявлял о своих атаках в Twitter (@DerpTrolling) и там же устраивал опросы, какой сервис ему атаковать следующим.

Увидев, какой резонанс у общественности вызвали атаки DerpTrolling, различные группировки последовали его примеру. В декабре 2014 года «рождественскую» атаку осуществили Lizard Squad, в 2015-м – Phantom Squad, в 2015-м – R.I.U. Star Patrol, а в 2017-м былую славу пытались вернуть отдельные киберпреступники, но уже без особого успеха.

Сложившаяся традиция «рождественских» DDoS-атак вынудила ФБР предпринять соответствующие шаги. В прошлом году ФБР и правоохранительные органы Нидерландов и Великобритании совместными усилиями отключили 15 доменов сервисов, специализировавшихся на заказных DDoS-атаках.

Томпсон был арестован летом 2018 года и в ноябре того же года признал свою вину. Суд приговорил его к 27 месяцев лишения свободы и обязал выплатить $95 тыс. компенсации компании Daybreak Games (раньше Sony Online

Entertainment).» ***(Пионер «рождественских» DDoS-атак отправится в тюрьму // SecurityLab.ru (https://www.securitylab.ru/news/499800.php). 04.07.2019).***

***

«Британським правоохоронним органам вдалося встановити підозрюваного у витоку документів з листування посла Великої Британії в США Кіма Даррока…

Британська служба розвідки MI-6 і співробітники британського центру з кібербезпеки встановили, що витік стався не в результаті злому комп'ютерів хакерами з іноземних держав…

Скандал з витоком документів… зачепив партію "Брекзит" Найджела Фаража. Так, стало відомо, що голова партії "Брекзит" депутат Річард Тайс перебуває у стосунках з Ізабель Оукшотт, журналісткою, яка минулого тижня опублікувала статтю з листуванням Даррока.

Тайс заперечує, що він має будь-яку причетність до витоку документів. Водночас деякі прихильники Даррока вважають, що скандал навколо нього сплановано, щоб замінити його на "бізнесмена, що виступає за Brexit", пише The Sunday Times.

Посол Великої Британії в США Кім Даррок оголосив про те, що йде у відставку після того, як британські ЗМІ опублікували документи, в яких він критикує президента США Дональда Трампа.» ***(У Британії встановили підозрюваного у витоку листів посла у США // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/140719-u-brytaniyi-vstanovyly-pidozryuvanogo-u-vytoku-lystiv-posla-u-ssha). 14.07.2019).***

***

«Гражданская гвардия Испании сообщила о задержании самого разыскиваемого киберпреступника в истории страны. Злоумышленник, которому приписывают кражу миллионов евро, использовал в атаках сайты-однодневки и вредоносные мобильные приложения.

По информации следствия, мошенник начал свою деятельность три года назад. Он создавал копии крупных интернет-магазинов, торгующих бытовой техникой и электроникой. Далее преступник загонял на эти площадки трафик через рекламу в поисковиках и социальных сетях. Через несколько дней сайты закрывались, а организатор кампании уходил с платежными данными посетителей. Правоохранители утверждают, что на счету мошенника несколько десятков таких ресурсов.

Со временем злоумышленник стал предлагать жертвам установить вредоносное приложение, которое также позволяло ему собирать информацию банковских карт. Пользователи в свою очередь полагали, что получают легитимный трекер заказов.

В результате мошенник ежемесячно получал до 300 тыс. евро. Похищенные средства он переводил на подконтрольные счета и обналичивал в банкоматах. К последним операциям он привлекал сообщников, двое из которых сейчас также

задержаны полицией. В ходе обысков правоохранители изъяли 50 мобильных телефонов и 100 SIM-карт.

