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

№ 8 (серпень)

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. – №8 (серпень) . – 81с.

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

«Тільки протягом першого кварталу поточного року в державному та приватному секторі зафіксовано понад півтора мільйона кіберінцидентів… Про це УНН повідомили у відповідь на запит у пресслужбі Держспецзв'язку.

"Так, зокрема Центром реагування на кіберзагрози Держспецзв'язку, який забезпечує раннє виявлення аномальних активностей та потенційно небезпечних подій у системах і мережах, підключених до інтернету, та являє собою механізм координації зусиль усіх учасників кіберзахисту державного й приватного секторів, у 1 кварталі 2019 року зафіксовано 1 582 054 кіберінциденти", - повідомили у відповіді.

У пресслужбі також зазначили, що протягом 1 півріччя 2019 року у порівнянні з 2018 роком, зокрема в українському комерційному сегменті, кількість кіберінцидентів значно збільшилася.

Водночас, звернень щодо кіберінцидентів від власників енергетичних систем України та фінансових установ не надходило. А після завершення виборів до парламенту спостерігається тенденція до зниження кількості кіберінцидентів…» ***(Марія Мамаєва. За перший квартал 2019 року в Україні зафіксовано понад 1,5 млн кіберінцидентів // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/exclusive/1818458-za-pershiy-kvartal-2019-roku-v-ukrayini-zafiksovano-ponad-1-5-mln-kiberintsidentiv). 12.08.2019).***

***

«В одном из государственных реестров, держателем которых является Министерство юстиции Украины, обнаружена уязвимость, позволяющая получить несанкционированный доступ к хранящейся в нем информации.

Об этом на своей странице в Facebook сообщил спикер Украинского киберальянса, известный в сети под ником Шон Таунсенд…

Сведения об уязвимости были опубликованы в рамках флешоба #fuckresponsibledisclosure (#frd).#FRD – флешмоб, основанный Украинский кибеаральянсом ещё в 2017-м году, направленный на выявление и публичное раскрытие уязвимостей государственных (и не только) информационных ресурсов. За время существования волонтеры акции раскрыли данные и помогли закрыть уязвимости на сотнях информационных ресурсов органов государственной власти, местного самоуправления и объектах критической инфраструктуры. Благодаря активности участников #frd были не только открыты уголовные дела (как в случае с «Энергоатомом»), но и сохранены чувствительные данные, способные повлиять на жизнь и здоровье миллионов украинцев.

Согласно сообщению спикера УКА, на одном из реестров Минюста (каком именно – не указано), была обнаружена уязвимость, позволяющая с помощью SQL-инъекция получить доступ к данным реестра…» ***(Владимир Кондрашов. В одном из государственных реестров Минюста обнаружили «дыру» // Internetua (http://internetua.com/v-odnom-iz-gosudarstvennyh-reestrov-minuasta-obnarujili-dyru). 05.08.2019).***

***

«Prozorro співпрацюватиме з етичними хакерами. Стартує bug bounty проект "Hack Prozorro". Ціль – тестування рівня захищеності системи. Відбір хакерів триватиме до 8 вересня.

"Білий хакінг сьогодні – один із світових трендів кібербезпеки. Все через свою ефективність. Google, Facebook, Amazon навіть запустили власні програми співпраці з етичними хакерами. В Україні такий досвід мають лише приватні компанії. Ми є першою держустановою, яка самостійно ініціювала bug bounty", – розповів генеральний директор ДП "ПРОЗОРРО" Василь Задворний.

Hack Prozorro пройде у форматі bug bounty марафону – учасники шукатимуть недоліки в захисті системи. За кожну знайдену валідну та унікальну вразливість отримуватимуть винагороду. Її розмір залежатиме від рівня критичності.

Учасники працюватимуть у тестовому середовищі, що жодним чином не зачепить продуктивну систему Prozorro. Закупівлі відбуватимуться в звичайному режимі.

Реєстрація хакерів триває до 8 вересня. Серед надісланих заявок представники Prozorro, bug bounty платформи HackenProof, компанії OptiData та хмарного провайдера DeNovo відберуть 15 етичних хакерів. За умовами проекту учасниками можуть бути лише українці з відповідним досвідом у кібербезпеці та баг-хантингу.

Безпосередньо марафон з пошуку вразливостей пройде 21 вересня. Призовий фонд завдяки підтримці партнерів складає $7 000. Він буде розподілений між кращими хакерами…» ***("Білі" хакери шукатимуть баги в Prozorro // Український телекомунікаційний портал (https://portaltele.com.ua/news/companies/bili-hakeri-shukatimut-bagi-v-prozorro.html). 16.08.2019).***

***

«Тільки протягом першого кварталу поточного року в державному та приватному секторі зафіксовано понад півтора мільйона кіберінцидентів. Про це УНН повідомили у відповідь на запит у пресслужбі Держспецзв'язку.

"Так, зокрема Центром реагування на кіберзагрози Держспецзв'язку, який забезпечує раннє виявлення аномальних активностей та потенційно небезпечних подій у системах і мережах, підключених до інтернету, та являє собою механізм координації зусиль усіх учасників кіберзахисту державного й приватного секторів, у 1 кварталі 2019 року зафіксовано 1 582 054 кіберінциденти", - повідомили у відповіді.

У пресслужбі також зазначили, що протягом 1 півріччя 2019 року у порівнянні з 2018 роком, зокрема в українському комерційному сегменті, кількість кіберінцидентів значно збільшилася.

Водночас, звернень щодо кіберінцидентів від власників енергетичних систем України та фінансових установ не надходило. А після завершення виборів до парламенту спостерігається тенденція до зниження кількості кіберінцидентів…» ***(Марія Мамаєва. За перший квартал 2019 року в Україні зафіксовано понад 1,5 млн кіберінцидентів // Інформаційне агентство «Українські Національні***

Новини» (https://www.unn.com.ua/uk/exclusive/1818458-za-pershiy-kvartal-2019-roku-v-ukrayini-zafiksovano-ponad-1-5-mln-kiberintsidentiv). 12.08.2019).

***

«В Украине начала работу оценочная миссия Евросоюза относительно готовности телекоммуникационной сферы Украины к интеграции с единым цифровым рынком ЕС…

"В Офисе Президента Украины прошла встреча советника Главы государства Михаила Федорова с оценочной миссией Европейского Союза при участии представителей DG Connect Европейской комиссии. Целью миссии является оценка готовности телекоммуникационной сферы Украины к интеграции с единым цифровым рынком ЕС (EU Digital Single Market – DSM)", - указали в Офисе.

Михаил Федоров указал, что "мы хотим и готовы быстро выполнить все условия, чтобы стать частью инициативы ЕС по созданию единого цифрового рынка. Для Украины это - сверхмощные цифровые и экономические перспективы".

Стратегия DSM сейчас успешно реализуется в Европе. Особое внимание было уделено вопросам защиты данных, конфиденциальности и кибербезопасности, включая вопросы управления Интернетом, добавили в ОПУ.

"Законопроект "Об электронных коммуникациях", внесен в перечень приоритетных для первоочередного рассмотрения и принятия. Депутаты из будущего комитета цифровых трансформаций Верховной Рады уже активно работают над ним", - добавил советник Президента.

Представители миссии ЕС акцентировали внимание на необходимости обеспечения независимости и эффективности регулятора в сфере телекоммуникаций, отметили в ОПУ.» ***(Цифровой рынок: В Украине начала работу оценочная миссия ЕС // “Багнет” (http://www.bagnet.org/news/politics/404612/v-ukraine-nachala-rabotu-otsenochnaya-missiya-es-po-tsifrovomu-rynku). 18.08.2019).***

***

«Международная аудиторская компания BDO объявила о начале работы в Украине направления кибербезопасности, которое будет предоставлять услуги диагностики и защиты важной информации и инфраструктуры в киберпространстве. Это направление определено как одно из стратегических в 2019-2020 гг., поэтому запланировано быстрое организационное и технологическое развитие его команды.

"BDO в Украине будет предоставлять услуги по кибербезопасности" Руководителем направления назначен Андрей Слободяник, специалист по кибербезопасности и успешный топ-менеджер крупных ИТ-компаний (MTI Group, ISSP). «Наш консалтинговый сервис направлен на обеспечение готовности компаний клиентов к любым современным вызовам киберпространства. Мы предлагаем целый ряд возможностей для разработки, создания и внедрения киберзащиты», – заявил Андрей Слободяник.

Отмечается, что «BDO Кибербезопасность» внедряет инновационные методы, которые обычно используются только в чувствительных отраслях, таких

как оборонные и военные организации, где существует нулевая толерантность к потере сугубо конфиденциальных данных или иному воздействию.

Стоит напомнить, что BDO является пятой по величине мировой сетью аудиторских и консалтинговых компаний с более чем 80 тыс. сотрудниками в 162 странах. BDO в Украине входит в глобальную сеть BDO с 1997 г. и предоставляет украинским клиентам услуги по аудиту, консалтингу, налоговые и юридические услуги, консультации по управлению и ИТ, финансовые консультации, услуги по устойчивому развитию. С мая 2016 г. BDO в Украине имеет исключительное право распространять лицензии на использование ПО SAP, а также оказывать полный спектр услуг по внедрению и обучению продуктам SAP с фокусом на SAP Business One.» ***(Вновь открытое направление по кибербезопасности BDO в Украине возглавил Андрей Слободяник // «Компьютерное Обозрение» (https://ko.com.ua/bdo_v_ukraine_budet_predostavlyat_uslugi_po_kiberbezopasnosti_129839). 16.08.2019).***

***

Національна система кібербезпеки

«В Апараті Ради національної безпеки і оборони України відбулося засідання робочої групи з питань реформування сфери забезпечення кібербезпеки у системі національної безпеки. Засідання відбулось під головуванням заступника Секретаря РНБО Олексія Данілова…

“В умовах стрімкого розвитку ІТ-технологій у світі питання кібербезпеки та кіберзахисту стосується не тільки державного сектору, а й кожного громадянина, який має смартфон або користується комп’ютером чи планшетом. Також ринок послуг та сервісів у сфері кібербезпеки має бути відкритим для приватного сектору в рамках державно-приватного партнерства”, — зазначив радник Секретаря РНБО з питань кібербезпеки Андрій Зюзь.

До складу робочої групи увійшли представники парламенту, органів державної влади, ІТ-індустрії, експерти, науковці, представники громадянського суспільства. Зокрема, у засіданні взяли участь радник Президента України Михайло Федоров, голова Комітету Верховної Ради України з питань інформатизації та зв’язку Олександр Данченко, представники громадської організації Ukrainian Cyber Alliance.

Учасники засідання обговорили стан справ у сфері кібербезпеки, актуальні загрози та шляхи їх нейтралізації. Особливий акцент був зроблений на необхідності напрацювання комплексного пакету змін до законодавства у зазначеній сфері, імплементації кращих практик США та країн ЄС, необхідності активізації державно-приватного партнерства тощо…» ***(Саша Картер. В РНБО зібрали робочу групу з питань реформ у сфері кібербезпеки України // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1817594-v-rnbo-zibrali-robochu-grupu-z-pitan-reform-u-sferi-kiberbezpeki-ukrayini). 07.08.2019).***

***

«Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ очолив Микола Кулешов.

Про це йдеться в указі президента Володимира Зеленського.

Раніше цей департамент очолював Олександр Климчук, якого президент Володимир Зеленський звільнив 26 червня.

Кулешов працює в СБУ з 1995 року. З 2014-го – перший заступник начальника департаменту.

Відповідав за заходи в рамках Трастового Фонду Україна-НАТО з питань кібербезпеки.

Ініціював створення Ситуаційного центру забезпечення кібербезпеки СБУ і з 2016 року організовує його функціонування…» ***(Зеленський призначив очільника департамента кібербезпеки СБУ // Економічна правда (https://www.epravda.com.ua/news/2019/08/10/650470/). 10.08.2019).***

***

«На заседании рабочей группы по вопросам реформирования сферы обеспечения кибербезопасности в системе национальной безопасности Украины, которое состоялось в СНБО, участники обсудили предложения в сфере киберзащиты, вопросы развития цифровой инфраструктуры государства и совершенствование госуправления в этих сферах…

"15 августа в Аппарате СНБО Украины под председательством заместителя секретаря СНБО Украины Алексея Данилова состоялось очередное заседание рабочей группы по вопросам реформирования сферы обеспечения кибербезопасности в системе национальной безопасности Украины... Участники рабочей группы обсудили предложения относительно мер в системе кибербезопасности, развития цифровой инфраструктуры государства и совершенствования государственного управления в этих сферах, предложенные участниками заседания", - говорится в сообщении.

Как отмечается, по итогам совещания было принято решение по созданию целевых групп для дальнейшей работы относительно правовых аспектов обеспечения кибербезопасности и совершенствования государственного управления; цифровизации и развития отрасли электронных коммуникаций; определения перспективной организационно-технической модели киберзащиты и совершенствования образования в сфере кибербезопасности.

В совещании приняли участие специалисты по вопросам кибербезопасности, представители органов государственной власти, парламента, IT-отрасли, эксперты, ученые, представители гражданского общества.» ***(В СНБО обсудили реформирование в сфере госбезопасности // Телеграф (https://telegraf.com.ua/ukraina/obshhestvo/5125792-v-snbo-obsudili-reformirovanie-v-sfere-gosbezopasnosti.html). 16.08.2019).***

***

«Прес-служба СБУ на своїй сторінці у Facebook повідомила, що українські правоохоронці зупинили кібератаки на ефірний сервер телерадіокомпанії "Чорноморка"…

Таким чином, СБУ встановила, що зловмисники через шкідливе програмне забезпечення отримали контроль над серверним обладнанням телерадіокомпанії та вивели систему з ладу.

Слід зазначити, що силовики локалізували кібератаку та блокували її негативний вплив.

Наразі роботу ТРК повністю відновили.» ***(СБУ блокувала кібератаку на український телеканал // 5 канал (https://www.5.ua/suspilstvo/sbu-blokuvala-kiberataku-na-ukrainskyi-telekanal-197372.html). 13.08.2019).***

***

«Правоохранители продолжают следствие по делу организованной преступной группы, которая торговала служебной информацией из закрытых информационно-поисковых систем Национальной полиции Украины «Армор» и «ЦУНАМИ». В группу входили сотрудники одного из территориальных управлений Нацполиции…

Согласно материалам дела, что некое лицо по предварительному сговору с сотрудниками территориальных подразделений Главного управления Национальной полиции в Днепропетровской области, используя мессенджер «Telegram», предоставлял сторонним лицам служебную информацию о персональных данных физических лиц, содержащейся в информационно-поисковых системах Национальной полиции Украины «Армор» и «ЦУНАМИ».

Информация из вышеупомянутых систем предоставлялась при условии полной или частичной предоплаты на карту «ПриватБанка», принадлежащую организатору незаконной торговли данными и на электронный кошелек мобильного приложения «EasyPay». По результатам оперативно-розыскных мероприятий, проведенных сотрудниками Приднепровского управления киберполиции Департамента киберполиции Национальной полиции Украины, установлено, что денежные средства из электронного кошелька «EasyPay» перечисляются на банковскую карточку «УниверсалБанк», принадлежащую организатору (по версии следствия) схемы и на банковскую карточку «ПриватБанк», принадлежащую следователю СО Саксаганского ОП Криворожского ОП ГУНП в Днепропетровской области.

На данный момент полиция провела обыск по месту жителя своего коллеги из Саксаганского отдела полиции и у предполагаемого организатора преступной группы, а также получила от суда разрешения на доступ к информации о банковском счете в ПриватБанке и к мобильным телефонам двух фигурантов дела.

На данный момент предполагаемому организатору группы и следователю Саксаганскогo ОП объявлено о подозрении в совершении преступлений, предусмотренных частями третьими статей 362 («Несанкционированные действия с информацией») и 368 («Принятие предложения, обещания или получение неправомерной выгоды должностным лицом») Уголовного кодекса Украины. Фигурантам дела грозит до 10 лет лишения свободы.» ***(Владимир Кондрашов. Полицейские продавали в Интернете служебную информацию // Internetua (http://internetua.com/policeiskie-prodavali-v-internete-slujebnuua-informaciua). 06.08.2019).***

***

«К штрафу в 17 тысяч гривен приговорили ранее неоднократно судимую украинку, которая через мессенджер Telegram продавала «базу жителей Украины». Базу, содержащую ФИО, адреса, паспортные данные, ИНН и другую информацию, женщина оценила в 12 тысяч гривен…

Согласно приговору, 21 февраля уроженка Днепропетровска на Интернет-форуме «https://zblock.co/» разместила объявление о продаже информации с ограниченным доступом. В объявлении под названием «Продам базу жителей Украины» рекламировалась продажа в электронном виде некой базы данных, содержащей ФИО, дату рождения, паспортные данные, контактный номер телефона, идентификационный номер налогоплательщика и адреса регистрации жителей Украины.

Следствие установило, что 28 марта этого года на Telegram-аккаунт «Baza545», используемый злоумышленницей, написал заинтересованный клиент. Ему уроженка Днепропетровска сообщила, что база будет стоить 12 тысяч гривен, которые необходимо перечислить на её карточку «Ощадбанка». В этот же день женщина прислала потенциальному покупателю в качестве образца три скриншота с конфиденциальной информацией – персональными данными жителей Украины.

В этот же вечер женщина через Telegram переслала покупателю файл с расширением XLSX, где были ФИО, дата рождения, паспортные данные, контактный номер телефона, идентификационный номер налогоплательщика и адреса регистрации жителей Украины. Правда, денег за это злоумышленница не получила «по причинам, не зависящим от её воли». В приговоре не объясняются причины неполучения денег – судя по всему, покупателем базы в деле выступали правоохранители.

В судебном заседании обвиняемая полностью признала свою вину.

…действия обвиняемой следует правильно квалифицировать по ч.1 ст.361-2 УК Украины как несанкционированный сбыт информации с ограниченным доступом, которая хранится в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации, – говорится в приговоре.

В результате, суд приговорил женщину к уплате штрафа в размере 17 тысяч гривен.» ***(Владимир Кондрашов. Украинку осудили за продажу базы с данными жителей страны // Internetua (http://internetua.com/ukrainku-osudili-za-prodaju-bazy-s-dannymi-jitelei-strany). 05.08.2019).***

***

«…Співробітники СБУ перевірили обладнання дата-центру ДП «ІСС» ДСА та виявили шкідливе програмне забезпечення MinerGate. Програма була встановлено на FTP-сервері та починаючи з 1 січня минулого року, використовуючи потужності й електроенергію ДСА України, здійснювала видобуток криптовалюти.

Деякі нюанси цієї справи викладені в ухвалі Печерського районного суду міста Києва від 18 липня 2019.

Суд призначив комплексну судову інженерно-технічну експертизу у кримінальному провадженні, проведення якої доручив експертам Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України.

Органи досудового розслідування встановили, що «Єдина судова інформаційно-телекомунікаційна система» не відповідає вимогам Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», постанови КМУ від 12.04.2002 № 522 «Про затвердження порядку підключення до глобальних мереж передачі даних», НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу», затверджених наказом ДСТСЗІ СБ України від 02.04.2003 № 33, та має численні вразливості для несанкціонованого доступу.

Оскільки нормативно затверджені вимоги безпеки функціонування інформаційно-телекомунікаційних систем та ЄСІТС не були дотримані, це призвело до блокування, знищення та виведення з ладу у період з 24.12.2018 по 25.01.2019 судової системи України.

Зокрема, на веб-сайтах судів та веб-порталі «Судова влада України» зникли всі новини за період з 6-го по 27 грудня 2018 року, не функціонував сервіс електронної пошти в ДСА України, судах та інших органах і установах у системі правосуддя, був відсутній доступ до ряду електронних послуг.