В настоящий момент Гражданская гвардия собирает информацию о пострадавших, которые могут поделиться своими историями на сайте ведомства…» ***(Egor Nashilov. В Испании задержали похитителя платежных данных // Threatpost (https://threatpost.ru/the-greatest-spanish-cybercrook-under-arrest/33385/). 09.07.2019).***

***

Технічні аспекти кібербезпеки

«…Корпорация Google объявила о троекратном увеличении размера максимальных сумм, выплачиваемых в рамках программы вознаграждения за найденные уязвимости в браузере Chrome и его компонентах.

В частности, «максимальная базовая сумма вознаграждения» за уязвимость в Chrome увеличена с $5 тыс. до $15 тыс., максимально возможная сумма награды - $30 тыс. Также возросла сумма стандартного вознаграждения за эксплоиты для уязвимостей Chrome OS, ведущих к компрометации Chromebook или Chromebox (до $150 тыс.).

Помимо прочего, компания приняла решение удалить возможность для сайтов определять, когда пользователь посещает ресурс в приватном режиме. Изменение будет реализовано с выпуском Chrome 76 в конце июля 2019 года. Сайты больше не смогут проверять наличие FileSystem API (отсутствие этого API указывает на то, что пользователь зашел на сайт в режиме инкогнито).

Как пояснили в компании, разработчики изменят поведение FileSystem API таким образом, чтобы исключить возможность отслеживания пользователей в приватном режиме. Также инженеры работают над мерами по устранению других способов определить, в каком режиме пользователь посещает сайт.» ***(Google втрое увеличила вознаграждение за уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/500002.php). 19.07.2019).***

***

«…Специалисты из Университета имени Бен-Гуриона (Израиль) разработали метод, позволяющий извлечь данные из физически изолированных систем с помощью светодиодных индикаторов Caps Lock, Num Lock и Scroll Lock на клавиатуре.

Новый метод получил название CTRL-ALT-LED. Для успешной атаки злоумышленнику потребуется предварительно заразить изолированную систему вредоносным ПО, по сути, CTRL-ALT-LED является всего лишь способом извлечь данные. По словам исследователей, вредоносная программа с помощью кастомного протокола передачи данных может заставить светодиодные индикаторы на подключенной по USB клавиатуре мигать с большой скоростью. Находящийся вблизи злоумышленник может записать эти вспышки и затем расшифровать

информацию с помощью той же схемы модуляции, которая использовалась для шифрования данных.

Команда исследователей протестировала метод на различных устройствах, включая камеры смартфона и «умных» часов, камеры видеонаблюдения, оптические сенсоры и датчики освещенности. В некоторых случаях для осуществления атаки злоумышленнику потребуется находиться рядом с устройством, чтобы записать вспышки с помощью смартфона либо смарт-часов, однако для этих целей также могут использоваться системы видеонаблюдения, в поле зрения которых находится клавиатура.

В ходе экспериментов ученым удалось извлечь данные со скоростью 3 тыс. бит/с при использовании чувствительных световых датчиков и примерно 120 бит/с в тестах с применением обычной камеры смартфона. Скорость варьировалась в зависимости от чувствительности камеры и расстояния до клавиатуры, модель клавиатуры роли не играла.

Как отмечают эксперты, рядовым пользователям пока нечего опасаться, новый метод в основном представляет угрозу для систем с высоким уровнем защиты, например, для правительственных сетей, в которых хранится секретная информация, или корпоративных сетей, содержащих закрытые сведения об интеллектуальной собственности.» ***(Ученые придумали новый способ кражи данных с физически изолированных систем // SecurityLab.ru (https://www.securitylab.ru/news/499923.php). 11.07.2019).***

***

«…Команда исследователей, в которую вошли представители четырех университетов США, изучили технологию Secure Encrypted Virtualization (SEV) от компании AMD и обнаружили, что при определенных обстоятельствах злоумышленники могут обойти ее защиту.

Результаты исследования были представлены на этой неделе на конференции безопасности ACM Asia Conference on Computer and Communications Security в Окленде (Новая Зеландия). В докладе под названием «The SEVerESt Of Them All: Inference Attacks Against Secure Virtual Enclaves» ученые описали два метода атак. Представленные ими техники позволяют недобросовестным администраторам облачных серверов или злоумышленникам, взломавшим гипервизор, определять запущенные на гостевой виртуальной машине приложения, защищенные с помощью SEV, а также внедрять и извлекать данные из виртуальных машин.

Как поясняет AMD, SEV защищает гостевые виртуальные машины как друг от друга, так и от ПО, запущенного на хосте, и его администраторов. Неважно, что происходит на одной виртуальной машине, это не должно затрагивать ни другие виртуальные машины, ни операционную систему хоста, ни гипервизор, ни администраторов. Тем не менее, исследователи продемонстрировали, что технология SEV не способна отражать атаки со стороны вредоносного гипервизора.

«Пассивно наблюдая за изменениями в журналах, злоумышленник может восстановить критическую информацию о действиях в зашифрованных гостевых системах», – сообщается в докладе исследователей.

Атака работает даже в отношении Secure Encrypted Virtualization Encrypted State (SEV-ES) – расширенной техники защиты памяти, шифрующей не только оперативную память, но и блок управления виртуальной машины. Это блок представляет собой область памяти, куда сохраняется содержимое реестра ЦП виртуальной машины, когда она вынуждена уступать гипервизору. По идее, шифрование должно помешать гипервизору понять контекст приостановленной виртуальной машины, однако исследователи доказали обратное…» ***(Представлены атаки обхода технологии безопасности SEV // SecurityLab.ru (https://www.securitylab.ru/news/499919.php). 11.07.2019).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«…Компании Vertical Structure и WhiteHat Security, занимающиеся вопросами кибербезопасности, сообщили о серьезной уязвимости в тысячах сетевых накопителях данных Lenovo. Эксплуатация уязвимости позволяла злоумышленникам получить удаленный доступ к миллионам файлов.

Уязвимость затрагивает снятые с производства сетевые накопители Iomega/LenovoEMC. Поиск Shodan выявил 5114 устройств, хранящих более 3 миллионов файлов. Они содержали около 20 000 документов, 13 000 электронных таблиц, 13 000 текстовых файлов и 405 000 изображений. В некоторых файлах хранилась конфиденциальная информация, включая номера платежных карт и финансовые записи.

По словам директора Vertical Structure Саймона Уиттакера (Simon Whittaker), реальное количество уязвимых устройств больше, поскольку 5114 устройств — только те, которые были проиндексированы.

Уязвимость связана с отсутствием в API механизма авторизации и возможностью удаленно просматривать и извлекать файлы. Уиттакер сравнил уязвимость с миллионами незащищенных бакетов Amazon S3.

Уязвимость могла быть проэксплуатирована неаутентифицированным злоумышленником для получения доступа к файлам на сетевых накопителях путем отправки специально сформированного запроса через API. Злоумышленник мог просканировать сеть на наличие уязвимых накопителей и отправить вредоносный запрос на IP-адрес целевого устройства. По словам Уиттакера, преступник мог также создать скрипт, который автоматизировал бы атаку и извлекал данные со всех уязвимых устройств.

Компании сообщили о своих находках Lenovo, которая присвоила уязвимости идентификационный номер CVE-2019-6160 и устранила ее.» ***(Уязвимость предоставила доступ к тысячам устаревших хранилищ Lenovo // SecurityLab.ru (https://www.securitylab.ru/news/499989.php). 18.07.2019).***

***

«Експерти з кібербезпеки виявили, що медіафайли, які передають через Вотсап і Телеграм, не є повністю захищеними.

…про це йдеться у новому звіті від аналітичної установи Symantec, яка займається питаннями кібербезпеки. Навіть, якщо у месенджерах увімкнений режим, що зашифровує усі повідомлення, зловмисники мають можливість отримати доступ до медіафайлів, які за допомогою них передаються.