Коли ДКІБ СБ України провело перевірку комп'ютерного та серверного обладнання ДП «ІСС» ДСА України, то виявилося наступне:

- шкідливе програмне забезпечення MinerGate, яке було інстальовано на FTP-сервері та починаючи з 01.01.2018, використовуючи потужності і електроенергію ДСА України, здійснювало видобуток електронних грошей (криптовалюти);

мало місце незаконне використання серверного обладнання ДСА України для роботи ряду приватних ресурсів;

- виявлений інсталяційний файл шкідливого програмного забезпечення з функцією спеціального технічного засобу негласного отримання інформації. Зазначене ШПЗ/СТЗ було встановлено на ряді ноутбуків ДП «ІСС», яке використовувались для налаштування серверів, ПЕОМ ДСА України та судів м. Києва та тривалий час здійснювало скриті аудіозаписи розмов оточення.

Згідно з листом ДСА України №10-4562/19 від 26.02.2019, у результаті блокування роботи судової системи України були понесені фінансові збитки при відновленні наслідків непрацездатності інформаційних систем.

Ще 22 травня 2019 року суд затвердив угоду про визнання винуватості з керівницею компанії, якій ДП «Інформаційні судові системи» виплатило 4,5 млн грн за невиконані роботи. Також підозри у цій справі було повідомлено двом екс-директорам ДП «Інформаційні судові системи» Віталію Живаєву і Леоніду Богданову…» ***(Сергей Студенников. Інформаційна судова система була заблокована внаслідок шкідливого програмного забезпечення // Судово-юридична газета (https://sud.ua/ru/news/publication/147123-informatsiyna-sudova-sistema-bula-zablokovana-vnaslidok-shkidlivogo-programnogo-zabezpechennya). 01.08.2019).***

***

«Служба безопасности Украины обнаружила в режимных помещениях Южно-Украинской атомной электростанции компьютерную технику, которая использовалась для майнинга криптовалют. По данным следствия, из-за несанкционированного размещения компьютерной техники произошло разглашение сведений о физической защите атомной электростанции, что является государственной тайной. К майнингу криптовалют, возможно, были причастны служащие части Национальной гвардии Украины, охраняющие АЭС…

Как нам стало известно, сотрудники следственного отдела Службы безопасности Украины в Николаевской области расследуют уголовное производство по сведениям о том, что должностные лица Южно-Украинской атомной электростанции в режимном помещении станции несанкционировано разместили компьютерное оборудование с подключением к сети Интернет, в результате чего произошло разглашение сведений о физической защите станции, которые являются государственной тайной.

10 июля в результате санкционированного обыска в кабинете №104 административного здания центрального пульта управления обособленного подразделения «Южноукраинская атомная электростанция» ГП «НАЭК «Энергоатом» было обнаружена и изъята компьютерная техника и комплектующие. Компьютерная техника была не санкционированно размещена на территории атомной электростанции, образовывала единую отдельную локальную сеть с выходом в общую сеть Интернет и использовались для получения криптовалют.

В кабинете №104 СБУ изъяла шесть видеокарт Radeon RX 470, два райзера (удлинители, которые используется для подключения дополнительных видеокарт к материнской плате, – Ред.), четыре блока питания, три системных блока (один из них – самодельный), свитч с блоком питания, свитч без блока питания, металлическую планку с тремя видеокартами, семью рейзерами и пятью кабелями к рейзерам, материнскую плату, флешку и жесткий диск. Также был изъят металлический каркас, на котором смонтированы материнская плата, три кулера, пять видеокарт, жесткий диск и два блока питания.

В этот же день обыски были проведены в помещениях, используемых воинской частью 3044 (Национальная гвардия Украины – Ред.), расположенной на территории Южноукраинской АЭС. В результате обыска было обнаружено и изъято 16 видеокарт, системный блок с инвентарным номером воинской части, семь жестких дисков, два твердотельных накопителя, флешку и роутер.

Кроме того, сотрудники СБУ в других помещениях ЮУ АЭС обнаружили и изъяли медиа-конвертер «СТС union», оптоволоконный и сетевые кабели, которых, по идее, в этих помещениях быть не должно…» ***(Владимир Кондрашов. На Южно-Украинской АЭС майнили криптовалюту // Internetua (http://internetua.com/na-uajno-ukrainskoi-aes-mainili-kriptovaluatu). 21.08.2019).***

***

Світові тенденції в галузі кібербезпеки

«Некоммерческая организация HITRUST, занимающаяся разработкой стандартов безопасности данных и сертификацией, запустила новую инициативу, призванную стимулировать ИБ-специалистов к улучшению средств контроля кибербезопасности в своих компаниях. HITRUST также представила результаты исследования, подтверждающие, что оценка зрелости и проработанности средств управления безопасностью позволяет определить их дальнейшую эффективность.

Как показывают результаты десятилетнего исследования, у организаций, чьи средства управления безопасностью согласно HITRUST CSF получили оценку в 79 балла и выше, вероятность того, что они будут продолжать работать аналогичным образом в будущем, составляет 99%. Чем выше оценка HITRUST CSF, тем меньше ошибок в управлении и ниже риск для пользователей.

В рамках новой инициативы HITRUST обновила свою программу CSF Assurance, добавив в нее рекомендации по оценке зрелости средств управления безопасности.

HITRUST предложила больше гибкости для организаций с высокой оценкой зрелости средств управления, увеличив период между проведением оценивания и предоставив им стимулы для реализации эффективной программы непрерывного мониторинга. С другой стороны, организации с оценкой зрелости ниже 79 баллов будут проходить процедуру оценивания CSF Assurance раз в год…» ***(HITRUST ввела оценку зрелости средств управления безопасностью // SecurityLab.ru (https://www.securitylab.ru/news/500399.php). 13.08.2019).***

***

«…Отсутствие автоматизированного механизма сбора данных, контекстного понимания инцидентов безопасности и визуального контроля над скрытыми в сети потенциальными угрозами существенно повышает риск организации стать жертвой кибератаки и снижает ее уверенность в собственной защищенности.

В ходе исследования специалисты Fidelis Cybersecurity опросили 300 специалистов IT-отделов (в том числе технических директоров, директоров по безопасности, директоров по информационным технологиям, инженеров и аналитиков) в организациях финансового и правительственного секторов, сектора здравоохранения и социальных служб.

По словам 57,43% опрошенных, в их организациях все более ощутимым становится отсутствие автоматизации, и решение данной проблемы является приоритетным. На отсутствие возможности осуществлять визуальный контроль жалуются 53,39% респондентов.

Как показывает исследование, большинство организаций постоянно добавляют в свои сети новые решения и подключенные устройства. Трафик увеличивается, а понимание максимальных возможности продуктов по интеграции отсутствуют. Как правило, новые устройства добавляются стихийно, а времени на обучение сотрудников и полного изучения функционала не хватает. В результате в безопасности предприятия появляются серьезные пробелы, а устройства «недоиспользуются».» ***(Отсутствие автоматизации остается главной проблемой для безопасников // SecurityLab.ru (https://www.securitylab.ru/news/500340.php). 08.08.2019).***

***

«…У соціальній мережі Інстаграм запустили програму для заохочення досліджень в області безпеки під назвою Data Abuse Bounty…

Відтепер у компанії почнуть давати винагороду за інформацію про сторонні додатки, які неправильно зберігають і використовують призначені для користувача дані. Наприклад, які зберігають імена користувачів та їх паролі.

Під перевірку потраплять також сервіси по накрутці підписників, коментарів і лайків.

Компанія «Фейсбук», у власності якої є соцмережа Інстаграм, поки що не називає розмір винагороди. Та при цьому там уточнюють, що середня виплата за участь у аналогічній програмі Facebook Bug Bounty становить $1500…» ***(Інстаграм почне платити за допомогу у захисті даних користувачів // MediaSapiens (https://ms.detector.media/web/cybersecurity/instagram_pochne_platiti_za_dopomogu_u_zakhisti_danikh_koristuvachiv/). 20.08.2019).***

***

«На конференции по кибербезопасности USENIX, прошедшей на прошлой неделе в городе Санта-Клара (Калифорния, США), был представлен доклад о возможных способах атак на анонимную сеть Tor. Его авторы, ученые Университета Джорджтауна и Исследовательской лаборатории ВМФ США, констатировали, что правительства многих стран рассматривают Tor как угрозу. Тоталитарные режимы беспокоит использование Tor правозащитниками и журналистами для обхода государственной цензуры. Но и у демократических стран хватает претензий к анонимной сети: общеизвестно, что она используется для торговли наркотиками и оружием, распространения детской порнографии и других видов противозаконного контента. Спецслужбы вкладывают значительные силы и средства в разработку инструментов деанонимизации пользователей Tor. Однако, по мнению авторов исследования, есть куда более простой способ подорвать позиции анонимной сети. Это обычные DDoS-атаки.

Ученые подсчитали, что атака, способная полностью блокировать сеть Tor, потребует колоссальной мощности в 512,73 Гбит/с и ее организация будет стоить более 7 миллионов долларов в месяц. Понятно, что это слишком большая сумма, тем более, что одного месяца явно недостаточно, чтобы все пользователи успели отвернуться от Tor. Но есть куда более простые и «бюджетные» варианты атак. Один из них – DDoS-атака на так называемые «мосты» Tor – специальные серверы, которые служат для входа в сеть. IP-адреса мостов не размещаются в общедоступных директориях и поэтому не могут быть заблокированы, в отличие от обычных узлов – поэтому именно мосты используются для входа в Tor в ряде стран, блокирующих узлы анонимной сети. В настоящий момент существует 38 мостов, из которых работают лишь 12. DDoS-атака, которая перекроет доступ к ним, обойдется всего лишь в 17 тысяч долларов в месяц. Но даже если все 38 мостов будут введены в строй, их блокировка атакой потребует примерно 31 тысячи долларов в месяц. Эти суммы вполне посильны спецслужбам любой страны.

Другой вариант – DDoS-атака на систему распределения сетевой нагрузки TorFlow. Она автоматически определяет степень загрузки узлов и перераспределяет трафик, чтобы избежать перегрузок и, соответственно, снижения скорости работы. Всего лишь 2,8 тысяч долларов в месяц хватит, чтобы организовать на TorFlow DDoS-атаку, в результате которой скорость загрузки страниц для всех пользователей снизится примерно на 80 процентов. Авторы исследования заключают, что спецслужбы вполне могут взять на вооружение такие DDoS-атаки для борьбы с Tor, поскольку они куда дешевле и эффективнее попыток деанонимизировать пользователей. Ученые также отмечают, что способы защититься от этих атак вполне очевидны, однако они требуют дополнительных инвестиций, а организация Tor Project уже на протяжении нескольких лет испытывает серьезную нехватку финансирования.» ***(Ученые рассказали, сколько стоит «уронить» Tor // ООО «Технический центр Интернет» (https://tcinet.ru/press-centre/technology-news/6663/). 19.08.2019).***

***

«Специалисты по кибербезопасности смогут заработать до $10 000 благодаря программе по поиску багов в программном обеспечении, запущенной ассоциацией Libra…

«Размер награды будет зависеть от конкретного бага. Это отличная возможность для сообщества Libra. Кроме того, она согласуется с ценностями сообщества информационной безопасности в целом», – отметил он.

В настоящее время организация уже проводит программу, в которой принимает участие 50 внешних специалистов, а сегодняшнее объявление является ее расширением. Для привлечения широкой общественности к поиску багов разработчики решили воспользоваться платформой HackerOne…

Глава по коммуникационному взаимодействию Ассоциации Libra Данте Диспарт отметил, что тестовая сеть криптовалюты по-прежнему находится на стадии разработки. Таким образом, обнаруженные сейчас уязвимости могут существенным образом повлиять на финальный релиз…» ***(Libra предлагает***

заработать до $10 000 на поиске багов // LetKnow OÜ (https://letknow.news/news/libra-predlagaet-zarabotat-do-10-000-na-poiske-bagov-28825.html). 27.08.2019).

***

Сполучені Штати Америки

«Министерство внутренней безопасности США, Агентство национальной безопасности и ФБР продолжают испытывать острую нехватку специалистов по кибербезопасности, и для привлечения квалифицированных кадров готовы идти на негласное смягчение требований к кандидатам. Об этом сообщает ресурс The Register, ссылаясь на беседы с анонимными источниками в названных ведомствах в ходе конференции по кибербезопасности Black Hat. Как известно, употребление наркотиков делает работу в правоохранительных органах и спецслужбах США невозможной. Однако похоже, что теперь американские власти готовы закрыть глаза на некоторые «грехи молодости». Особенно это касается марихуаны, употребление которой уже легализовано в нескольких штатах.

«Я и сам в старших классах был не прочь выкурить косяк-другой, - рассказал на условиях анонимности один из сотрудников АНБ США, – и, если сейчас вы без проблем проходите тесты на наркотики, это никак не влияет на вашу работу или возможность трудоустройства». В свою очередь один из присутствовавших на конференции агентов ФБР сообщил, что даже однократное употребление в прошлом любых наркотиков закрывает двери перед соискателями работы. Но для марихуаны сделано исключение: кандидат может получить работу, если употреблял ее в принципе, но не делал этого на протяжении трех последних лет.

Не вполне понятно, как может быть проверено такое утверждение: даже самые совершенные тесты обнаруживают следы употребления наркотических веществ на протяжении максимум трех последних месяцев. Как бы там ни было, очевидно, что правоохранительные органы и спецслужбы испытывают острую потребность в «белых хакерах» высокого класса и готовы простить им некоторые их прошлые привычки.» ***(ФБР готово простить специалистам по кибербезопасности любовь к марихуане // ООО «Технический центр Интернет» (https://tcinet.ru/press-centre/technology-news/6651/). 08.08.2019).***

***

Російська Федерація та країни ЄАЕС

«Более половины DDOS-атак на органы власти России ведется с территории США, заявил глава комиссии Совета Федерации по защите государственного суверенитета Андрей Климов…

Ранее он также заявил, что США и их сторонники пытаются повлиять на выборы в Мосгордуму с помощью провокаций. По его словам, признаки внешнего вмешательства есть в протестных акциях в Москве…» ***(Сергей Гурьянов. США***

оказались главным источником DDOS-атак на Россию // Деловая газета «Взгляд» (https://vz.ru/news/2019/8/8/991482.html). 08.08.2019).

***

«Комитет национальной безопасности (КНБ) Казахстана завершил тестирование национального сертификата безопасности и разрешил гражданам удалить приложение со своих смартфонов.

"В результате создана система по предотвращению киберугроз как в кибер-, так и информационном пространстве", — рассказали в КНБ.

По данным ведомства, за последний месяц власти Казахстана выявили более 8 млн фактов вирусной активности,

130 тысяч кибератак и случаи кибершпионажа в отношении государственных органов и компаний.

"Применение сертификата безопасности в дальнейшем будет осуществляться при возникновении угрозы национальной безопасности в виде кибер- и информационных атак, с предварительным уведомлением граждан Республики Казахстан", — добавили в ведомстве…» ***(Спецслужбы Казахстана разрешили удалить сертификат безопасности // kasparov.ru (http://www.kasparov.ru/material.php?id=5D4ADAE6DB353). 07.08.2019).***

***

Протидія зовнішній кібернетичній агресії

«КНДР зібрала близько 2 мільярдів доларів на програми зброї масового знищення за допомогою масштабних кібератак на банки та біржі криптовалют. Про це йдеться в конфіденційній доповіді ООН...

Доповідь підготували для санкційного комітету Північної Кореї Ради безпеки ООН незалежні експерти, що протягом півроку стежили за ситуацією.

У документі наголошується, що КНДР "продовжувала розвивати свої ядерні та ракетні програми, хоча й не проводила ядерних випробувань або запусків міжконтинентальних балістичних ракет".

"Північна Корея використовувала кіберпростір для вчинення все більш високотехнологічних атак з метою викрадання коштів у фінансових інститутів і бірж криптовалют для отримання доходу", - йдеться в доповіді.

Також зазначається, що Пхеньян використовував кіберпростір для відмивання викрадених коштів.

"Кібердіячі КНДР, багато з яких діють за вказівками Генерального бюро розвідки, збирають кошти на північнокорейські програми зброї масового ураження. За приблизними оцінками, загальна виручка на сьогодні сягає близько двох мільярдів доларів", - йдеться в доповіді…» ***(Денис Масліков. КНДР зібрала 2 млрд доларів на військові програми за допомогою кібератак принтери // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1817380-kndr-zibrala-2-mlrd-dolariv-na-viyskovi-programi-za-dopomogoyu-kiberatak). 06.08.2019).***

***

«Журналисты The Insider и Bellingcat стали объектами наиболее изощренной из всех последних фишинговых атак ГРУ. Вместе с ними среди целей оказались не менее десяти других журналистов и сотрудников НКО из России, Европы и США. Атаки имели несколько волн и начались примерно в конце апреля 2019 года.

В начале апреля хакеры зарегистрировали 11 доменных имен для того, чтобы маскировать атаки под письма ProtonMail. Факт фишинга подтвердила администрация швейцарского защищённого почтового сервиса ещё в конце июля текущего года — по её словам, атака не увенчалась успехом из-за бдительности как самих журналистов Bellingcat, так и сервиса, который предпринял ряд мер для нейтрализации возникшей опасности.

Bellingcat и ProtonMail убеждены, что за фишинговой атакой стоят российские хакеры и ГРУ. Об инциденте уведомили швейцарское ведомство по компьютерной безопасности.

В ходе фиксации всех атак, начиная с конца апреля по конец июля, The Insider и Bellingcat выяснили, что атака шла с нескольких адресов, а рассылаемый фишинг представлял собой фейковые предупреждения от лица ProtonMail о подозрительных попытках входа или о взломе аккаунта.

В почте отправитель отображался обычно как support[@]protonmail.ch (действительный адрес ProtonMail), но реальными отправителями (его можно увидеть, например, если нажать «ответить на письмо») были аккаунты с бесплатного почтового сервисе mail.uk — kobi.genobi[@]mail[.]uk and notifysendingservice[@]mail[.]uk.

Текст фишинговых писем и по содержанию и по оформлению был очень похож на реальные предупреждения ProtonMail и содержал в себе гиперссылку, пройдя по которой пользователь должен был перейти в настройки, чтобы поменять пароль и «защитить» свой аккаунт.

Руководство ProtonMail назвало эту атаку наиболее изощренной из всех, с которыми приходилось сталкиваться компании. Также в компании пояснили, что скрипты фальшивых доменов были синхронизированы с реальным доменом ProtonMail, что в теории могло бы позволять обходить двухфакторную аутентификацию (то есть, если бы пользователь вводил код второго фактора на фишинговом сайте, этот же код автоматически вводился бы и на реальном). Правда, неизвестно, удалось ли хакерам использовать этот прием.

Попытка ввести журналистов в заблуждение была очень убедительной, однако никто из них не попался на удочку и не выдал свой пароль, подчеркнул журналист-расследователь Belligcat Кристо Грозев.

Грозев координировал расследование сети по делу об отравлении в марте 2018 года в Солсбери бывшего двойного агента Сергея Скрипаля. Именно журналисты Bellingcat выяснили тогда настоящие имена агентов Главного управления Генштаба вооруженных сил РФ (бывшее ГРУ) Александра Петрова и Руслана Боширова, предположительно стоящих за этим отравлением.

По словам Грозева, «нет никаких сомнений, что ответственность за хакерскую атаку несет военная разведка ГРУ». С ним согласен и начальник швейцарской компании-провайдера ProtonMail Энди Йен.» ***(Госхакеры организовали фишинговую атаку на журналистов с адресов ProtonMail // РосКомСвобода (https://roskomsvoboda.org/48832/). 12.08.2019).***

***

«…Национальная служба по вопросам кибер- и информационной безопасности Чехии подозревает в недавней кибератаке на компьютеры Министерства иностранных дел зарубежные государства. Служба не уточняет, какая именно страна подозревается, сообщает издание Denik N.

Председатель партии STAN Вит Ракушан потребовал созвать комитет по вопросам безопасности парламента в связи с атакой.