Шкідливі програми можуть отримати доступ до файлів — зображень, відео чи аудіо, — які Вотсап і Телеграм зберігають у пам'яті девайсів. Справа в тому, що Вотсап за замовчуванням зберігає файли через сховище гаджета, а Телеграм робить це, коли ввімкнено функцію «Зберегти в галерею».

Дослідники зазначають, що у такому випадку шкідливі програми можуть отримати доступ до файлів навіть раніше, ніж користувачі їх відкриють власноруч.

Юзери зазвичай користуються опцією завантаження файлів на пристрій, оскільки це полегшує подальшу роботу з ними. Утім такий крок значно зменшує захист даних.

Разом з тим, аналітики пишуть, що, на жаль, і шифрування у месенджерах не може захистити користувачів на сто відсотків. «Ми вже про це зазначали: жоден код не може бути позбавлений слабких місць», — пишуть дослідники…» ***(Дослідники виявили слабке місце у Вотсапі і Телеграмі // MediaSapiens (https://ms.detector.media/web/cybersecurity/doslidniki_viyavili_slabke_mistse_u_whatsapp_i_telegram/). 16.07.2019).***

***

«Фахівець в області кібербезпеки Лаксман Мутийя виявив в соціальній мережі Instagram уразливість, яка дозволяє отримати доступ до будь-якого акаунта всього за десять хвилин. Про це він детально розповів у власному блозі. Схоже, будь-який аккаунт під загрозою, і це ніяк не можна виправити.

Мова йде про недосконалість системи відновлення пароля, яка відправляє на смартфон або електронну пошту користувача повідомлення з цифровим кодом з метою отримати підтвердження, що пароль змінює саме він. Є дуже велика вірогідність, що компанія не виправить цю помилку найближчим часом.

На думку експерта, відправивши мільйон кодів, можна зрештою знайти вірну комбінацію. Єдиною перешкодою є обмеження соцмережі на кількість можливих запитів. Звичайно ж, це обмеження можна обійти, причому без використання яких-небудь пасток.

Мутийя зміг обійти обмеження, використовуючи тисячі IP-адрес для відправки кодів. Він також встановив, що для злому будь-якого Instagram-аккаунта знадобиться п'ять тисяч IP-адрес, з яких повинна здійснитися відправка мільйона запитів…» ***(Зламати будь-який Instagram-аккаунт за 10 хвилин: хакери виявили нову уразливість // znaj.ua (https://techno.znaj.ua/247262-zlamati-bud-yakiy-instagram-akkaunt-za-10-hvilin-hakeri-viyavili-novu-urazlivist). 17.07.2019).***

***

«Австралийским специалистам в области информационной безопасности удалось сбить с толку движок антивируса на базе ИИ, разработанный

BlackBerry Cylance, заставив его признать безопасным вредоносное ПО. Это открытие заставляет усомниться в надёжности популярной сегодня методологии, использующей для обеспечения кибербезопасности искусственный интеллект.

Алгоритм машинного обучения системы защиты конечных точек Cylance PROTECT сотрудникам фирмы Skylight Cyber удалось эффективно обойти без внесения каких-либо изменений в код вредоносной программы. К нему просто добавляли строки из благонадёжного ПО: распознавав их ИИ-алгоритм Cylance выносил положительный вердикт, игнорируя любой встречающийся далее вредоносный код.

«Насколько я знаю, это первая в мире подтверждённая глобальная атака на механизм машинного обучения антивирусной компании, — сказал один из авторов метода, Ади Ашкенази (Adi Ashkenazy). — После примерно четырех лет супер-ажиотажа [связанного с искусственным интеллектом] я считаю это отрезвляющим примером того, как данный подход создаёт новую поверхность атаки, невозможную ранее [с прежним антивирусным ПО]».

Кевин Боцек (Kevin Bocek), вице-президент по стратегиям безопасности фирмы Venafi, со своей стороны напомнил, что идея обмана продвинутых антивирусов не нова, в частности, именно благодаря такой способности оказались столь эффективными атаки Stuxnet.