Как стало известно ранее, 31 июля нынешнего года киберпреступники атаковали компьютеры Министерства иностранных дел Чехии. Злоумышленникам не удалось получить доступ к конфиденциальной информации из-за систем защиты, однако они успели взломать несколько ящиков электронной почты сотрудников МИД.» ***(Чехия подозревает зарубежные страны в кибератаках на МИД // SecurityLab.ru (https://www.securitylab.ru/news/500458.php). 14.08.2019).***

***

«Официальные круги Запада уже открыто говорят о необходимости превентивных кибератак в отношении других стран и публично к ним готовятся, заявил заместитель секретаря Совета безопасности России Олег Храмов.

По его словам, в доктринах стран Запада глобальное информационное пространство рассматривается как «виртуальный театр боевых действий».

«Для достижения этих целей Запад разрабатывает все новые и новые способы использования информационных технологий для силового воздействия на своих политических оппонентов», – сказал он в интервью «Российской газете».

Он указал, что подготовка к таким акциям уже начала носить публичный характер – в частности, на сайте АНБ США указана одна из основных задач исследований: «создание средств проникновения в труднодостижимые цели, которые представляют угрозу государству, где бы, когда бы или от кого бы они ни исходили».

«Фактически официальные круги стран Запада открыто заявляют о необходимости проведения превентивных кибератак», – добавил замсекретаря СБ.

Он также добавил, что США хотят придать легитимность своим обвинениям в адрес других стран, которые якобы совершали кибератаки. Это, отметил он, нужно для проведения против этих государств военных операций.

«Для придания хоть какой-то легитимности надуманным обвинениям в проведении кибератак американцы продвигают новую концепцию – «выяви и пристыди» («name and shame»)», – сказал он.

Храмов добавил, что основным доказательным аргументом в определении виновного будет, видимо, «известный тезис «хайли лайкли» («highly likely») – «с высокой вероятностью».

«Цель ясна – легализовать возможность проведения не только информационных, но и военных операций против «неудобных» государств, вплоть до применения ядерных арсеналов», – указал замсекретаря Совбеза.

Также он прокомментировал запрет Вашингтона на использование в госорганах США продукции российской «Лаборатории Касперского» и действия против китайской Huawei. Храмов заявил, что это «откровенное «выдавливание» с рынка конкурентов»…» ***(Сергей Гурьянов. Россия оценила намерения Запада проводить превентивные кибератаки // Деловая газета «Взгляд» (https://vz.ru/news/2019/8/14/992386.html). 14.08.2019).***

***

«Разведслужбы обеспокоены тем, что в 2020 году иностранные хакеры могут не только атаковать системы, но и попытаться манипулировать ими, испортить или уничтожить данные.

Власти США намерены примерно через месяц ввести в действие программу, направленную на защиту баз данных избирателей и систем от хакерских атак в преддверии выборов 2020 года…

По словам бывших и нынешних чиновников, разведслужбы обеспокоены тем, что в 2020 году иностранные хакеры могут не только атаковать системы, но и попытаться манипулировать ими, испортить или уничтожить данные.

«По нашим оценкам, эти системы подвергаются высокой степени риска», – отметил один высокопоставленный чиновник, добавив, что это один из немногих элементов избирательных технологий, который регулярно подключается к Сети.

В Агентстве по кибербезопасности и безопасности инфраструктуры (Cybersecurity Infrastructure Security Agency, CISA), входящем в состав Министерства внутренней безопасности, опасаются, что базы данных могут подвергнуться атаке программ-шифровальщиков. От атак с использованием подобного вредоносного ПО уже пострадали десятки американских городов, включая Балтимор и Атланту.

Меры по противодействию программам-вымогателям предпринимаются наряду с более масштабными действиями по определению наиболее вероятных векторов кибератак, направленных на выборы в ноябре 2020 года, отмечают чиновники.

В рамках программы CISA избирательные органы штатов будут готовить к подобным сценариям, предоставляя обучающие материалы, устраивая тестирование на проникновение в системы и проверки на наличие уязвимостей. Также будут предоставляться рекомендации по предотвращению и восстановлению от подобных атак. Тем не менее, в рекомендациях не будет указано, следует ли в случае заражения программой-вымогателем выплачивать выкуп или нет.» ***(В США запустят программу по защите избирательных систем от кибератак // SecurityLab.ru https://www.securitylab.ru/news/500642.php). 27.08.2019).***

***

«В армии Соединенного Королевства появилось специализирующееся на ведении информационной войны подразделение, задача которого – воздействовать на общественное мнение и противников государства.

Подразделение получило наименование Шестая дивизия, оно призвано реагировать и предпринимать ответные меры на атаки в Сети. «Характер ведения войны продолжает меняться по мере того, как границы между обычными и нетрадиционными способами ведения войны становятся все более размытыми. Армия должна оставаться адаптирующейся и развиваться как боевая сила», – заявил командующий сухопутными силами Великобритании генерал-лейтенант Айван Джонс…

Шестая дивизия призвана «противостоять «пагубной деятельности», которую якобы ведет Россия, и «угрозам со стороны технологически развитых террористических групп, таких как ИГ*».

Командиром подразделения назначен нынешний глава Сил боевого и тылового обеспечения британской армии генерал-майор Джеймс Баудер, в состав ведомства по борьбе с киберугрозами войдут служащие подразделений британской армии, а также военно-морского флота и ВВС…» ***(Елизавета Булкина. В Британии появилось подразделение по борьбе с «кибератаками» со стороны России // Деловая газета «Взгляд» (https://vz.ru/news/2019/8/1/990393.html). 01.08.2019).***

***

Захист персональних даних

«Несмотря на утечку данных и взломы крупных компаний, включая ритейлеров и поставщиков финансовых услуг, пользователи интернета по-прежнему полагаются на одни и те же пароли для нескольких веб-сайтов, говорится в новом исследовании Google. По результатам исследования, 1,5% всех учетных данных в интернете могут быть использованы для кибератак, поскольку были раскрыты вследствие утечек.

Для проведения исследования компания Google в феврале текущего года создала сервис уведомлений об утечках данных и связанное с ним расширение браузера Chrome Password Checkup, собирающее анонимные и хешированные учетные данные. С тех пор, как Google сделал его доступным, в нем приняли участие более 650 000 пользователей.

Когда пользователь входит на сайт с установленным расширением, анонимизированный хеш учетных данных отправляется на сервер Google и сверяется с 4 млрд имен пользователей и паролей, раскрытых в результате утечек.

В случае совпадения появляется уведомление, которое предупреждает пользователя и предлагает сменить пароль.

По данным анонимной статистики, 1,5% из 21 177 237 отслеживаемых логинов и паролей были обнаружены в утечках данных. Однако только 26% предупрежденных пользователей сменили пароли. Из них 60% сменили пароли на более безопасные.

Больше всего предупреждающих уведомлений было на интернет-порталах для взрослых (3,6%) и развлекательных сайтах с потоковым видео (6,3%)…» ***(Исследование: пользователи неохотно меняют скомпрометированные пароли // РосКомСвобода (https://roskomsvoboda.org/48953/). 16.08.2019).***

***

«…Один из сайтов Европейского центрального банка (ЕЦБ) был взломан. Злоумышленники получили доступ к конфиденциальной информации пользователей, однако внутренние системы банка не были скомпрометированы.

Для проведения фишинговых операций киберпреступники установили вредоносное ПО на внешний сервер ЕЦБ, где была размещена система Banks' Integrated Reporting Dictionary (BIRD), сообщает издание Bloomberg.

Web-сайт BIRD предоставляет банкам подробную информацию о составлении статистических отчетов и физически отделен от других внешних и внутренних систем ЕЦБ. По словам представителей банка, в руки злоумышленников попали адреса электронной почты, имена и данные о должностях 481 подписчика новостной рассылки BIRD, однако пароли остались нетронутыми. Утечка была обнаружена во время регулярного технического обслуживания, после чего ЕЦБ закрыл web-сайт и предупредил пользователей о раскрытии их данных…» ***(Данные пользователей Европейского центрального банка были похищены // SecurityLab.ru (https://www.securitylab.ru/news/500486.php). 16.08.2019).***

***

«Данные пользователей биометрической СКУД Biostar 2 от компании Suprema хранились на незащищенном сервере.

Исследователи безопасности из vpnmentor Hoam Ротем (Noam Rotem) и Рэн Локар (Ran Locar) обнаружили в открытом доступе биометрические данные 1 млн человек. Отпечатки пальцев, данные для распознавания лиц, незашифрованные логины и пароли администраторов и другая информация хранились в открытой базе данных на незащищенном сервере.

База данных принадлежит южнокорейской компании Suprema, разработчику системы контроля и управления доступом (СКУД) Biostar 2, используемой в офисных зданиях, на складах и пр. Для того чтобы войти в здание, человек должен пройти идентификацию по отпечаткам пальцев и лицу.

В прошлом месяце Suprema сообщила об интеграции Biostar 2 с системой управления доступом AEOS, используемой на 5,7 тысячах предприятий в 83

странах мира. В частности, Biostar 2 используется в британском Скотланд-Ярде, банках и на оборонных предприятиях.

Исследователи обнаружили открытую базу данных на прошлой неделе во время сканирования портов в поисках знакомых блоков IP-адресов. Изменяя критерии поиска URL-адресов в Elasticsearch, они смогли без труда просматривать содержимое БД. Более того, исследователи могли изменять данные и добавлять новых пользователей.

В общей сложности Ротем и Локар получили доступ к 27,8 млн записей и 23 ГБ данных, в том числе к панелям администрирования, отпечаткам пальцев, данным для распознавания лиц, фотографиям, незашифрованным логинам и паролям, журналам посетителей, сведениям об уровне доступа и персональным данным сотрудников организаций.

Ротем и Локар предприняли несколько попыток уведомить Suprema о проблемной БД. В среду, 14 августа, уязвимость была закрыта, однако компания так ничего и не ответила исследователям…» ***(Используемая полицией биометрическая СКУД допустила утечку данных 1 млн человек // SecurityLab.ru (https://www.securitylab.ru/news/500471.php). 15.08.2019).***

***

«…Фахівці з кібербезпеки виявили незахищену базу даних платформи Suprema Biostar 2, що містить відбитки пальців, зображення, імена, паролі та іншу особисту інформацію про більш ніж млн. людей…

Зазначається, що наразі вразливість системи виправили. Експерти з кібербезпеки рекомендують компаніям, що використовують Biostar 2, змінити паролі для доступу до системи.

“Відбитки пальців більш ніж мільйона осіб, а також інформація про розпізнавання особи, незашифровані імена користувачів і паролі, а також особисті дані співробітників були виявлені у загальнодоступній базі даних компанії, послугами якої користується поліція столиці Великобританії, оборонні підприємства і банки”, – йдеться у повідомленні…» ***(У відкритий доступ злили біометричні дані більше мільйона українців // "То є Львів" (https://inlviv.in.ua/ukraine/u-vidkrytyj-dostup-zlyly-biometrychni-dani-bilshe-miljona-ukrayintsiv). 16.08.2019).***

***

«Взломщики атаковали один из старейших книжных магазинов Мексики, удалив базу данных с информацией о 1,2 млн покупок и личными данными почти 1 млн пользователей. За возвращение информации злоумышленники потребовали с компании выкуп в 0,05 Btc (чуть больше 38 тыс. руб. по курсу на момент написания статьи).

Атака оказалась успешной из-за того, что администраторы Librería Porrúa оставили незащищенной базу данных под управлением MongoDB. За три дня до инцидента эту базу обнаружили с помощью Shodan исследователь Боб Дьяченко (Bob Diachenko) и специалисты Comparitech. Подключиться к ней и управлять данными мог абсолютно любой пользователь, поскольку сотрудники магазина не

подключили механизм аутентификации. Проблему усугублял тот факт, что хранилище было доступно сразу по двум IP-адресам — это упрощало его обнаружение.

Эксперты сообщили компании о возможности утечки, однако сотрудники Librería Porrúa не успели отреагировать. Через три дня после обнаружения открытой базы данных преступники удалили все ее содержимое и оставили сообщение с требованием выкупа. Прошло еще около суток, прежде чем хранилище исключили из публичного доступа.

Пострадали коммерческие записи Librería Porrúa: инвойсы с подробностями покупок, хешированные данные платежных карт, коды активации, токены, имена и контактные данные покупателей. Также в базе находилась информация о клиентах магазина: полные имена, даты их рождения и прочие личные сведения.

Специалисты отмечают, что простым сложением этих цифр невозможно установить реальное число пострадавших пользователей — в некоторых случаях данные пересекаются. Так или иначе, покупатели, чьи данные находились в базе, могут стать мишенью спамеров и фишеров. Большой объем личной информации позволит злоумышленникам тщательно планировать такие атаки. Кроме того, эксперты призывают клиентов Librería Porrúa внимательно читать письма от лица магазина — вполне возможно, что такие сообщения будут поступать от преступников.

Получили ли преступники выкуп и удалось ли восстановить удаленные данные, неизвестно. Представители пострадавшей компании воздерживаются от комментариев по поводу инцидента…» ***(Julia Glazova. Вымогатели удалили базу данных книжного магазина // Threatpost (https://threatpost.ru/libreria-porrua-mongodb-database-wiped/33698/). 07.08.2019).***

***

«Разработчики браузеров Google и Mozilla Firefox заблокируют работу правительственного сертификата безопасности, который скачали казахстанские граждане, говорится в совместном заявлении двух компаний. Решение было принято в связи с исследованием, проведенным платформой Censored Planet. Оно показало, что казахстанские интернет-провайдеры предоставляли пользователям доступ в интернет, только если те устанавливали разработанный властями цифровой сертификат на всех девайсах и использовали его во всех браузерах. С помощью сертификата власти могли отслеживать активность граждан на определенных сайтах. Речь, например, шла о Facebook, Twitter, Google и еще 34 сайтах.

«Мы серьезно относимся к принятию таких решений, но защита наших пользователей и интернета в целом — это то, ради чего Firefox существует», — написал в сообщении старший директор Mozilla по вопросам доверия и безопасности Маршалл Эрвин.

«Мы не позволим любой организации скомпрометировать персональные данные пользователей Chrome, будь то государственная или коммерческая структура. Мы внедрим защиту от этого сертификата и всегда будем принимать

соответствующие меры для жителей по всему миру», — в свою очередь отмечает старший технический директор Google Париса Табриз.

В ответ на недавние действия правительства Казахстана, Chrome, наряду с другими браузерами, предпринял шаги для защиты пользователей от перехвата или изменения соединений TLS с веб-сайтами, также говорится в блоге компании…» ***(«Казах-посередине» заблокирован Google и Mozilla // РосКомСвобода (https://roskomsvoboda.org/49053/). 21.08.2019).***

***

«…В системах бронирования авиабилетов некоторых авиалиний, находящихся в ведении самих предприятий, обнаружены серьезные уязвимости, подвергающие риску данные клиентов.

Многие авиакомпании позволяют клиентам просматривать и вносить изменения в информацию о рейсе, используя уникальный шестизначный номер бронирования, состоящий из букв и цифр. В свою очередь, этот номер связан с записью регистрации пассажира (PNR) со всеми персональными данными и информацией о полете.

По словам исследователя Ахмеда Эль-Фанаджели (Ahmed El-fanagely), обнаружившего уязвимость, некоторые авиакомпании не внедрили специальные механизмы защиты своих систем бронирования. В связи с этим любой злоумышленник может с помощью брутфорса получить PNR-идентификатор. Ахмед разработал инструмент, позволяющий получить доступ к информации о рейсе случайного человека, используя распространенные фамилии и брутфорс. Также можно отслеживать перелеты конкретного человека, зная фамилию и авиакомпанию, которую он использует. Злоумышленник может использовать этот метод для получения доступа к различным типам информации, включая имя, контактные данные, данные билета, маршрут, номер паспорта, дату рождения и даже информацию об оплате.

Уязвимость затрагивает несколько крупных авиакомпаний в Европе и на Ближнем Востоке. Пострадавшие компании используют систему управления бронированием от Amadeus — расположенного в Испании поставщика глобальных распределительных систем (GPC), услугами которого пользуются более 200 авиакомпаний по всему миру…» ***(Уязвимость в системах бронирования авиабилетов ставит под угрозу данные клиентов // SecurityLab.ru (https://www.securitylab.ru/news/500626.php). 26.08.2019).***

***

«Как стало известно из нового отчёта Cyber Threats and Healthcare американской компании FireEye, специализирующейся на кибербезопасности, хакеры, предположительно из Китая, взломали сайт крупной индийской организации здравоохранения и похитили 6,8 млн. записей, содержащих информацию о пациентах и врачах. Записи содержат конфиденциальную персональные данные пациентов, информацию об их лечащих врачах, диагнозах и историю лечения. Киберпреступники продают украденные данные на подпольных

рынках – в период с октября 2018 г. по март 2019 г. аналитики FireEye обнаружили несколько баз данных, которые стоили более 2 тыс. долл.

Также в отчете эксперты отметили, что хакерские группировки, базирующиеся в Китае, стали чаще выбирать целями атак медицинские учреждения, специализирующиеся на борьбе с раком. По мнению аналитической компании, это отражает растущую обеспокоенность КНР по поводу роста заболеваемости раком и смертности в стране, а также призвано помочь сократить государственные расходы на здравоохранение.

Другая вероятная мотивация деятельности хакеров – финансовая. В КНР один из самых быстрорастущих фармацевтических рынков в мире. Доступ к исследованиям международных компаний создает выгодные возможности для китайских фирм. Это может позволить китайским корпорациям выводить на рынок новые лекарства быстрее, чем западные конкуренты, говорится в отчёте FireEye.» ***(Хакеры похитили и продают 7 млн. медицинских записей индийской организации // Компьютерное Обозрение (https://ko.com.ua/hakery_pohitili_i_prodayut_7_mln_medicinskih_zapisej_indijskoj_organizacii_129916). 23.08.2019).***

***

Кіберзлочинність та кібертероризм

«…Команда исследователей, состоящая из специалистов Microsoft и ученых китайского, южнокорейского и американского университета, проанализировала 250 тыс. сайтов из списка Alexa и выявила три техники, в настоящее время используемые киберпреступниками для перехвата кликов.

В ходе исследования под названием «All Your Clicks Belong to Me: Investigating Click Interception on the Web («Все ваши клики принадлежат мне: Исследование перехвата кликов в Сети») специалисты создали фреймворк Observer для мониторинга перехвата кликов. Из-за динамического, событийного характера web-приложений оценить скрипты для кликджекинга, просто взглянув на код приложения, невозможно, в связи с этим и был разработан инструмент Observer.

На 613 из 250 тыс. изученных сайтов исследователи обнаружили 437 сторонних скриптов для перехвата кликов. Общая аудитория этих сайтов составляет 43 млн пользователей в день.

Сторонние скрипты обманом заставляют жертв нажимать на элементы сайта, либо выглядящие как оригинальный контент, либо незаметные и размещенные поверх оригинального контента. Некоторые скрипты перехватывают клики с целью монетизации, отметили исследователи. Так, 36% от 3251 уникального URL-адреса для перехвата кликов связаны с рекламой – главным способом монетизации в Сети. Помимо монетизации, киберпреступники используют кликджекинг для заражения систем пользователей вредоносным ПО.

В список техник кликджекинга входит перехват гиперссылок (с помощью сторонних скриптов, взаимодействующих с оригинальными URL-адресами, или огромных ссылок, закрывающих большую часть страницы), добавление в элемент

страницы слушателя событий, связанного с навигацией, а также различные визуальные техники (например, копирование оригинального элемента или использование прозрачных слоев).» ***(На сайтах с аудиторией 43 млн пользователей в день обнаружены скрипты для кликджекинга // SecurityLab.ru (https://www.securitylab.ru/news/500494.php). 16.08.2019).***

***

«…Исследователи из компании Cofense обнаружили целенаправленную фишинговую кампанию против сотрудников фирмы энергетической отрасли. В рамках атак злоумышленникам удалось обойти шлюз электронной почты Microsoft.

Документы, связанные с фишинговыми лендинговыми страницами, распространялись через Google Документы. Сообщения были отправлены от имени генерального директора компании с целью обманом заставить сотрудников открыть «важное сообщение», передаваемое через Google Docs.

Отправленные через Google Диск письма позволили злоумышленникам обойти защиту от фишинга, предоставляемую облачным сервисом фильтрации электронной почты Microsoft Exchange Online Protection. В действительности документ был связан с документом Google Docs, который перенаправлял потенциальных жертв на фишинговые страницы злоумышленников. Там пользователям предлагалось ввести свои учетные данные для доступа к срочному сообщению генерального директора.

Однако киберпреступники использовали устаревшую информацию для создания своих фишинговых писем, предоставив жертвам возможность заподозрить неладное. По словам исследователей, некоторые письма создавались с помощью шаблонов, предназначенных для быстрой генерации настраиваемых фишинговых сообщений. Как минимум две фразы, использованные в последних атаках, были ранее обнаружены в рамках аналогичной фишинговой кампании, нацеленной на учебные заведения.» ***(Злоумышленники используют Google Диск в рамках фишинговой кампании // SecurityLab.ru (https://www.securitylab.ru/news/500493.php). 16.08.2019).***

***

«Количество кибератак за последние шесть лет выросло на 57%.

По данным Национального координационного центра по компьютерным инцидентам, за 2018 год на критические инфраструктуры РФ было совершено более 4,3 млрд кибератак. Об этом сообщил заместитель секретаря Совета безопасности РФ Олег…

По словам Храмова, количество кибератак за последние шесть лет выросло на 57%. Если за период с 2014 по 2015 год случаи скоординированных целенаправленных атак составляли около 1,5 тыс. в год, то в 2018 году их количество превысило 17 тыс. Особую опасность представляют атаки, направленные на выведение из строя оборудования объектов критической инфраструктуры.

С начала нынешнего года было предотвращено внедрение вредоносного программного обеспечения на более чем 7 тыс. объектов критических инфраструктур. Целями атак злоумышленников становились объекты кредитно-финансовой сферы (38% от всех атак), органов государственной власти (35%), оборонной промышленности (7%), сферы науки и образования (7%) и сферы здравоохранения (3%).

По данным американской компании Webroot, в 2018 году на долю США пришлось 63% интернет-ресурсов, распространяющих вредоносное ПО, тогда как доля Китая и России составляет всего 5% и 3% соответственно.» ***(За 2018 год на РФ было совершено около 4,3 млрд кибератак // SecurityLab.ru (https://www.securitylab.ru/news/500473.php). 15.08.2019).***

***

«…На пользователей в Израиле была направлена новая мошенническая кампания, в рамках которой использовался SMS-фишинг. Злоумышленники от имени легитимных организаций отправляли SMS-сообщения с целью убедить жертву загрузить вредоносное приложение, перейти по ссылке или предоставить личную информацию, такую как данные банковского счета или кредитной карты.

По словам исследователей из Check Point, сообщения поступали от одного из крупнейших банков Израиля и содержали следующий текст: «Здравствуйте, сэр. В вашем аккаунте обнаружена подозрительная активность. Авторизируйтесь для подтверждения своего аккаунта». При переходе по ссылке в SMS жертва попадает на поддельную web-страницу банка, принадлежащую легитимному, но скомпрометированному сайту. В этом случае любая введенная информация раскрывается злоумышленникам, включая логин, пароль, имя, фамилию, адрес электронной почты, идентификационный номер, имя владельца кредитной карты, номер кредитной карты, дату истечения срока ее действия и cvv…» ***(Пользователи в Израиле подверглись новой фишинг-атаке // SecurityLab.ru (https://www.securitylab.ru/news/500405.php). 13.08.2019).***

***

«…Специалисты компании ReversingLabs предупредили о новой фишинговой кампании, в ходе которой злоумышленники используют для выманивания учетных данных пользователей не лендинговые страницы, а PDF-документы.

«Одним из векторов атак, который можно легко упустить из виду, является похищение учетных данных через документы с активированными скриптами JavaScript. Метод атаки основывается не на использовании вредоносных ссылок или спуфинге доменов, а на скриптах в документах, обеспечивающих такой же результат», - сообщили исследователи.

В ходе обнаруженной специалистами ReversingLabs фишинговой кампании, нацеленной на пользователей в Германии, злоумышленники рассылают поддельные налоговые накладные от Amazon, для просмотра которых пользователю якобы нужно авторизоваться в своей учетной записи Amazon Seller. При открытии вложенного в электронное письмо PDF-документа появляется

созданное с помощью JavaScript окно авторизации, запрашивающее электронный адрес и пароль.

Неискушенный пользователь может подумать, что так должно быть и это просто новый способ защиты данных, и ввести свой пароль. После того, как информация была введена в поле, она сразу же отправляется мошенникам.» ***(Фишеры похищают учетные данные пользователей Amazon через PDF-документы // SecurityLab.ru (https://www.securitylab.ru/news/500332.php). 07.08.2019).***

***

«…Как сообщают специалисты команды X-Force IRIS компании IBM, за последние шесть месяцев количество атак на промышленные предприятия увеличилось в два раза. Половина атакованных предприятий задействованы в производственном секторе, а целью атак является подрыв производственных процессов…

Главным предназначением вредоносного ПО наподобие Industroyer, NotPetya или Stuxnet является не скрытое похищение данных, а выведение из строя оборудования. В их функционал входит блокировка компьютера, выведение системы из строя, удаление файлов и т.п.

По словам исследователей, обычно вредоносное ПО Stuxnet, Shamoon или Dark Seoul, предназначенное для выведения из строя промышленного оборудования, используется хакерами, действующими в интересах того или иного государства. Тем не менее, с конца 2018 года компоненты для удаления файлов в свое ПО стали добавлять рядовые киберпреступники. Ярким примером являются атаки с использованием вымогательского ПО LockerGoga и MegaCortex.

По данным IBM, в первой половине 2019 года количество атак с использованием подобного вредоносного ПО удвоилось по сравнению со вторым полугодием 2018 года. Наибольшему риску кибератак с использованием деструктивного вредоносного ПО подвергаются компании нефтегазовой промышленности и образовательные учреждения. Большая часть таких атак, зафиксированных IBM, пришлась на организации в Европе, США и странах Среднего Востока.

Наиболее распространенный вектор заражения – фишинговые письма, похищение учетных данных для авторизации во внутренней сети, атаки watering hole и взлом подрядчиков, имеющих прямую связь с целевой организацией.

Эксперты отмечают две формы целевых атак. Первая предполагает продолжительное нахождение атакующего в сети жертвы до непосредственного нападения. Вторая форма – быстрая атака, осуществляемая сразу же после проникновения в сеть.» ***(За последние полгода удвоилось число атак на промышленные предприятия // SecurityLab.ru (https://www.securitylab.ru/news/500285.php). 05.08.2019).***

***

«…Дослідники з Університету Флориди і Google вивчили психологію фішингових листів і те, як хакери використовують людську натуру, щоб

спонукати їх натискати на шкідливі посилання. Професор UF Даніела Олівейра, яка очолювала дослідження разом з доктором Наталі Ебнер, представила дані на конференції з кібербезпеки Black Hat в Лас-Вегасі. До Олівейрі приєдналася Елі Бурштейн, яка очолює дослідницьку групу Google по боротьбі зі зловживаннями.

Фішингові атаки – це онлайн-біда сьогодення, де хакери видають себе за законні установи в надії отримати особисту інформацію, таку як паролі. Відповідно до щорічного звіту Verizon, фішинг, який зазвичай відбувається по електронній пошті, є основною причиною витоку даних. За словами Бурштейн, Google блокує близько 100 млн фішингових листів щодня.

Зловмисники постійно змінюють і оновлюють свої проекти, щоб зробити їх більш ефективними…

В ході тритижневого експерименту 158 учасників, яким сказали, що вони беруть участь в дослідженні про те, як люди використовують інтернет, будуть отримувати фішингові електронні листи один раз в день. Дослідники відстежуватимуть, чи натиснули вони на нього. Листи ґрунтувалися на реальних фішингових кампаніях, виявлених Google.

Фішингові електронні листи створені для використання людської натури. Вони вважають, що люди швидко приймають рішення, не замислюючись, немов перехід по посиланню був рефлексом, а не когнітивним рішенням…

Коли справа доходить до прийняття рішень, наш мозок може працювати двома способами, говорить дослідник, посилаючись на теорію подвійного процесу. Ваш мозок працює автоматично для повсякденної діяльності, наприклад, для чищення зубів. Великі рішення, такі як покупка будинку, вимагають обмірковування. За її словами, кліки по посиланнях електронної пошти належать до дій, прийнятих нашвидкоруч і хакери покладаються на це…

На щастя, у всіх нас є психологічний захист, який працює у фоновому режимі. Олівейра каже, що люди з високим рівнем стресу краще виявляють обман, як фішингові електронні листи, і більш скептично ставляться до онлайн-шахрайства. Саме тому, деякі фішингові кампанії використовують психологічні тригери, щоб поліпшити настрій людей. Просто майте на увазі, що коли ви в гарному настрої, ваш природній захист стає слабшим.» ***(Грицина Вікторія. Google дослідив зв'язок між поганим настроєм і хакерами // Pingvin.pro (https://pingvin.pro/gadgets/news-gadgets/google-doslidyv-zv-yazok-mizh-poganym-nastroyem-i-hakeramy.html). 08.08.2019).***

***

«Грузинський телеканал «Пірвелі» 13 серпня зазнав кібератаки, яка спричинила збій у роботі медіа.

Про це повідомляє керівництво каналу TV Pirveli на Facebook-сторінці…

У ефірі телеканалу наразі не виходять інформаційні та політичні передачі, натомість транслюють лише художні фільми.

«Сьогодні вранці на центральний сервер каналу була здійснена кібератака, яка повністю паралізувала його роботу, через що повноцінне мовлення неможливе. У ефір не вийшла передача "Діловий ранок" й досі не виходять інформаційні та політичні передачі», – йдеться в повідомленні.

За даними керівництва каналу, кібератака сталася о 05:00 (о 04:00 за київським часом). Міністерство внутрішніх справ Грузії проводить перевірку…» ***(Грузинський телеканал зазнав кібератаки // Детектор меді (https://detector.media/infospace/article/169826/2019-08-13-gruzinskii-telekanal-zaznav-kiberataki/). 13.08.2019).***

***

«Согласно отчету компании Carbon Black, специализирующейся в области кибербезопасности, занимающиеся скрытым майнингом мошенники также зарабатывают на сборе защищенных данных.

Согласно отчету, хорошо известная бот-сеть скрытого майнинга Access Mining содержит дополнительный компонент, способный собирать IP-адреса, информацию о домене, имена пользователей и пароли. Исследователи из Carbon Black Грег Фосс (Greg Foss) и Мариан Лян (Marian Liang) говорят, что бот-сеть собирала конфиденциальные данные последние два года, заработав на этом миллионы.

Согласно сообщениям, 500 000 машин были подвергнуты атаке троянов с использованием протокола скрытого майнинга XMRig, что привело к получению мошенниками 8 900 XMR. Большинство зараженных машин находилось в России, Восточной Европе и Азиатско-Тихоокеанском регионе.

За этот период 500 000 компьютеров были взломаны не только с помощью протокола Ghost, но и программного обеспечения для сбора данных. В отчете говорится, что множество программ, взятых на GitHub, таких как Eternal Blue и Mimikatz, и внедренных в XMRig, помогали хакерам обновлять свое ПО.

Хакеры превратили сбор защищенных данных во вторичный источник дохода. При том, что одна зараженная машина приносит доход в среднем $6.75, 500 000 устройств позволяют заработать $1.69 млн. Зараженные устройства можно даже арендовать на 24-48 часов в качестве источника пассивного дохода для хакеров. В зависимости от местоположения и владельца компьютера, ценность устройства может меняться.

Фосс и Лян говорят, что появление Access Mining, скорее всего, является результатом падения цены Monero после «медвежьего» рынка 2018 года. После их отчета фирма выпустила серию советов для решения возможных проблем.» ***(Хакеры зарабатывают на сборе защищенных данных // LetKnow OÜ (https://letknow.news/news/hakery-zarabatyvaet-na-sbore-zashchishchennyh-dannyh-27795.html). 08.08.2019).***

***

«Официальный представитель МВД Беларуси Ольга Чемоданова разместила в своем Telegram-канале информацию о кибератаках на отечественные предприятия. По этим данным сотрудниками управления по раскрытию преступлений в сфере высоких технологий зафиксировано более десятка таких атак.

Представитель ведомства сообщает, что волна кибервирусов затронула компании всех форм собственности. Она также описала сам процесс передачи

вируса. На электронную почту предприятия поступает письмо, якобы отправленное партнерами. Темой письма обозначается «Окончательный расчет», «Счет-фактура» или что-то подобное. К письму прикреплен файл в расширением «*.exe». Открытие такого вложения приводит к заражению вирусом, при этом на экране появляется заставка об обновлении ОС.

Сразу после этого запускается вредоносный процесс. В частности, формируется платежное поручении на перевод мошенникам финансовых средств на расчетный счет. Ольга Чемоданова сообщает, что в последнем случае со счета минской фирмы было переведено 14 тысяч белорусских рублей…» ***(Светлана Пономарева. Белорусские предприятия атакуют хакеры // "Бизнес лидер" (http://www.profi-forex.by/news/entry5000041079.html). 17.08.2019).***

***

«…Специалисты Positive Technologies подвели итоги второго квартала 2019 года и выяснили, что доля целенаправленных атак продолжает расти, почти все атаки на промышленные компании совершались с помощью вредоносного ПО, а доля заражений майнерами вновь вернулась на прежний уровень.

Увеличение доли целенаправленных атак — основной тренд второго квартала (59%, что на 12 процентных пунктов больше, чем в первом квартале). Общее количество уникальных киберинцидентов (как целенаправленных, так и массовых) на 3% превзошло показатель первого квартала 2019 года.

По данным экспертов, кража информации остается главной целью киберпреступников. Более половины атак во втором квартале совершалось с этой целью. При этом юридические лица были атакованы в первую очередь (29%) с целью кражи персональных данных. Для частных лиц высок риск компрометации учетных записей и данных банковских карт (44% и 34% соответственно от всего объема украденной информации у частных лиц).

«В компаниях могут храниться большие базы персональных и учетных данных клиентов. Злоумышленников также привлекают логины и пароли сотрудников компании-жертвы. Вот почему персональные и учетные данные — наиболее распространенные виды информации, которые интересуют киберпреступников при атаках на юридические лица. Что касается частных лиц, то они не всегда заботятся о безопасности своих учетных записей: используют нестойкие и одинаковые пароли, вводят учетные данные, не удостоверившись в надежности ресурса, выдают информацию о себе, которая может помочь подобрать пароль. Это объясняет высокую долю украденных учетных данных в атаках на частные лица», — отмечает аналитик Positive Technologies Яна Авезова.

Что касается финансовой выгоды, то ее злоумышленники преследуют в 30% и 42% атак на юридические и частные лица соответственно.

Во втором квартале 2019 года эксперты отметили вернувшийся интерес злоумышленников к криптоджекингу. Курс биткойна уверенно растет, и преступники продолжают развивать ПО для скрытого майнинга.

В минувшем квартале эксперты отметили рост доли заражения вредоносным ПО среди государственных учреждений (62% против 44% в первом квартале 2019

года). Наиболее часто государственные учреждения подвергались атакам трояновшифровальщиков. Так, под удар попала IT-инфраструктура нескольких городов США. В результате атак властям двух городов даже пришлось заплатить выкуп на общую сумму более миллиона долларов США, так как IT-ресурсов этих небольших населенных пунктов оказалось недостаточно для противостояния злоумышленникам.

Почти все атаки на промышленные предприятия (96%) во втором квартале 2019 года совершались с использованием вредоносного ПО. Как отмечают эксперты, активные попытки проникновения во внутреннюю IT-инфраструктуру промышленных компаний предпринимает группировка RTM. «В прошлом квартале мы зафиксировали 26 вредоносных рассылок этой группы, — рассказывает директор экспертного центра безопасности Positive Technologies (PT Expert Security Center) Алексей Новиков. В списке адресатов, кроме финансовых учреждений, более десятка промышленных организаций в России и СНГ. Все письма составлены на русском языке и имеют схожую тематику; как правило, они содержат якобы финансовые документы (акты, счета) с просьбами проверить, подписать документы или осуществить оплату. Троян RTM ворует учетные записи, записывает видео, делает снимки экрана и передает их на сервер злоумышленников».

Во втором квартале специалисты PT ESC зафиксировали атаки группы TaskMasters, направленные на промышленные предприятия России. «После публикации нашего исследования о группе TaskMasters, а также доклада на конференции PHDays 9, посвященного деятельности группы, злоумышленники предприняли ряд мер для предотвращения передачи трафика за пределы компьютера жертвы. Это свидетельствует о том, что группа знает об обнаружении и, вероятно, приостановила свои действия», — подчеркнул Алексей Новиков.

Среди наиболее часто атакуемых организаций во втором квартале оказались и медучреждения. Вредоносное ПО, нарушающее работоспособность IT-систем организации, представляет особую угрозу для учреждений здравоохранения, где подобного рода инциденты могут дорого обойтись как самой компании, так и ее клиентам. Так, в результате апрельской атаки шифровальщика на офтальмологическую клинику JFJ Eyecare зашифрованными оказались персональные данные пациентов.

Сотрудники медицинских организаций нередко подвергаются и фишинговым атакам, как в случае с сотрудником одной из клиник Новой Шотландии (Канада). В результате успешной атаки в руки злоумышленников попали логин и пароль сотрудника, а данные около трех тысяч пациентов оказались под угрозой.

Эксперты отмечают, что злоумышленники могут атаковать медицинские организации с целью получения сведений не только о пациентах, но и сотрудниках. Так, за 500 долл. США в дарквебе продавались пакеты документов врачей: дипломы о медицинском образовании, рекомендации, лицензии на медицинскую деятельность. Эти случаи — наглядный пример того, что ценная информация представляют собой основную цель злоумышленников, и они продолжают пользоваться легкомысленным отношением к ее защите.» ***(Positive Technologies: десятки промышленных и финансовых организаций атакует троян, записывающий действия пользователей // Positive Technologies***

(https://www.ptsecurity.com/ru-ru/about/news/desyatki-promyshlennyh-i-finansovyh-organizaciy-atakuet-troyan-zapisyvayushchiy-deystviya-polzovateley/). 20.08.2019).

***

«Даниил Кручинин, основатель и CEO p2p-маркетплейса по продаже билетов на мероприятия Eticket4, рассказывает о выводах, которые сделал после нескольких DDoS-атак…

Первая по-настоящему крупная DDoS-атака на наш сайт произошла в октябре 2018-го – с пятницы на субботу. Киберпреступники специально выбирают такое время атаки, когда вы будете наименее к ней готовы…

Последняя атака на наш сайт случилась в июле этого года, после того как несколько крупных СМИ опубликовали новость о привлечении инвестиций. Буквально на следующий день на нас обрушилась атака более 40 мегабит/сек – самая мощная за всю работу нашего сервиса…

В этот раз мы решили проблему буквально за полтора часа, наши клиенты и партнеры практически ничего заметили. Мы были полностью готовы, потому что извлекли уроки и сделали правильные выводы из прошлых атак. Вот несколько главных рекомендаций, которые пригодятся всем.

Обеспечьте круглосуточную техническую поддержку

Техническая поддержка должна работать 24 часа в сутки семь дней в неделю, а системный администратор в любое время суток должен быть в доступе…

На информационной безопасности нельзя экономить

После того как мы справились с атакой в октябре 2018 года, мы сразу же максимально усилили инфраструктуру информационной безопасности – с запасом.