По мнению Грегори Уэбба (Gregory Webb), главы антивирусной фирмы Bromium, новое исследование демонстрирует порочность практики полного перекладывания на машины функции принятия решений о том, что хорошо и что плохо.» ***(Исследователям удалось обмануть интеллектуальный алгоритм антивируса // Компьютерное Обозрение (https://ko.com.ua/issledovatelyam_udalos_obmanut_intellektualnyj_algoritm_antivirusa_129520). 22.07.2019).***

***

«Специалисты в области кибербезопасности из компании Symantec обнаружили новую уязвимость мессенджера WhatsApp. С ее помощью злоумышленники получают доступ к медиафайлам, отправленным через приложение.

В ОС Android приложения могут сохранять мультимедиа, например изображения и аудиофайлы, либо во внутреннем хранилище, доступном только через приложение, либо во внешнем хранилище, более широко доступном для других приложений.

WhatsApp по умолчанию сохраняет медиафайлы во внешнем хранилищи, а Telegram делает это, когда в приложении включена функция “Сохранить в галерею”.

Вредоносное ПО с доступом к внешнему хранилищу может быть использовано для доступа к мультимедийным файлам WhatsApp и Telegram, возможно, даже до того, как пользователь их увидит.

Если юзер загружает, например, вредоносное приложение, а затем получает фотографию в WhatsApp, хакер может манипулировать изображением, даже если

получатель этого не заметит. Таким образом, теоретически он может даже изменить исходящее мультимедийное сообщение.

Исследователи называют атаку Media File Jacking. По большей части, это известная проблема и компромисс между конфиденциальностью и доступностью для приложений-мессенджеров на ОС Android.

Представители WhatsApp заявляют, что изменение данной системы хранения скажется негативно на возможностях сервиса при обмене файлами, а возможно – породит новые проблемы с конфиденциальностью.» ***(В мессенджере WhatsApp найдена новая уязвимость // (https://www.kopirkin.com.ua/v-messendzhere-whatsapp-najdena-novaya-uyazvimost/). 16.07.2019).***

***

«Эксперты обнаружили серьезную уязвимость в компьютерах Apple Mac. С помощью сервиса видеозвонков Zoom злоумышленники могут получить доступ к веб-камере пользователей.

Несмотря на то, что компания Apple считается эталоном в сфере защиты персональных данных пользователей, иногда разработчики из Купертино допускают фатальные ошибки.

Одной из таких стала уязвимость в компьютерах Mac, которую недавно обнаружил специалист по кибербезопасности Джонатан Лейтсшух. Ошибка в системе не просто может предоставить злоумышленникам доступ к информации пользователя на компьютере, а позволяет управлять его веб-камерой.

По словам Лейтсшуха, уязвимость грозит около 4 млн клиентов Apple, которые пользуются сервисом для видеозвонков Zoom. Эта программа устанавливает веб-сервер на Mac, но запросы на этот сервер могут отправлять любые веб-сайты.

«Хакеры» могут просто создать приглашение на видеоконференцию Zoom, при переходе по которому у пользователей Mac автоматически включится камера. Примечательно, что удаление вредоносного для Apple сервиса видеосвязи может не решить проблему, — установленный веб-сервер может скачать программу заново.

В Zoom считают уязвимость «незначительным риском» и пообещали исправить проблему в следующем обновлении сервиса…» ***(В компьютерах Apple обнаружена серьезная уязвимость // AOinform (https://www.aoinform.com/news/v_kompjuterakh_apple_obnaruzhena_sereznaja_ujazvimost/2019-07-10-30807). 10.07.2019).***

***

Нові надходження до Національної бібліотеки України імені В.І. Вернадського

Береза В. В. Поняття та класифікація повноважень Департаменту кіберполіції Національної поліції України / В. В. Береза // Вісник Харківського національного університету внутрішніх справ. - 2018. - № 3. - С. 30-39.