Тариф, достаточный для защиты от мощной атаки, обходится нам до 100 тысяч рублей в месяц. Также увеличивается ФОТ, ведь системный администратор должен быть всегда в доступе, затраты на техническую поддержку тоже увеличиваются…

Не бойтесь жертвовать конверсией в пользу безопасности

Защита должна быть настроена не только против DDoS-атак, но и против фрода, который тоже может принести большие финансовые и репутационные потери. Правда, тут может возникнуть дилемма.

Установка капчи против «левых» айпишников при регистрации, обязательное использование 3D-Security при оплате – все это серьезно снижает конверсию. Без них она сразу увеличивается на 10-15%, а то и все 25%...

Не спешите платить деньги хакерам

Как я уже говорил, фрод и DDoS – неизбежный этап развития. Чем вы популярнее, чем больше компания на виду, тем выше шанс, что вы привлечете внимание не только новых пользователей и клиентов, но и злоумышленников. Или вас закажут ваши конкуренты. Займитесь защитой прямо сейчас.

Но если вы все-таки оказались не готовы, у вас сейчас нет ресурсов для выстраивания защиты и дорога каждая секунда, а хакеры выставили небольшой чек – возможно, на этом этапе будет проще заплатить. Но после нужно сразу же начинать строить хорошую защиту от DDoS. Потому что к вам обязательно

вернутся – вы ведь уже попали в список компаний, с которых можно стрясти деньги.

Не мешайте работать своей команде

Сейчас во время крупных атак я стараюсь максимально дистанцироваться – чтобы не мешать работать сотрудникам. Мы постоянно мониторим работу сайта, и если он «лежит» хотя бы пару минут, то об этом оповещаются все ключевые сотрудники, включая топ-менеджеров.

Я слежу за происходящим, но не названиваю и не достаю сотрудников постоянными вопросами. У них есть план действий (конечно, если вы не экономили на команде при найме) и напряженная, нервная ситуация, а моя долбежка вряд ли им поможет.» ***(Даниил Кручинин. Вы ошибаетесь, если думаете, что вас это не касается. Пять выводов, которые я сделал после DDoS-атак // Rusbase (https://rb.ru/opinion/spravitsya-s-ddos-atakoj/). 16.08.2019).***

***

«Оригинальную фишинговую компанию зафиксировали ИБ-специалисты компании Avanan. Киберпреступники рассылают электронные письма, замаскированные под сообщения голосовой почты Office 365, и перенаправляют жертву на скомпрометированный сайт при помощи механизма, получившего название MetaMorph Obfuscation (обфускация MetaMorph). Алгоритм не вызывает подозрения у защитных систем, поскольку вредоносная ссылка скрыта в метатеге документа.

Как пояснили исследователи, обычно злоумышленники размещают адрес страницы в специализированных HTML-тегах, таких как <a href> или <script> — документы с подобными вложениями легко детектируют встроенные средства безопасности Microsoft Office. В случае с MetaMorph Obfuscation киберпреступники использовали оператор <meta> с параметром http-equiv=»refresh», который позволяет принудительно открыть целевой сайт.

Фишинг через голосовую почту Office 365

Атака начинается с электронного письма, имитирующего уведомление голосовой почты Office 365. Чтобы затруднить выявление опасного контента, большая часть текста в теле сообщения располагается в изображениях, а получателю предлагают открыть приложенный к письму HTML-файл, чтобы прослушать послание. Вредоносный документ запускается в браузере и переадресует жертву на принадлежащий мошенникам ресурс.

Сайт, копирующий оформление страницы авторизации Office 365, предлагает посетителю ввести логин и пароль своей учетной записи. Полученные данные скрипт диалоговой формы пересылает на сервер злоумышленников, расположенный в Пакистане. Его IP-адрес жестко зашит в коде веб-страницы, что необычно для подобных ресурсов – обычно киберпреступники скрывают местоположение центра управления.

Готовые шаблоны страниц, имитирующих службы авторизации Office 365, Amazon, Google и других известных сайтов в комплекте с платформами для их размещения предлагают арендные сервисы. За ежемесячную плату киберпреступники обещают заказчикам размещение фишинговых ресурсов, а

также гарантируют их работоспособность и оперативную замену в случае блокировки. Стоимость такой услуги в дарквебе варьируется от 30 до 80 долларов.» ***(Egor Nashilov. Мошенники прячут фишинговые ссылки в метатегах // Threatpost (https://threatpost.ru/phishing-via-html-meta-tags-with-fake-voicemail-notifications/33815/). 18.08.2019).***

***

«Эксперты обнаружили тщательно спланированную фишинговую атаку против неназванной энергетической компании. Преступники воспользовались легитимной функцией Google Drive, что обойти защитные системы и заманить сотрудников на вредоносную страницу…

Конечной целью кампании были учетные данные корпоративных пользователей. Злоумышленники разместили на облачном сервисе Google сообщение якобы от главы атакуемой организации. В тексте говорилось о некоем бизнес-проекте, к обсуждению которого приглашались сотрудники. За подробностями их направляли на следующую страницу, где и размещалась фишинговая форма.

Преступники отправили ссылку на файл через функцию «Поделиться». Этот легитимный механизм не вызывает вопросов у почтовых фильтров, а системы антифишинга не могут проверить контент, на который ведут такие уведомления. В результате организаторы кампании легко достучались до жертв…

Исследователи отмечают, что такие угрозы все же можно купировать автоматическими средствами. Продвинутые антифишинговые системы проверяют сайт, на который хочет перейти пользователь, и если домен зарегистрирован недавно, блокируют страницу.

Кроме того, внимательные пользователи могли сами заподозрить неладное. Хотя преступники постарались оформить фишинговое письмо в стиле целевой организации, корпоративный логотип и другие элементы оказались прошлогодними. Обратный адрес ложного гендиректора также не соответствовал принятым в компании правилам.

Не уточняя, удалось ли преступникам в итоге добиться своей цели, эксперты заключают, что такие атаки показывают важность обучения пользователей основам ИБ. Исследования показали, что такие курсы повышают компетенции сотрудников, причем эти знания не пропадают и через год. Впрочем, работники энергетических предприятий демонстрируют худшие способности к усвоению, чем пользователи из других отраслей…» ***(Egor Nashilov. Базовая функция Google Drive упростила целевой фишинг // Threatpost (https://threatpost.ru/google-drive-spear-phishing-fools-ms-spam-filters/33810/). 17.08.2019).***

***

«Американский штат Техас столкнулся с беспрецедентным всплеском кибератак с использованием вымогательского ПО. Первые из них были зафиксированы утром 16 августа, а к настоящему моменту нападениями поражены 23 государственных учреждения штата. Их компьютерные системы заблокированы

зловредами-шифровальщиками, злоумышленники требуют выкуп за возвращение доступа к файлам.

В заявлении, распространенном Управлением информационных ресурсов штата Техас, не приводятся какие-либо подробности атак и не уточняются суммы выкупа. Сказано лишь, что пораженными в большинстве случаев оказались компьютерные системы муниципалитетов «небольших населенных пунктов». Также сообщается, что атаки носят скоординированный характер и, вероятнее всего, организованы одним человеком либо группой лиц. Для расследования инцидентов и предотвращения новых атак привлечены силы Министерства внутренней безопасности и ФБР США. Ранее сообщалось, что что на Конференции мэров городов США в июле нынешнего года была принята резолюция, согласно которой муниципалитеты отказываются от переговоров с хакерами и не будут платить им выкуп. Однако этот документ не имеет обязывающей юридической силы.» ***(Кибервымогатели покоряют Техас // ООО «Технический центр Интернет» (https://tcinet.ru/press-centre/technology-news/6662/). 19.08.2019).***

***

«Компьютерное пиратство больно бьет не только по разработчикам легитимного программного обеспечения, но и по создателям зловредов. Об этом на конференции по кибербезопасности Bsides, прошедшей в Лас-Вегасе, рассказала Уайнона де Сомбре - аналитик компании Recorded Future. Для подготовки своего выступления она с мая 2018 по май 2019 года пристально отслеживала публикации в форумах и чатах, аудиторию которых составляют разработчики вредоносного ПО. По словам Де Сомбре, зловреды, получившие признание среди киберпреступников, обычно повторяют судьбу легитимных программ: их взламывают и наводняют рынок их копиями, которые продаются существенно дешевле, чем оригинальный продукт, либо вообще распространяются бесплатно.

Хорошим примером может служить история троянца AZORult, зловреда для Windows, способного похищать с инфицированных компьютеров сохраненные пароли, файлы cookie, историю браузеров и другие конфиденциальные данные. Зловред продавался на киберкриминальных черных рынках самим разработчиком и всего за несколько месяцев обрел большую популярность у хакеров. Вскоре после этого произошла утечка некоторых частей исходного кода AZORult и форумы наводнили взломанные версии троянца. Разработчик попытался защитить свое детище: он выпустил обновленную версию ПО, добавив ряд важных функций и ускорив процесс похищения данных. Но почти тут же и эта версия оказалась взломана пиратами.

Таким образом, пиратство, как ни парадоксально это прозвучит, служит иногда и добрую службу: профессиональные и квалифицированные вирусописатели не видят смысла тратить время и силы на разработку и поддержку своих вредоносных программ и покидают черные рынки – именно это и произошло с разработчиком AZORult.» ***(Создатели вредоносного ПО страдают от пиратов // ООО «Технический центр Интернет» (https://tcinet.ru/press-centre/technology-news/6649/). 07.08.2019).***

***

«Индекс угроз Fortinet Threat Landscape Index обновляет свой исторический максимум, свидетельствуя о продолжении роста числа кибератак. Стараясь избежать обнаружения, злоумышленники становятся все более изощренными в своих методах запутывания и противодействия анализу.

Fortinet объявила результаты своего очередного ежеквартального исследования глобальных угроз Global Threat Landscape Report.

Исследование показывает, что киберпреступники продолжают искать новые возможности для осуществления атак по всей поверхности цифровых структур используют тактики обхода, а также методы противодействия анализу, которые делают их атаки еще более изощренными

Индекс угроз Threat Landscape Index в этом квартале обновил свой исторический максимум и увеличился почти на 4% от изначального значения по сравнению с прошлым годом. Высокий балл за этот промежуток стал пиковым значением и был зафиксирован на момент закрытия второго квартала 2019 года. Увеличение этого показателя обусловлено ростом активности вредоносных программ и эксплойтов

С более подробным разбором индекса Threat Landscape Index и его подиндексом, а также анализом эксплойтов, вредоносного кода и ботнета и другими важными выводами для руководителей по информационной безопасности можно ознакомиться в нашем блоге. Ниже приведены основные выводы из отчета.

Фил Квэйд (Phil Quade), директор по информационной безопасности в Fortinet:

«Постоянно расширяющееся разнообразие и изощренность методов атак, которые используют сегодня злоумышленники, напоминают нам о том, что киберпреступники всегда стараются использовать скорость и улучшающиеся возможности подключения в своих интересах. Поэтому при организации защиты важно следовать тем же принципам и постоянно расставлять приоритеты в этих важных аспектах кибербезопасности – таким образом организация сможет эффективнее управлять киберугрозами и минимизировать киберриски. Но чтобы работа по этим ключевым аспектам безопасности приносила свои плоды, организациям важно использовать в отношении каждого элемента своей инфраструктуры безопасности комплексный платформенный подход, который включает в себя сегментацию и интеграцию, действенный анализ угроз и автоматизацию в сочетании с машинным обучением»…

Многие современные вредоносные инструменты уже включают в себя функции для обхода антивирусов или уклонения от других инструментов для обнаружения угроз, при этом, стараясь избежать обнаружения, злоумышленники становятся все более изощренными в своих методах запутывания и противодействия анализу.

Например, недавняя спам-кампания показывает, как злоумышленники используют и модернизируют эти методы противодействия защите. Кампания включает в себя создание фишинговых писем с вложениями, которые по сути являются зараженными Excel документами с вредоносным макросом. Этот макрос

способен отключать инструменты безопасности и выполнять произвольные команды, вызывая проблемы с памятью, при этом макрос работает только на компьютерах японских пользователей. Кроме того, одним из свойств, которые в частности использует этот макрос, является незадокументированное свойство xlDate.

Другой пример включает в себя вариант банковского троянского вируса Dridex, который изменяет имена и хэши файлов при каждом входе жертвы в систему, что затрудняет обнаружение вредоносного ПО на зараженных хост-системах.

Растущая популярность методов противодействия анализу и все новые тактики обхода служат напоминанием о необходимости многоуровневого подхода к защите и об актуальности средств обнаружения, основанных на анализе поведения…

Вредоносная программа Zegost, созданная для хищения данных, стала ключевым элементом целенаправленной фишинговоой кампании с применением не совсем обычных методов. Как и у других программ, похищающих данные пользователей, основная цель Zegost заключается в сборе информации об устройстве жертвы и доставке этой информации злоумышленнику. При этом в отличие от других подобных программ, Zegost сконфигурирован таким образом, чтобы оставаться незамеченным. Например, Zegost использует функции для очистки журналов событий. Такие возможности доо сих пор не наблюдались в обычных вредоносных программах. Еще одной любопытной особенностью в Zegost стали его способности обхода защиты, и, в частности, команда, позволяющая этой вредоносной программе оставаться в состоянии покоя до 14 февраля 2014 года, после чего запускался основной вредоносный код.

Злоумышленники, создавшие Zegost, используют весь арсенал эксплойтов, чтобы устанавливать и поддерживать соединение с системами жертв, что делает эту угрозу намного более долгосрочной по сравнению с другими угрозами, представленными сегодня.

Программы-вымогатели все активнее используются для более таргетированных атак

Атаки, нацеленные сразу на несколько городов, на местные органы власти и образовательные учреждения служат напоминанием о том, что программы-вымогатели никуда не уходят и по-прежнему продолжают представлять серьезную угрозу для многих организаций. Атаки с использованием программ-вымогателей продолжают меняться и теперь уже не носят тот массовый, приспособленческий характер, но все чаще нацелены на конкретные организации, которые по, мнению злоумышленников, в состоянии заплатить выкуп, или для которых выкуп станет более удобным и эффективным решением проблемы. В некоторых случаях киберпреступники провели значительную работу по зондированию почвы, и только затем начали разворачивать свои программы-вымогатели на тщательно отобранных системах, чтобы максимально использовать возможности.

Например, программа-вымогатель RobbinHood предназначена для атаки на сетевую инфраструктуру организации и способна отключать сервисы Windows, предотвращающие шифрование данных, а также отключать сетевые ресурсы.

Еще одна более свежая программа-вымогатель под названием Sodinokibi способна стать новой угрозой для организаций. Функционально она не очень отличается от большинства инструментов вымогателей. Основная ее изюминка заключается в векторе атаки, который использует более новую уязвимость, которая допускает выполнение произвольного кода и не требует какого-либо взаимодействия с пользователем, как другие вымогатели, доставляемые вместе с фишинговой электронной почтой.

Независимо от вектора атаки, программы-вымогатели по-прежнему представляют серьезную угрозу для организаций, выступая напоминанием о необходимости установки обновлений безопасности и повышения осведомленности пользователей. Кроме того, уязвимости протокола удаленного рабочего стола (RDP), такие как BlueKeep, являются предупреждением о том, что службы удаленного доступа могут открывать новые возможности для киберпреступников и могут также использоваться в качестве вектора атаки для распространения программ-вымогателей…

Между домашними принтерами и критически важной инфраструктурой сегодня также появляется растущая линейка систем управления для дома и малого бизнеса. Эти интеллектуальные системы привлекают сравнительно меньше внимания со стороны злоумышленников, чем их промышленные аналоги, но и это может измениться с учетом возросшей хакерской активности, наблюдаемой в отношении таких устройств, как системы управления окружающей средой, камеры видеонаблюдения и системы безопасности. Было обнаружено, что уязвимость, связанная с решениями для управления зданием, сработала в 1% организаций, что может показаться незначительным, но этот показатель выше, чем обычно для продуктов ICS или SCADA.

Киберпреступники ищут новые возможности для захвата управления устройствами контроля в домах и на предприятиях. Иногда эти типы устройств не являются такими приоритетными, как другие, или выходят за рамки традиционного управления ИТ. Безопасность интеллектуальных жилых систем и систем малого бизнеса заслуживает повышенного внимания, особенно потому, что доступ злоумышленника к таким системам может иметь серьезные последствия для безопасности. Это особенно актуально для удаленных рабочих сред, где важен безопасный доступ…

Динамический, упреждающий и осуществляемый в режиме реального времени анализ угроз позволяет выявлять тенденции, в частности, меняющийся характер методов атак, ориентированных на поверхность цифровой структуры а также позволяет расставлять приоритеты в отношении кибергигиены. Ценность анализа угроз и способность принимать меры на основании этих данных значительно снижаются, если их нельзя реализовать в режиме реального времени на каждом устройстве безопасности. Только комплексный, интегрированный и автоматизированный подход к безопасности может обеспечить защиту всего сетевого окружения, от IoT до периферии, ядра сети и мультиоблачной инфраструктуры, с сохранением высокой скорости и масштабности…

В квартальном отчете о глобальном исследовании угроз Fortinet представлены данные, собранные отделом FortiGuard Labs, с помощью обширной

сети датчиков во 2-м квартале 2019 года. Сбор данных осуществлялся в глобальном и региональном масштабах. В отчет также включен индекс угроз Fortinet Threat Landscape Index (TLI), состоящий из индивидуальных индексов для трех основных и дополнительных аспектов кибер-безопасности – эксплойтов, вредоносного кода и бот-сетей, которые позволяют судить об их распространенности и объеме в текущем квартале.» ***(Киберпреступники повышают ставку на тактики обхода и противодействие анализу с целью избежания обнаружения // IKSMEDIA.RU (http://www.iksmedia.ru/news/5603170-Kiberzloumyshlenniki-povyshayut-sta.html). 07.08.2019).***

***

«Эксперты сообщили о направленной кибератаке на три американские компании в сфере ЖКХ. Злоумышленники, которые предположительно входят в спонсируемую неким государством группировку, пытались установить неизвестный ранее RAT-троян.

По данным специалистов, вредоносные сообщения рассылали с 19 по 25 июля — операторы кампании замаскировали их под письмо от одной из регулирующих организаций. В тексте адресату сообщали о провале сертификации и отправляли за подробностями в приложенный файл Word. Встроенные в документ макросы загружали и устанавливали RAT-троян, который получил название LookBack…

Возможности написанного на C++ зловреда включают чтение системной информации, создание снимков экрана и выполнение команд, передвижение мыши, перезагрузку компьютера. Создатели трояна снабдили его несколькими модулями:

Средства коммуникации с удаленным сервером — прокси-утилита GUP и коммуникационный компонент SodomNormal, который передает ей на отправку данные от RAT. Прокси-утилита в свою очередь пересылает информацию злоумышленникам по HTTP-соединению.

Загрузчик на основе легитимной библиотеки libcurl.dll, в которую добавлена функция работы с командами оболочки.

Основной компонент SodomMain, обеспечивающий удаленный контроль над компьютером.

Как рассказали аналитики, преступники постарались замаскировать свое присутствие на компьютерах жертвы. Название процесса GUP совпадает с одной из программ, с которой работает Notepad++. Этой же цели служит вышеупомянутая libcurl.dll — преступники превращают ее в средство доставки RAT, добавляя одну новую функцию…

Аналитики связали инциденты с группировкой APT10, которая в 2018 году провела похожие атаки на нескольких японских бизнесменов. Такой вывод эксперты сделали на основе использованных Word-макросов, в которых используется та же техника маскировки, что и в прошлогодних случаях.

Еще одно свидетельство в пользу этой версии — прокси-механизм LookBack, который напомнил исследователям инструменты APT10. Тем не менее, поскольку ни сам троян, ни использованная инфраструктура ранее не были замечены в кибератаках, от однозначных выводов специалисты воздержались.

«Хотя окончательная атрибуция потребует дальнейшей работы, угроза подобных кампаний для сферы ЖКХ несомненна, — указали эксперты. — Судя по фишинговым посланиям, злоумышленники хорошо знакомы с устройством этой отрасли, что позволило им составить убедительные письма. Такие кампании угрожают всем, кто пользуется услугами атакованных организаций, поэтому и влияние их следует оценивать шире, чем [в случае единичных инцидентов в рамках отдельных инфраструктур]»…» ***(Egor Nashilov. Коммунальные службы США попали под прицельную кибератаку // Threatpost (https://threatpost.ru/lookback-in-anger-at-us-utility-services/33702/). 07.08.2019).***

***

«Банковские вредоносные программы превратились в очень распространенную угрозу. По сравнению с 2018 годом их число выросло на 50%.

Компания Check Point Software Technologies выпустила отчет Cyber Attack Trends: 2019 Mid-Year Report. Хакеры продолжают разрабатывать новые наборы инструментов и методы, нацеленные на корпоративные данные, которые хранятся в облачной инфраструктуре; личные мобильные устройства; различные приложения и даже популярные почтовые платформы. Исследователи отмечают, что сейчас ни один из секторов полностью не защищен от кибератак.

Эксперты Check Point выявили ключевые тренды киберугроз в первом полугодии 2019:

Мобильный банкинг: количество атак возросло вдвое по сравнению с 2018 годом. Сегодня банковские вредоносные программы — очень распространенная мобильная угроза. Банковское вредоносное ПО способно похитить платежные и учетные данные, средства с банковских счетов жертв. Новые версии банковских вредоносных программ готовы к массовому распространению для всех, кто готов за них заплатить.

Атака на цепь поставок: киберпреступники могут расширить свое влияние, использовав атаку на цепочку поставок компании. При таком типе кибератаки хакеры внедряют вредоносный код непосредственно в программное обеспечение компании-жертвы. После выполнения этого вредоносного кода преступники могут получить доступ к приватной информации компании.

Электронная почта: злоумышленники используют различные методы для обхода решений безопасности и спам-фильтров. Например, они рассылают сложные закодированные электронные письма, а также сложный базовый код, который смешивает обычные текстовые буквы с символами HTML. Кроме того, злоумышленники применяют методы социальной инженерии, а также изменение и персонализацию содержимого электронных писем.

Облачные хранилища: растущая популярность общедоступных облачных сред привела к увеличению числа кибератак, нацеленных на огромные объемы конфиденциальных данных, находящихся на этих платформах. Самые серьезные угрозы для безопасности облаков в 2019 году: неправильная конфигурация и плохое управление облачными ресурсами…

Самое активное вредоносное ПО в первом полугодии 2019 года

Emotet (29%) — продвинутый, самораспространяющийся модульный троян. Emotet когда-то использовался в качестве банковского трояна, а в последнее время используется в качестве доставки других вредоносных программ или вредоносных кампаний. Он использует несколько методов, чтобы избежать обнаружения. Также распространяется через фишинговые спам-сообщения, содержащие вредоносные вложения или ссылки.

Dorkbot (18%) — червь на основе IRC, предназначенный для удаленного выполнения кода его оператором. Также с его помощью можно загрузить дополнительные вредоносные программы в зараженную систему для кражи конфиденциальной информации.

Trickbot (11%) — Trickbot - это вариант Dyre, появившийся в октябре 2016 года. С момента своего первого появления он был нацелен на банки в основном в Австралии и Великобритании, а в последнее время он начал появляться также в Индии, Сингапуре и Малезии.

Самые активные криптомайнеры в первом полугодии 2019 года

Coinhive (23%) — криптомайнер, предназначенный для добычи криптовалюты Monero без ведома пользователя, когда тот посещает веб-сайты. Coinhive появился только в сентябре 2017 года, но уже поразил 12% организаций по всему миру.

Cryptoloot (22%) — майнер, встраиваемый в сайт с помощью JavaScript кода. Добывает криптовалюты Monero без разрешения пользователя.

XMRig (20%) — Программное обеспечение с открытым исходным кодом, впервые обнаруженное в мае 2017 года. Используется для майнинга криптовалюты Monero.

Самые активные мобильные угрозы первого полугодия 2019 года

Triada (30%) — Модульный бэкдор для Android, который предоставляет привилегии суперпользователя для загруженных вредоносных программ, а также помогает внедрить его в системные процессы. Triada также был замечен за подменой URL-адресов, загружаемых в браузерах.

Lotoor (11%) — программа, использующая уязвимости в операционной системе Android для получения привилегированного root-доступа на взломанных мобильных устройствах.

Hidad (7%) — Модульный бэкдор для Android, который предоставляет права суперпользователя для загруженного вредоносного ПО, а также помогает внедрить его в системные процессы. Он может получить доступ к ключевым деталям безопасности, встроенным в ОС, что позволяет ему получать конфиденциальные данные пользователя.

В России было очень активно вредоносное мобильное ПО, которое назвали «Агент Смит». Под видом скрытого приложения, связанного с Google, вредоносная программа использует известные уязвимости Android и автоматически заменяет установленные приложения вредоносными версиями незаметно для пользователя. Пользователи загружали приложение из популярного неофициального магазина приложений 9Apps. Агент Смит заразил в России около 57 тысяч устройств.

Топ вредоносного ПО для банков в первом полугодии 2019 г.

Ramnit (28%) — банковский троян, который похищает данные учетных записей клиентов банка, пароли FTP, файлы cookies для сессий и личные данные.

Trickbot (21%) — доминирующий банковский троян, постоянно пополняемый новыми возможностями, функциями и векторами распространения. Это позволяет Trickbot быть гибким и настраиваемым вредоносным ПО, которое может распространяться в рамках многоцелевых кампаний.

Ursnif (10%) —троян, работающий на платформе Windows. Обычно он распространяется через наборы эксплойтов - Angler и Rig. Он может похищать информацию, связанную с платежным программным обеспечением Verifone Point-of-Sale (POS). Для этого троян связывается с удаленным сервером, чтобы загрузить собранную информацию и получить инструкции. После этого он загружает файлы в зараженную систему и выполняет их.

Отчет за первое полугодие 2019 года «Cyber Attack Trends: Annual Report 2019» показывает весь возможный ландшафт киберугроз. Выводы основаны на данных Global Threat Impact Index и ThreatCloud Map, которые были разработаны ThreatCloud intelligence, самой большой совместной сетью по борьбе с киберпреступностью, которая предоставляет данные об угрозах и тенденциях атак из глобальной сети датчиков угроз. База данных ThreatCloud, содержащая более 250 миллионов адресов, проанализированных для обнаружения ботов, более 11 миллионов сигнатур вредоносных программ и более 5,5 миллионов зараженных сайтов, продолжает ежедневно идентифицировать миллионы вредоносных программ.» ***(Никто не защищен от кибератак // IKSMEDIA.RU (http://www.iksmedia.ru/news/5601217-Nikto-ne-zashhishhen-ot-kiberatak.html). 01.08.2019).***

***

«0,1% атак приходятся на технические решения для захвата токенов МФА, но они случаются крайне редко.

В облачных сервисах Microsoft ежедневно совершается около 300 млн попыток мошеннического входа в учетные записи. Многофакторная аутентификация (МФА) может помочь защитить учетные записи от многих типов атак.

По словам специалистов из Microsoft, пользователи, включившие многофакторную аутентификацию для своих учетных записей, в итоге блокируют 99,9% автоматических атак. Рекомендация распространяется не только на учетные записи Microsoft, но и на любой другой профиль, web-сайт или online-сервис. Если поставщик услуг поддерживает многофакторную аутентификацию, Microsoft рекомендует использовать ее, независимо от того, является ли она чем-то простым, как одноразовые SMS-пароли или расширенные биометрические решения.

По словам исследователей из Microsoft, такие старые советы, как «никогда не используйте пароль, который когда-либо был скомпрометирован» или «используйте действительно длинные пароли», в последние годы не очень помогают. В настоящее время киберпреступники имеют в своем распоряжении различные методы, позволяющие получить учетные данные пользователей, и в большинстве случаев пароль и его сложность не имеют значения.

От постоянных попыток мошеннического входа защитит включение многофакторной аутентификации. Она не сможет заблокировать только 0,1% атак, в ходе которых киберпреступники используют технические решения для захвата токенов МФА, но они происходят крайне редко.» ***(Использование многофакторной аутентификации блокирует 99,9% взломов // SecurityLab.ru (https://www.securitylab.ru/news/500636.php). 27.08.2019).***

***

«…После некоторого затишья управляющие серверы ботнета Emotet возобновили свою активность. Исследователи из Cofense Labs первыми обнаружили возрождение инфраструктуры ботнета, а специалисты из Black Lotus опубликовали список активных серверов.

Emotet ранее был известен как банковский троян, но потом изменил курс и превратился в ботсеть, распространяя различные виды вымогательского ПО. Сейчас Emotet является одной из самых опасных в мире угроз. Сеть используется для распространения банковского трояна Trickbot и вымогателей Ryuk. Такая комбинация вредоносов получила название «тройная угроза» и использовалась в рамках атак на государственные администрации в США в июле 2019 года.

По словам специалистов, серверы только возобновили свою активность и еще не было зафиксировано попыток распространения вредоносов. Предполагается, что операторам необходимо время на восстановление систем и подготовку новой вредоносной кампании. Серверы расположены в самых разных странах, в том числе в Бразилии, Мексике, Германии, Японии и США.

Учитывая интенсивную активность, эксперты ожидают новую вредоносную кампанию в ближайшее время. По их оценкам, злоумышленники будут придерживаться старой схемы распространения вымогательского ПО.» ***(Ботнет Emotet возобновил свою активность // SecurityLab.ru (https://www.securitylab.ru/news/500608.php). 26.08.2019).***

***

«Інтернет-сайти фінських держслужб зазнали кібератаки: певний час були недоступними, зокрема, сайти поліції, податкової служби та прикордонної охорони. Зараз робота цих сайтів частково відновлена…

"Інтернет-сайти держслужб працюють з перебоями через хакерські атаки. Атаки зазнали, зокрема, система ідентифікації Suomi.fi. Перешкоди в мережі почалися вже вчора", - йдеться у повідомленні.

Причина та обставини атаки з'ясовуються. Поки немає інформації про те, як довго перешкоди триватимуть…» ***(Сайти фінських держслужб зазнали кібератаки // Європейська правда (https://www.eurointegration.com.ua/news/2019/08/22/7099973/). 22.08.2019).***

***

«Аферисты, мошенники и вымогатели разных мастей активизировались в интернете. Под ударом оказалась известная украинская компания «Центр Биржевых Технологий». В сети появилась ложная информация, порочащая

репутацию ЦБТ. Развод и вымогательство — такова была цель аферистов с сайтов Forex brokers pro и Chargeback me, которые сфабриковали компромат и планировали шантажировать ЦБТ, оставаясь безнаказанными.

Но реакция не заставила себя ждать. Борьбу против атак на своего давнего клиента начала рекламная компания «Амиллидиус» — эксперт по защите репутации в сети с многолетним успешным опытом. По инициативе «Амиллидиус» 14 августа 2019 года в УНИАН состоялась пресс-конференция «Современные кибератаки на компании. Как защититься и противостоять им в текущих реалиях».

Руководитель «Амиллидиус» Богдан Терзи в своем выступлении обрисовал суть деятельности мошенников и преступную схему, по которой действуют Forex brokers pro и Chargeback me. Масштабы впечатляют — фейковые досье созданы более чем на 700 компаний, где всех без разбора обвиняют в обмане и воровстве. За устранение негатива, а вернее замену негативной статьи на хвалебную компании приходится платить, причем на постоянной основе. Кто-то соглашается, но многие компании не поддавались на шантаж, среди них и Центр Биржевых Технологий. Мошенники должны быть наказаны, — уверены в ЦБТ.

Другой способ, которым аферисты набивают свои карманы — обман недовольных клиентов компаний, стремящихся вернуть свои деньги. Им обещают всяческое содействие и берут предоплату за услуги. После чего переписка прекращается, а свои обязательства мошенники и не думают выполнять.

Почему же вымогателям пока удается уйти от ответа? Во-первых, они серьезно позаботились о конспирации. Но ведь существует киберполиция и спецслужбы. И тут возникает второе препятствие — несовершенство украинского законодательства, как подчеркнул на пресс-конференции Максим Рудик, управляющий партнер компании Центр Биржевых Технологий. Развод, клевета и вымогательство процветают из-за отсутствия у правоохранительных органов необходимых инструментов и полномочий для поимки и наказания мошенников. А бизнес на финансовых рынках — самый высокодоходный в мире — притягивает их как магнит…» ***(ЦБТ: развод, запланированный Forex brokers pro, обречен на неудачу! // ESGROUP (https://ubr.ua/ukraine-and-world/events/tsbt-razvod-zaplanirovannyj-forex-brokers-pro-obrechen-na-neudachu-3885816). 19.08.2019).***

***

Діяльність хакерів та хакерські угруповування

«Корпорація Microsoft оголосила про атаки російських хакерів - за словами її IT-експертів, зловмисники використовують для проникнення в мережі принтери і VoIP-телефони. Про це компанія повідомила на конференції з безпеки в сфері високих технологій в Лас-Вегасі… [6 серпня]…

Виявлені експертами зломи корпоративних мереж змогли бути здійснені, тому що використовували для роботи з приладами не змінені стандартні паролі, а на одному не було встановлено останнє оновлення, попереджає Microsoft.

Фахівці Microsoft вважають, що до атак причетна група кіберзлочинців, відома як Strontium (інші назви - Fancy Bear, APT28 і Sofacy). Раніше її пов'язували

з Головним управлінням (ГУ) Генштабу збройних сил Росії…» ***(Ілля Нежигай. Microsoft повідомила про атаки хакерів з РФ через принтери // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1817551-microsoft-povidomila-pro-ataki-khakeriv-z-rf-cherez-printeri). 07.08.2019).***

***

«…В прошлом месяце хакерский форум Cracked.to стал жертвой взлома, организованного сайтом-конкурентом. По данным сервиса Have I Been Pwned, в результате кибератаки были скомпрометированы учетные записи 321 тыс. участников форума.

В Сеть утекла база данных, содержащая 749 161 электронный адрес с соответствующими IP-адресами (большинство из них анонимизированы), хеши паролей, личные сообщения и имена пользователей. База данных была сформирована с помощью ПО MyBB.

Как сообщает издание Ars Technica, взлом был осуществлен участниками хакерского форума Raidforums. Специалисты проанализировали утекший файл размером 2,11 ГБ и обнаружили в нем 397 тыс. незашифрованных личных сообщений, в которых обсуждались взломы учетных записей Fortnite, продажа эксплоитов и другая информация, которую киберпреступники желали бы сохранить в тайне.

Создатель Raidforums сообщил, что взломать сайт конкурента удалось через уязвимость, но подробностей атаки не представил…» ***(В Сеть утекли данные участников хакерского форума Cracked.to // SecurityLab.ru (https://www.securitylab.ru/news/500484.php). 16.08.2019).***

***

«…Недавно обнаруженная киберпреступная группировка из Нигерии под названием Curious Orca перед осуществлением BEC-атаки вручную проверяет подлинность электронных адресов своих жертв.

BEC-атаки (Business Email Compromise) представляют собой мошенническую схему, при которой злоумышленники просят сотрудника компании перевести деньги на подконтрольный им банковский счет, отправив просьбу в электронном письме якобы от имени директора компании или доверенного партнера.

На первом этапе атаки Curious Orca составляет список сотрудников, которых можно атаковать, и проверяет подлинность собранных данных. Как сообщают специалисты Agari Cyber Intelligence Division (ACID), злоумышленники скрупулезно ищут и проверяют данные сотрудников, которых намерены атаковать, а также ищут в открытых источниках сведения о лице, за которое намерены себя выдавать (например, сведения о главе компании).

Большинство мошенников, специализирующихся на BEC-атаках, используют для лидогенерации специальные сервисы, предоставляющие им большую часть, если не всю, информацию, необходимую для осуществления атаки.

«Когда мошенники находят через поиск корпоративных сотрудников, отвечающих нужным критериям, сервис предоставит электронную таблицу с

необходимой информацией и даже укажет, проводила ли их компания ранее проверку адресов электронной почты», - цитирует исследователей издание Bleeping Computer.

Тем не менее, многие мошенники не гнушаются для большей надежности вручную проверять полученные данные. Так, Curious Orca начинает с составления списка сотрудников и их вероятных электронных адресов. Для проверки подлинности электронных адресов мошенники отправляют пустые письма с темой «i» и смотрят, были ли они доставлены.

Лидогенерация – маркетинговая тактика, направленная на поиск потенциальных клиентов с определенными контактными данными.» ***(Мошенники проверяют подлинность данных перед BEC-атаками // SecurityLab.ru (https://www.securitylab.ru/news/500406.php). 13.08.2019).***

***

«…Печально известная APT-группа Fancy Bear (другое название APT28) атакует корпоративные IoT-устройства с целью проникновения в сети компаний и создания плацдарма для дальнейших атак.

«В апреле исследователи безопасности Microsoft Threat Intelligence Center обнаружили, что инфраструктура известного противника подключается к нескольким внешним устройствам. В ходе дальнейших исследований были выявлены попытки злоумышленников скомпрометировать популярные IoT-устройства (телефон VOIP, офисный принтер, видеодекодер)», - сообщают специалисты компании Microsoft.

В двух случаях злоумышленники использовали заводские пароли по умолчанию, а еще в одном проэксплуатировали уязвимость в устройстве, на котором не были установлены последние обновления. Через скомпрометированное IoT-устройство атакующие могли проникнуть в корпоративную сеть и взломать подключенные к ней уязвимые компьютеры. С помощью несложного сканирования они могли продвигаться по сети и получать доступ к привилегированным учетным записям.

Используя анализатор пакетов tcpdump, атакующие анализировали трафик в локальной сети в поисках дополнительных данных о следующих жертвах и административных группах. На каждое скомпрометированное устройство группировка устанавливала shell-скрипт, непрерывно передающий на C&C-сервер поток информации, позволяющей ей сохранять свое присутствие в корпоративной сети.

Хотя специализацией Fancy Bear является кибершпионаж, специалисты Microsoft затрудняются сказать, какие цели преследовала группировка в данной конкретной кампании. Атаки были обнаружены на ранних стадиях, и установить их цель пока нельзя.» ***(Fancy Bear атакует популярные IoT-устройства // SecurityLab.ru (https://www.securitylab.ru/news/500302.php). 06.08.2019).***

***

«…Исследователи безопасности из компании Dragos идентифицировали новую киберпреступную группировку, получившую название Hexane,

нацеленную на системы промышленного контроля на предприятиях в нефтегазовом и телекоммуникационном секторах.

По словам специалистов, злоумышленники начали свою преступную деятельность в середине 2018 года, и используют вредоносные документы для проникновения в сеть. В первой половине 2019 года группировка сконцентрировала атаки на нефтяных и газовых компаниях на Ближнем Востоке, в основном в Кувейте. Преступники также совершили попытки атак на телекомпровайдеров в странах Ближнего Востока, Центральной Азии и Африки.

По словам специалистов, преступники обходят защиту объектов через доверенных поставщиков, компрометируя устройства, программное обеспечение и телекоммуникационные сети, используемые целевыми объектами в рамках АСУ ТП.