Досліджено положення нормативноправових актів на предмет висвітлення повноважень Департаменту кіберполіції Національної поліції України. Наведено класифікацію повноважень Департаменту кіберполіції Національної поліції України з урахуванням основних напрямів діяльності досліджуваного органу державної влади. Сформульовано авторське визначення терміна «повноваження Департаменту кіберполіції Національної поліції України».

Шифр зберігання НБУВ: Ж69872

***

Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти : монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька. - Житомир, 2019. - 279 с.

Розглянуто теоретичні та практичні основи забезпечення інформаційної безпеки людини, суспільства, держави у кібернетичному та інформаційному просторах з використанням синергетичного підходу. Розкрито синергетичні ефекти, які виникають внаслідок ведення інформаційної та кіберборотьби. Представлено практичні рекомендації щодо застосування розроблених методологічних засад та наведено модельні приклади.

Шифр зберігання НБУВ: ВА832546

***

Корнієнко Б. Я. Безпека інформаційно-комунікаційних систем та мереж : навч. посіб. для студентів спец. 125 "Кібербезпека" / Б. Я. Корнієнко. - Київ, 2018. - 225 с.

Розглянуто питання захисту комп’ютерних систем, захисту операційних систем, побудови системи інформаційної безпеки, захищених віртуальних мереж та протоколи безпеки.

Шифр зберігання НБУВ: ВА834494

***

Матеріали IV Міжнародної науково-практичної конференції «Інноваційний розвиток науки нового тисячоліття» (26-27 жовтня 2018 року). - Хмельницький, 2018. - Ч. 1. - 119 с.

Зі змісту:

- Дубовик О.І. Проблематика корпоративних мереж та методи захисту проти атак.

Шифр зберігання НБУВ: В357719/1

***

Публічне управління та публічна служба в Україні: стан проблем та перспективи розвитку : матеріали наук.-практ. конф. за міжнар. участю, 07-08 верес. 2018 р. - Київ : Ліра-К, 2018. - 519 с.

Зі змісту:

- Сорока С. Аналіз національної системи кібербезпеки як складової інформаційної безпеки держави.

Шифр зберігання НБУВ: ВА832593

***

Скоробогатова Н. Є. Аналіз поширення кіберзагроз у глобальній економіці та мінімізації збитків від них / Скоробогатова Н. Є., Проценко К. Р. // Сучасні проблеми економіки і підприємництва.- 2018.- № 22.- С. 49-56.

Досліджено масштаби поширення кібератак та світовий досвід формування системи кібербезпеки. Проаналізовано основні етапи ідентифікації ризиків кіберзагроз. Здійснено кореляційний аналіз взаємозв'язку між основними показниками, що впливають на рівень кіберзагроз: кількість користувачів інтернету, глобальний інноваційний індекс, індекс розвитку людського потенціалу, кількість захищених інтернет-серверів, ВВП загалом та на душу населення, експорт ІКТ, індекс розвитку ІКТ, індекс людського розвитку.

Шифр зберігання НБУВ: Ж74463

***

Шведун В. О. Державна система забезпечення кібербезпеки: Особливості формування та впровадження / В. О. Шведун, О. В. Надьон // Вісник Національного університету цивільного захисту України. Серія : Державне управління. - 2019. - Вип. 1. - С. 308-313.

Визначено функції державного забезпечення кібербезпеки. Виокремлено напрями функціонування державної системи моніторингу кіберпростору. Виділено складові комплексної державної системи захисту інформації.

Шифр зберігання НБУВ: Ж74479

***

Information control systems and technologies : Materials of the VII International scientific-practical conference, 17th - 18th September, 2018. - Odessa, 2018. - 355 p.

Зі змісту:

- Михайлоа С.А., Шевцов Ю.С. Методологические основы организации кибербезопасности судових информационных систем;
- Журиленко Б.Е. Влияние величины финансовых затрат на вероятностную надежность технической защиты информации.

Шифр зберігання НБУВ: ІВ226246

***