Преступная деятельность Hexan демонстрирует сходство с атаками группировок Magnallium (APT33) и Chrysene, поскольку все они нацелены на нефтегазовые объекты и используют подобные методы. Chrysene сосредоточена на компаниях и организациях в Северной Америке, Европе, Израиле и Ираке, и использует сложное вредоносное ПО не только для атак, но и для шпионажа. В июне нынешнего года хакерская группировка Xenotime расширила свой список целей, включив в него энергетические предприятия в США и странах Азиатско-Тихоокеанского региона. В прошлом году команда специалистов из Dragos включила вышеуказанные группы в список группировок, представляющих наибольшую опасность для АСУ ТП.» ***(Новая кибергруппировка Hexane атакует промышленные предприятия на Ближнем Востоке // SecurityLab.ru (https://www.securitylab.ru/news/500251.php). 01.08.2019).***

***

«В Китае жертвами хакерских атак группы APT41 стали предприятия в сферах здравоохранения, телекоммуникаций, финтеха, медиа, а также криптовалютные биржи. Об этом сообщили аналитики специализирующейся на кибербезопасности компании FireEye.

По их словам, преступную деятельность финансирует китайское правительство.

Эксперты считают, что жертвами APT41 становятся участники индустрий, развитие которых является приоритетом в текущей китайской пятилетке.

Одновременно с этим, APT41 преследует и собственные цели, извлекая финансовую выгоду из атак, что несвойственно другим группам при китайском правительстве, подчеркнули в FireEye.

Известно, что в APT41 входят как минимум два человека по псевдонимами Чзан Сюйгуан и Вольфжи. Вероятно, у группы есть связи с другими хакерскими организациями вроде BARIUM и Winnti.

В FireEye также оценили, в какое время дня APT41 атаковала игровую индустрию (свою профильную цель) и предприятия из других сфер. Оказалось, что это происходило за рамками стандартного рабочего дня — вероятно, эти люди помимо прочего имеют основную работу.» ***(В Китае «правительственные»***

хакеры атакуют криптобиржи // LetKnow OÜ (https://letknow.news/news/v-kitae-pravitelstvennye-hakery-atakuyut-kriptobirzhi-27813.html). 08.08.2019).

***

«Хакеры совершили атаку на образовательную сеть финского города Пори…

Отмечается, что информационный взлом был замечен в образовательной сети.

В сервере городской сети образования была установлена вредоносная программа, через которую злоумышленники попытались собрать данные. Это, возможно, поставило под угрозу защиту личной информации пользователей – электронную почту и пароли.

В качестве меры предосторожности пароли всех пользователей были изменены…» ***(Хакеры атаковали город в Финляндии // Единый информационный портал (http://ua-ru.info/news/142511-hakery-atakovali-gorod-v-finlyandii.html). 09.08.2019).***

***

«Интернет-биржа одежды и обуви StockX сообщила о взломе своих баз данных, который привел к компрометации 6,8 млн записей с персональной информацией пользователей. По данным экспертов, похищенные сведения уже можно купить на подпольных площадках.

Компания не уточняет детали инцидента, однако впервые о проблемах стало известно 1 августа. В этот день клиенты StockX получили уведомления с просьбой сменить пароль якобы из-за «обновления систем безопасности»…

Такая постановка вопроса обеспокоила как пользователей, так и ИБ-экспертов. Первые заподозрили, что их пытаются обмануть фишеры, вторые заметили, что внедрение защитных систем не требует смены паролей. Со своей стороны, представители StockX лишь подтвердили легитимность рассылки и призвали следовать инструкциям.

Только 3 августа в компании заявили, что настоящая причина требования — «подозрительная активность, потенциально связанная с пользовательскими данными».

«Мы немедленно провели тщательное расследование с привлечением сторонних экспертов, — говорится в сообщении StockX. — Собранные улики позволяют предположить, что неизвестные взломщики получили доступ к определенной информации наших клиентов, включая имена, электронные адреса и точки доставки, логины, хешированные пароли и историю покупок. По имеющимся у нас данным, финансовую и платежную информацию инцидент не затронул».

Из сообщения также следует, что в дополнение к обновлению паролей специалисты компании внедрили «высокочастотную ротацию учетных данных на всех серверах и устройствах», а также закрыли свой облачный периметр. Представители StockX отказались раскрывать другие подробности, сославшись на продолжающееся расследование…

По данным онлайн-изданий, украденная информация уже попала на подпольные торговые площадки — неизвестный продавец предлагает ее за $300.

Злоумышленник уточнил, что взлом произошел еще в мае и коснулся 6,7 млн пользователей. В подкрепление своих слов преступник отправил журналистам 1000 записей из похищенной базы, которые оказались достоверными.

Как уточняют специалисты, взломщики получили больше информации, чем говорилось в заявлении StockX. Помимо прочего, похищенные данные включают модели клиентских устройств и версии установленных ОС, размеры обуви и валюту для расчетов.

Эксперты полагают, что сложившаяся ситуация грозит StockX крупными штрафами — в частности, до 4% годовой прибыли в соответствии с требованиями GDPR. Этот закон устанавливает, что компании обязаны сами сообщать об инцидентах с персональными данными, в то время как представители StockX в своих заявлениях ссылались на обновление систем безопасности. Последующие вопросы СМИ они проигнорировали.

Как ранее выяснили аналитики, в настоящее время под угрозой взлома находятся более 500 тыс. интернет-магазинов. В зоне особого риска площадки под управлением CMS Magento — в этой категории проверку безопасности провалили почти 90% сайтов. Атаки на такие магазины могут разом охватывать сотни и тысячи ресурсов, приводя к компрометации пользовательских данных.» ***(Egor Nashilov. Преступники украли данные миллионов клиентов StockX // Threatpost (https://threatpost.ru/stockx-got-hacked/33711/). 07.08.2019).***

***

«Компания ESET изучила атаки киберпреступной группировки Machete на госструктуры Латинской Америки. Основная цель хакеров — кибершпионаж, при этом особое внимание уделяется поиску данных о дислокации военных объектов.

Весной 2019 года эксперты ESET зафиксировали более 50 зараженных компьютеров, которые регулярно связывались с C&C-сервером злоумышленников. Большинство атакованных компьютеров принадлежат вооруженным силам Венесуэлы. Под удар попали и другие госучреждения, включая полицейские и образовательные структуры.

Эксперты ESET изучили новую версию набора вредоносных инструментов Machete. Злоумышленники регулярно модифицируют свое ПО и вносят изменения в механизмы распространения.

Способ заражения выглядит следующим образом: потенциальная жертва получает письмо со ссылкой или вложенным документом. При этом рассылка вредоносных сообщений носит точечный характер — письма получает ограниченное число лиц.

В качестве приманки выступают документы, хорошо известные в армейских кругах — например, радиограммы. Злоумышленники также используют профессиональный сленг, что заставляет получателей фишингового письма поверить в обман.

Атака начинается с запуска самораспаковывающегося файла и установки бэкдор-компонентов. Один из них представляет собой шпионский модуль, который копирует и шифрует документы, делает скриншоты экрана, определяет геолокацию, скачивает историю браузера и перехватывает введенный с клавиатуры текст.

Каждые десять минут украденные данные передаются на C&C-сервер.

«Операторы Machete используют эффективные методы фишинг-атаки. За время киберкампаний, нацеленных на латиноамериканские страны, они собрали достаточно информации и усовершенствовали свою тактику, чтобы успешно замаскировать фишинговые письма под рабочие коммуникации», — говорит исследователь ESET Матиас Порольли.

Киберпреступники из группировки Machete ведут деятельность как минимум с 2010 года. В ходе изучения набора инструментов для кибершпионажа эксперты ESET пришли к выводу, что группировка является испаноговорящей: исходные коды содержат ряд терминов на испанском языке.» ***(Раскрыты детали атаки на военные ведомства Венесуэлы // IKSMEDIA.RU (http://www.iksmedia.ru/news/5601597-Raskryty-detali-ataki-na-voennye.html). 05.08.2019).***

***

«Представитель посольства России в Лондоне сообщил об атаке хакеров на сайт дипмиссии в понедельник.

…DDoS атака была зафиксирована в 16:30 (18:30 мск), в результате чего работа была нарушена. Ресурс начал функционировать в нормальном режиме только к 12:00 (14:00 мск) вторника. По факту кибератаки проводится расследование.

Посольство принесло посетителям сайта извинения и выразило сожаление в связи с возможными неудобствами.» ***(Сайт посольства РФ в Британии подвергся атаке хакеров // Новости Великобритании на русском языке (https://theuk.one/sajt-posolstva-rf-v-britanii-podvergsya-atake-xakerov/). 21.08.2019).***

***

Вірусне та інше шкідливе програмне забезпечення

«Trend Micro, международная компания в области кибербезопасности, обнаружили 85 мошеннических приложений в Google Play, замаскированные под приложения для редактирования фотографий и игры. Данные приложения содержали рекламу, которая рассказывала про схемы зарабатывания денег. Согласно данным, зараженные приложения уже установили более 8 млн раз. Обнаруженные приложения были удалены из онлайн-магазина Google Play. Эксперты в области кибербезопасности отметили, что это была редкая группа рекламных программ. Во-первых, отображение рекламы трудно закрыть. Во-вторых, данные программы используют уникальные методы, которые дают возможность избежать обнаружения при помощи поведения пользователя и

временных сигналов. Кроме того, преступники могли дистанционно настраивать частоту показа рекламы на зараженных устройствах.» ***(В Google Play нашли десятки зараженных приложений // PAYSPACE MAGAZINE (https://psm7.com/google-play-market/v-google-play-nashli-desyatki-zarazhennyx-prilozhenij.html). 19.08.2019).***

***

«Разработчики антивирусной программы ESET обнаружили новый вирус Varenyky, который не только ворует пароли от аккаунтов и финансовую информацию, но и умеет записывать компрометирующее видео того, как пользователь смотрит порноролики…

После того, как через веб-камеру записан «компромат» на владельца экрана, он получает это видео на почту вместе с письмом от хакеров, в котором они обещают разослать его всем контактам. Предотвратить подобный позор можно отправив виртуальным вымогателям определенную сумму на электронный кошелек.

Заражение вирусом Varenyky происходит через электронную почту: пользователи получают официальный счет от каких-либо известных компаний, а после открытия файла вирус устанавливается на компьютер…» ***(Екатерина Квитка. Вирус Varenyky: смотреть «взрослые» фильмы стало куда опасней // Hyser Media (https://hyser.com.ua/community/107031-virus-varenyky-smotret-vzroslye-filmy-stalo-kuda-opasney). 17.08.2019).***

***

«Компания Varonis, которая специализируется на вопросах по кибербезопасности, обнаружила новый вирус-майнер под названием Norman. Вредонос скрывает свое присутствие из списка задач операционной системы. В отчете Varonis сообщается, что вирус был случайно обнаружен во время аудита компании, которая подверглась атаке. Ключевая особенность вредоноса-майнера в том, что при открытии диспетчера задач в ОС Windows вредоносное ПО быстро завершает процесс майнинга. Поэтому пользователь не догадывается, что его компьютер подвергся заражению. После того, как человек закрывает диспетчер задач, программа снова начинает майнить криптовалюту. Отмечается, что Norman добывает криптовалюту Monero с помощью популярного майнера XMRig. Вирус написан на языке программирования .NET и был обфусцирован с помощью Agile. Интересно, что вирус также общается с удаленным сервером, используя код на языке PHP. После проведения глубокого анализа вируса специалисты по кибербезопасности пришли к выводу, что страна происхождения вредоноса — Франция или же другая франкоговорящая страна. Это подтверждает множество фраз на французском, найденных в коде…» ***(Обнаружен вирус-майнер, который скрывает свое присутствие в системе // PaySpace Magazine (https://psm7.com/security/obnaruzhen-virus-majner-kotoryj-skryvaet-svoe-prisutstvie-v-sisteme.html). 15.08.2019).***

***

«**Эксперты компании ThreatFabric обнаружили в Интернете новый банковский троян Cerberus, который авторы предлагают в аренду.** Создатели зловреда открыто продвигают его через Twitter и YouTube и утверждают, что разработали его с нуля…

Исследователи отмечают, что Cerberus появился на рынке банкеров для Android очень своевременно. В марте 2019 года на подпольных хакерских площадках появились сообщения об аресте автора Anubis, который с 2017 года был ведущим MaaS-сервисом среди мобильных банковских троянов. После этого исходный код трояна был опубликован в Интернете, однако зловред лишился поддержки, так что у Cerberus есть все шансы занять его место.

По словам экспертов, лидеры этого сегмента подпольного рынка сменяются примерно раз в один-два года…

Функционально новый троян не представляет собой ничего революционного, несмотря на то, что его код действительно оригинальный и не является копией Anubis. Единственная интересная особенность Cerberus состоит в использовании акселерометра Android-устройства для отслеживания перемещений. Таким образом зловред определяет, что он поразил реальную цель, а не оказался в антивирусной песочнице. Троян запускается только после того, как внутренний шагомер убедится, что пройденная пользователем дистанция превышает заданную в коде отметку.

В остальном поведение Cerberus не слишком отличается от прочих банковских зловредов. Он распространяется под видом приложения Flash Player. Оказавшись на устройстве, троян скрывает свою иконку и запрашивает доступ к службе специальных возможностей. Если жертва предоставляет ему это разрешение, Cerberus уже самостоятельно выдает себе права на отправку сообщений и совершение телефонных звонков. Кроме того, он отключает встроенное защитное решение Google Play Protect, чтобы избежать блокировки.

Троян обладает функциями кейлоггинга и создания невидимых окон, которые и позволяют ему перехватывать пользовательские данные. Аналитики нашли в коде список из 30 приложений, для которых Cerberus создает оверлеи. Банковские программы составляют половину этого списка.

Прочие вредоносные возможности включают сбор данных о зараженном устройстве, установку, запуск и удаление приложений. Модульная архитектура Cerberus позволяет операторам добавлять и новые функции…

Специалисты нашли Twitter-аккаунт, посвященный продвижению Cerberus среди потенциальных клиентов. К удивлению экспертов, преступники охотно вступают в переписку даже с представителями ИБ-сообщества, не опасаясь, что те помешают их деятельности. По мнению аналитиков, такое поведение связано с желанием злоумышленников получить скандальную славу или невысоким уровнем их развития.

Помимо Twitter, преступники создали канал на YouTube, где опубликовали видео с инструкцией по работе с Cerberus. Видео охватывают все этапы работы, начиная с заражения устройства и заканчивая удалением зловреда.» ***(Julia Glazova. Банковский троян Cerberus считает шаги пользователей Android // Threatpost***

(https://threatpost.ru/new-android-banker-cerberus-counts-users-steps/33784/). 14.08.2019).

***

«Группировка Cloud Atlas обновила средство доставки бэкдора, с помощью которого она шпионит за высокопоставленными целями в Восточной Европе и Центральной Азии. Благодаря использованию полиморфного вредоносного ПО преступникам удается обходить системы безопасности…

Впервые вредоносные кампании группировки Cloud Atlas, также известной как Inception, зафиксировали эксперты «Лаборатории Касперского» в 2014 году. Ее атаки направлены на государственные, финансовые, религиозные организации, предприятия авиакосмической отрасли.

Аналитики связывают этих преступников с другой известной группировкой — Red October. Об их родстве говорит совпадение некоторых целей и технические особенности кибератак.

На всем протяжении своей деятельности Cloud Atlas использует одну схему. Первоначальное заражение происходит через целевой фишинг, цель которого — убедить жертву открыть вредоносный документ Word. Этот файл в свою очередь доставляет на компьютер бэкдор. Его важная особенность заключается в том, что код полезной нагрузки не пишется напрямую на диск, а выполняется через специально созданный и зашифрованный скрипт Visual Basic.

В октябре 2018 года аналитики обнаружили в атаках группировки имплантат, который они назвали PowerShower. Этот PowerShell-скрипт выполняет роль валидатора и скачивает на зараженную машину несколько модулей полезной нагрузки. В числе таких компонентов:

Средство копирования иотправки на удаленный сервер файлов *.txt, *.pdf, *.xls, *.doc.

Шпионский модуль дляопределения активных процессов на компьютере, имени пользователя и домена Windows.

Похититель паролей набазе утилиты с открытым кодом LaZagn.

Характерные особенности кампаний Cloud Atlas в 2019 году

Начиная с апреля 2019 года участники Cloud Atlas стали применять новый имплантат — написанное на Visual Basic HTML-приложение. Именно оно отвечает за активацию PowerShower и основного бэкдора.

Главная задача обновления — обмануть системы обнаружения вторжений по индикаторам компрометации. Преступники добиваются этой цели благодаря полиморфной природе используемых компонентов — код меняется от атаки к атаке, что приводит и к изменению хешей.

Приложение, которое размещено на удаленном сервере, последовательно доставляет в атакованную систему три файла:

Полиморфный бэкдор VBShower, который выполняет функции валидатора вместо PowerShower.

Лончер бэкдора.

Специально созданный файл сданными о компьютере, получаемыми от

Чтобы скрыть свое присутствие, последний удаляет все файлы в папках %APPDATA%\..\Local\Temporary Internet Files\Content.Word\ и %APPDATA%\..\Local Settings\Temporary Internet Files\Content.Word\. Сделав это и закрепившись на компьютере через системный реестр, он отправляет на удаленный сервер файл с данными о зараженном компьютере и ждет полезную нагрузку.

По словам экспертов Kaspersky, финальной целью злоумышленников остается доставка инсталлятора для PowerShower или все того же бэкдора, который Cloud Atlas использует с начала своей деятельности. Аналитики заключают, что, несмотря на простые методы, преступники все же достигают своих целей…» ***(Egor Nashilov. Группировка Cloud Atlas вооружилась полиморфным бэкдором // Threatpost (https://threatpost.ru/cloud-atlas-gears-up-with-new-vbshower-backdoor/33777/). 13.08.2019).***

***

«…Специалисты компании Cofense обнаружили новую фишинговую операцию, в рамках которой злоумышленники заражают компьютеры на базе Windows инструментом для удаленного администрирования (RAT) Quasar, используя поддельные резюме.

В то время как фальшивые резюме и другие типы документов являются довольно распространенным методом доставки вредоносного ПО, одна из особенностей новой кампании заключается в использовании нескольких методов, усложняющих проведение анализа векторов заражения.

Quasar – известный открытый инструмент, разработанный на языке C#, который ранее неоднократно был замечен в операциях различных хакерских группировок, например, APT33, APT10, Dropping Elephant, Stone Panda или The Gorgon Group. Функционал программы включает возможность удаленного подключения к рабочему столу, записи нажатий на клавиатуре и кражи паролей жертв, загрузки и эксфильтрации файлов, управления процессами на зараженном устройстве, а также возможность съемки скриншотов и записи с web-камер.

В рамках новой фишинговой кампании злоумышленники под видом резюме распространяют защищенные паролем документы Microsoft Word. После ввода пароля «123», указанного в фишинговом сообщении, документ запрашивает активацию макроса. Однако в отличие от других подобных атак в данном случае макрос содержит «мусорный» код, закодированный в base64, призванный вывести из строя аналитические инструменты, установленные на компьютере.

«При успешном запуске макроса на экране отобразится ряд изображений, якобы загружающих контент, но одновременно с этим добавляющих «мусорную» строку в содержимое документа. Далее отобразится сообщение об ошибке, но в то же время в фоновом режиме на компьютер загрузится и запустится вредоносный исполняемый файл», - пояснили эксперты.

Заражение программой Quasar происходит через самораспаковывающийся исполняемый файл размером 401 МБ, загружаемый с подконтрольного злоумышленникам сервера. Большой размер архива усложняет задачу анализа вредоносного ПО, отмечают исследователи.» ***(Киберпреступники начали***

распространять Quasar RAT через фальшивые резюме // SecurityLab.ru (https://www.securitylab.ru/news/500639.php). 27.08.2019).

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«…Киберпреступник, атаковавший такие крупные компании, как Uber, Sainsbury's, Nectar, Groupon, T Mobile, AO.com и Argos, выплатит более $1,1 млн в качестве компенсации жертвам фишинговых атак.

27-летний Грант Уэст (Grant West), известный в Сети как «Courvoisier», начал свою фишинговую кампанию в 2015 году. Он атаковал популярные компании для доступа к финансовым данным десятка тысяч клиентов, которые затем продавал в даркнете за разные криптовалюты. По результатам расследования, Уэста идентифицировали как лидера группировки Organised Crime Network, атаковавшей расположенные в Лондоне организации. Наряду с финансовыми данными он также продавал инструкции по проведению кибератак.

Сотрудники правоохранительных органов в ходе операции под кодовым названием «Operation Draba» конфисковали все средства преступника. Также в доме Уэста была обнаружена SD-карта с 78 млн уникальных имен пользователей и паролей, а также данными 63 тыс. банковских карт. Дальнейшее расследование выявило, что преступник организовывал атаки с ноутбука своей девушки. На устройстве был обнаружен файл с именем «fullz», содержащий финансовую информацию более 100 тыс. пользователей.

Изучив материалы дела, суд постановил продать всю конфискованную цифровую валюту Уэста (на сумму более £922 тыс.) и выплатить пострадавшим компенсацию.» ***(Организатор фишинговых атак выплатит своим жертвам более $1,1 млн // SecurityLab.ru (https://www.securitylab.ru/news/500627.php). 26.08.2019).***

***

Технічні аспекти кібербезпеки

«Android-устройства могут поставляться со встроенным вредоносным ПО и бэкдорами из-за недостаточного контроля и проверки. По словам исследователя Мэдди Стоун (Maddie Stone) из Google Project Zero, злоумышленники пользуются этой возможностью для размещения вредоносного кода прямо на стадии разработки и заражения таким образом цепочки поставок.

Сертифицированные устройства Android, поставляющиеся с предварительно установленными приложениями Google, используют утвержденные образы сборки для мобильной операционной системы. Они проходят тщательное тестирование

перед выпуском потребителям, проверяющее соблюдение модели безопасности и разрешений Android, а также наличие последних обновлений ОС.

Однако большинство поставщиков Android используют более дешевую версию операционной системы Google — AOSP (Android Open-Source Project). Защиту от вредоносных приложений в таком случае обеспечивает встроенный Google Play Protect (GPP). Злоумышленники видят возможность в этой схеме, ведь достаточно убедить одного производителя включить вредоносный код среди предустановленных приложений и заражение способно охватить тысячи пользователей.

В качестве примера Стоун привел ботнет Chamois , использующийся для мошенничества через SMS, клики, установки приложений. Вредонос распространялся в виде SDK сторонним разработчикам, которые принимали его за рекламную библиотеку и невольно включали в свое приложение. Операторам Chamois удалось заразить около 7,4 миллиона устройств в марте 2018 года. Пользователи видели на своих телефонах предустановленное приложение, которое могло загружать бэкдор Chamois, троян Snowfox и ПО для кликфрода.» ***(Android-устройства могут поставляться со встроенным вредоносным ПО // SecurityLab.ru (https://www.securitylab.ru/news/500403.php). 13.08.2019).***

***

«…Процесс шифрования в космосе проходит не так, как на Земле, и может нарушаться под воздействием космического излучения. В связи с этим Европейское космическое агентство (ЕКА) разработало новый протокол кибербезопасности, который в настоящее время проходит тестирование на международной космической станции (МКС).

Случайное переключение ячеек памяти под воздействием космического излучения звучит маловероятно, и на деле действительно встречается крайне редко. Тем не менее, одного такого инцидента будет достаточно для того, чтобы подорвать всю космическую программу. Если в какой-то момент из-за воздействия космического излучения доступ к спутникам будет отключен, уже ничего нельзя будет сделать.

На крупных, дорогостоящих спутниках, например, GPS, или на межпланетных космических кораблях используются специальным образом защищенные компьютеры, однако они очень дорого стоят и слишком много весят. Когда нужно минимизировать расходы и освободить пространство, такие решения не подходят.

По словам специалиста ЕКА Лукаса Армборста (Lukas Armborst), агентство тестирует два связанных между собой способа защиты компьютеров, неустойчивых к космическому излучению. Для тестирования эксперты используют компьютер Raspberry Pi Zero, практически не внося в него никаких изменений (за исключением незначительных модификаций для соответствия стандартам безопасности МКС).

Эксперимент ЕКА получил название Cryptography International Commercial Experiments Cube (Cryptographic ICE Cube, CryptIC). Первый способ защиты, разработанный в рамках CryptIC, представляет собой довольно традиционный подход – вшитые резервные копии ключей. Если под воздействием космического

излучения произойдет случайное переключение ячеек памяти и ключ шифрования станет непригодным, можно будет воспользоваться запасным ключом.

По подсчетам специалистов, если на пятилетнюю космическую миссию припадет один такой случай, в запасе нужно иметь 20 резервных ключей. Тем не менее, для более продолжительных миссий потребуется что-то понадежнее. Здесь на помощь приходит второй способ, заключающийся в изменении конфигурации аппаратного обеспечения.

По словам Армборста, ядра микропроцессора в CryptIC представляют собой не зафиксированные компьютерные микросхемы, а настраиваемые, программируемые шлюзы. «Эти ядра являются резервными копиями одного и того же функционала. Когда одно ядро выходит из строя, можно использовать другое, а в это время неисправное ядро перезагрузит свою конфигурацию и восстановится», – пояснил Армборст.

Другими словами, программное обеспечение для шифрования будет работать параллельно с самим собой, и одна его часть будет готова к работе и послужит шаблоном для восстановления на случай выхода другого ядра из строя из-за воздействия космического излучения.» ***(На МКС проходит тестирование орбитальных протоколов кибербезопасности // SecurityLab.ru (https://www.securitylab.ru/news/500263.php). 02.08.2019).***

***

«…Используя крошечный электронный имплант, хакер под псевдонимом MG, превратил зарядный кабель Apple в устройство для кражи данных и заражения компьютеров вирусами. Разработка была официально представлена на конференции по кибербезопасности DEFCON 2019.

“Он выглядит как обычный кабель, и работает точно так же. Даже ваш компьютер не заметит разницы. Пока я не возьму удаленное управление кабелем на себя”, - говорит MG.

Кабель с секретом получил название O.MG Cable. Его работа была продемонстрирована прямо на конференции. Как только жертва подключает кабель к компьютеру, хакер получает возможность запускать команды на устройстве. Для этого ему необходимо находиться на расстоянии в 90 метров от цели. По словам разработчика, кабель предоставляет беспрецедентный контроль над компьютером жертвы. “Это все равно, что сидеть за клавиатурой и мышкой жертвы, но не находясь там физически”, - говорит хакер.

Также кабель может быть настроен на автономную работу. В этом случае он тихо и без участия хакера загружает на компьютер вирус.

Самое забавное, что O.MG Cable позиционируется как коммерческий продукт. На DEFCON 2019 MG продавал кабели по $200 за штуку. А в ближайшее время хакер намерен начать сотрудничество с компанией Hak5 и наладить массовый выпуск таких кабелей. По его словам, кабель станет ценным инструментом для обеспечения безопасности.

Конечно, не вполне понятно, как именно разработка подобного рода может способствовать укреплению безопасности. Зато ясно другое - в будущем вы дважды подумаете, прежде чем одалживать у кого-то кабель для подзарядки

смартфона.» ***(Разработан зарядный USB-кабель, заражающий компьютер вирусом // IGate (https://igate.com.ua/news/23833-razrabotan-zaryadnyj-usb-kabel-zarazhayushhij-kompyuter-virusom). 14.08.2019).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«…Исследователь Педро Кабрера (Pedro Cabrera) продемонстрировал на конференции Defcon насколько уязвимы для взлома современные Smart TV, использующие подключенный к интернету стандарт HbbTV. Злоумышленники могут заставить телевизоры показывать любое видео, отображать фишинговые сообщения, запрашивающие пароли пользователя, внедрять кейлоггеры и запускать ПО для криптомайнинга…

Кабрера продемонстрировал, как с помощью квадрокоптера DJI, оснащенного программно-определяемой радиостанцией, можно передавать более мощный сигнал и перекрывать сигнал легитимных телевизионный сетей. Радиус атаки в данном случае зависит только от диапазона и мощности усилителя сигнала.

В другой ситуации исследователь смог управлять стандартом HbbTV, позволяющим телевизорам подключаться к интернету. Кабрера с помощью того же радиосигнала смог обмануть HbbTV умных телевизоров, чтобы они подключались к заданному им URL-адресу web-сервера. По словам исследователя, эта уязвимость не затрагивает стандарт ATSC, используемый в США, поскольку он не отправляет и не извлекает данные из URL-адресов.

Также данную уязвимость злоумышленники могут эксплуатировать для проведения фишинг-атак. По подозрениям исследователя, это может быть эффективнее подобного мошенничества через электронную почту.» ***(Злоумышленники могут с помощью дронов взламывать Smart-TV // SecurityLab.ru (https://www.securitylab.ru/news/500476.php). 15.08.2019).***

***

«…Исследователи из компании Palo Alto Networks обнаружили 34 млн уязвимостей в крупных облачных сервисах. По словам специалистов, проблемы появились не по вине провайдеров, а из-за приложений, которые развертывают клиенты в облаке.

По результатам отчета, охватывающего период с января 2018 года по июнь 2019 года, в сервисе Elastic Compute Cloud от Amazon Web Services специалистами было обнаружено более 29 млн уязвимостей, в Google Compute Engine — около 4 млн, а в Azure Virtual Machine от корпорации Microsoft — 1,7 млн.

Главными причинами возникновения уязвимостей являются устаревшие серверы Apache и уязвимые пакеты jQuery. Также список проблем пополнила растущая популярность контейнерных платформ. Специалисты обнаружили более

23 тыс. контейнеров Docker и чуть более 20 тыс. контейнеров Kubernetes с заводскими конфигурациями, доступными в интернете.

Хакеры также хорошо осведомлены о данной ситуации, говорится в отчете. Около 65% всех атак на облачные сервисы связаны с неправильной конфигурацией. Атаки всегда завершались утечкой данных.

Исследователи также были удивлены количеством вредоносного программного обеспечения для майнинга криптовалюты, в том числе от группировки Rocke.» ***(В Google Cloud, AWS и Azure обнаружили 34 млн уязвимостей // SecurityLab.ru (https://www.securitylab.ru/news/500469.php). 15.08.2019).***

***

«…Уязвимость в Bluetooth, получившая название KNOB, облегчает подбор ключа шифрования, используемого во время подключения устройств, и позволяет манипулировать данными, передаваемыми между двумя девайсами. Проблема затрагивает устройства с поддержкой Bluetooth BR/EDR (Bluetooth Classic) с версиями спецификаций 1.0 - 5.1.

Уязвимость (CVE-2019-9506) позволяет атакующему уменьшить длину ключа шифрования, используемого для установки соединения. В некоторых случаях длину ключа можно уменьшить до одного октета. Благодаря этому злоумышленнику будет гораздо легче осуществить брутфорс-атаку и подобрать ключ шифрования, используемый устройствами при подключении друг к другу.

Заполучив ключ, атакующий может манипулировать передаваемыми между устройствами данными, в том числе внедрять команды, осуществлять мониторинг нажатий клавиш и пр.

Проэксплуатировать уязвимость не так-то легко, и для осуществления атаки требуются определенные условия. Во-первых, оба устройства должны поддерживать Bluetooth BR/EDR. Во-вторых, во время подключения устройств друг к другу атакующий должен находиться поблизости. В-третьих, атакующему устройству нужно успеть перехватить, манипулировать и повторно передать сообщения о согласовании длины ключа между двумя устройствами и одновременно блокировать передачи от обоих.

Кроме того, для получения ключа шифрования мало лишь укоротить его длину, нужно его еще успешно взломать. Атаку требуется повторять при каждом последующем подключении устройств.

Сведения об эксплуатации уязвимости в реальных атаках на данный момент отсутствуют.» ***(Уязвимость KNOB в Bluetooth позволяет манипулировать передаваемыми данными // SecurityLab.ru (https://www.securitylab.ru/news/500467.php). 14.08.2019).***

***

«…ПО, «закопанное» в Windows еще со времен Windows XP, позволяет получить полный контроль над системой. Атака возможна благодаря уязвимости CVE-2019-1162, исправленной компанией Microsoft с выходом обновлений безопасности во вторник, 13 августа.

Исследователь безопасности Тэвис Орманди (Tavis Ormandy) рассказал , как компонент программного интерфейса Text Services Framework (TSF) может использоваться вредоносным ПО или авторизованным злоумышленником для повышения привилегий до уровня системы. Обладая привилегиями на уровне системы, вредонос или киберпреступник может получить полный контроль над компьютером.

Речь идет о компоненте CTextFramework (CTF), присутствующем в TSF со времен Windows XP. «Не удивительно, что такой сложный, непонятный и устаревший протокол полон уязвимостей повреждения памяти. Многие объекты Component Object Model просто доверяют вам маршалирование указателей через порт Advanced Local Procedure Call, а проверка границ или целочисленного переполнения сводится к минимуму», – пояснил Орманди.

По словам исследователя, выполнять некоторые команды может только владелец окна на переднем плане. Тем не менее, злоумышленник может выдать себя за владельца атакуемого Windows-ПК без каких-либо доказательств, просто соврав о своем идентификаторе потока. Поэтому Орманди удалось написать PoC-код, позволивший ему проэксплуатировать уязвимость в CTF через приложение «Блокнот» и запустить оболочку командной строки с привилегиями системы.

«Еще одна интересная атака – захват контроля над диалогом UAC, запущенным как NT AUTHORITY\SYSTEM. Непривилегированный стандартный пользователь может инициировать запуск consent.exe с помощью команды 'runas' ShellExecute() и получить привилегии системы», – сообщил Орманди.

TSF – программный интерфейс, позволяющий выполнять ввод текста, не зависящий от языка и устройств ввода.» ***(Взломать Windows можно через «Блокнот» // SecurityLab.ru (https://www.securitylab.ru/news/500465.php). 14.08.2019).***

***

«…Исследователи из Netflix и Google обнаружили ряд уязвимостей в нескольких реализациях протокола HTTP/2. Эксплуатация уязвимостей позволяет злоумышленникам вызвать отказ в обслуживании на необновленных серверах.

Проблемы затрагивают серверы, поддерживающие HTTP/2. Согласно статистике W3Techs, это составляет 40,0% от всех web-сайтов в интернете.

Всего было обнаружено восемь уязвимостей, которые могут быть проэксплуатированы удаленно. По словам исследователей, все векторы атак являются вариациями одной и той же схемы, когда клиент провоцирует ответ с уязвимого сервера, а затем отказывается его прочитать. В зависимости от возможности сервера управлять очередями, клиент способен использовать его чрезмерную память и ЦП для обработки входящих запросов.

Уязвимостям были присвоены следующие CVE: CVE-2019-9511, CVE-2019-9512, CVE-2019-9513, CVE-2019-9514, CVE-2019-9515, CVE-2019-9516, CVE-2019-9517 и CVE-2019-9518. Их эксплуатация позволяет атакующему запрашивать огромное количество данных по нескольким потокам, отправлять продолжительные пинги HTTP/2-пиру и потоки фреймов или заголовков без имен и

значений на уязвимый сервер. В зависимости от того, как данные будут становиться в очередь и потреблять избыточные ресурсы ЦП, это может привести отказу в обслуживании.

Как сообщает координационный центр CERT, уязвимости затрагивают продукты таких поставщиков, как Amazon, Apache, Apple, Facebook, Microsoft, nginx, Node.js и Ubuntu. Некоторые компании уже исправили обнаруженные проблема, а также зафиксировали несколько безуспешных атак злоумышленников.» ***(В реализациях HTTP/2 обнаружены опасные DoS-уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/500461.php).14.08.2019).***

***

«…Уязвимости в фотоаппаратах Canon позволяют заражать их вредоносным ПО, в том числе вымогательским. Уязвимости можно проэксплуатировать как с помощью беспроводного подключения (по Wi-Fi), так и при подключении фотоаппарата к компьютеру через USB-порт.

Исследователи компании Check Point осуществили реверс-инжиниринг прошивки цифровых зеркальных фотоаппаратов Canon EOS 80D и обнаружили в ней шесть уязвимостей. Если говорить точнее, проблемы связаны с реализацией протокола Picture Transfer Protocol (PTP), используемого для передачи изображений с цифровых камер на ПК и другие носители.

На проходившей на прошлой неделе конференции DEF CON специалист Check Point Эйял Иткин (Eyal Itkin) представил два сценария атак на Canon EOS 80D. Первый предполагает вектор заражения через USB-порт и позволяет заразить фотоаппарат вредоносным ПО. Для реализации второго сценария требуется создать вредоносную точку доступа Wi-Fi. Как только атакующий окажется в одной LAN-сети с камерой, он сможет запустить эксплоит.

По словам исследователя, все шесть уязвимостей (CVE-2019-5994, CVE-2019-5995, CVE-2019-5998, CVE-2019-5999, CVE-2019-6000 и CVE-2019-6001) действительно работают. Наиболее опасной является CVE-2019-5995, позволяющая незаметно для пользователя установить на его устройство вредоносное обновление прошивки.» ***(Уязвимости в Canon EOS 80D позволяют заразить камеру вымогательским ПО // SecurityLab.ru (https://www.securitylab.ru/news/500400.php). 13.08.2019).***

***

«Спеціаліст в галузі кібербезпеки Метт Віксі заявив, що у смартфонів є вразливість, яка дозволяє хакерам отримати доступ до їхніх налаштувань і перетворити пристрій на акустичну зброю.

Зловмисники можуть нашкодити людині, якщо змусять пристрій постійно відтворювати звуки, що дезорієнтують, на високих або низьких частотах.

– У деяких атаках використовувалися відомі вразливості на конкретному пристрої, їх можна реалізувати локально або віддалено. Інші атаки вимагають або близькості до пристрою, або фізичного доступу до нього, – розповів Віксі.

За його словами, для подібного нападу достатньо підключення до пристрою за допомогою Wi-Fi або Bluetooth.

Щоб підтвердити сказане, фахівець зламав кілька гаджетів за допомогою програми-сканера і змусив їх відтворювати неприємні звуки, у результаті чого пристрої вийшли з ладу.» ***(Хакери можуть перетворити звичайний смартфон на зброю – експерт // ФАКТИ. ICTV (https://fakty.com.ua/ua/lifestyle/gadzhety/20190812-hakery-mozhut-peretvoryty-zvychajnyj-smartfon-na-zbroyu-ekspert/). 12.08.2019).***

***

«Американська компанія "Apple" пропонує дослідникам кібербезпеки до одного мільйона доларів, якщо вони знайдуть прогалини в iPhone…

Про це повідомляє CBC із посиланням на компанію…

Проте поточна пропозиція стосується лише прогалин, завдяки яким можна здобути доступ до смартфона на відстані, а не з самого телефону користувачів.

…Apple вже пропонувала винагороду за знахідку прогалин в iPhone, проте, тоді її могли отримати лише дослідники, яких компанія визначала сама.

Наприклад, попередня пропозиція становила 200 тисяч доларів, і її можна було отримати за знахідку незначних багів, які можна було виправити оновленням програмного забезпечення.

Зазначається, що ідея американської компанії з'явилася у той час, коли у світі все більшає побоювань щодо зламу смартфонів дисидентів, журналістів і правозахисників зі сторони влади…» ***(Apple обіцяє до мільйона доларів тим, хто знайде "шпарини" у безпеці iPhone // SVOBODA.FM (http://svoboda.fm/ukraine/267263.html). 09.08.2019).***

***

«В бортовой системе Boeing 787 найдена цифровая уязвимость, сообщил исследователь компании по компьютерной безопасности IOActive Рубен Сантамарта на конференции по кибербезопасности Black Hat в Лас-Вегасе.

Он представил информацию о ряде уязвимостях в коде для компонента самолета Boeing 787 Dreamliner, известного как Crew Information Service/Maintenance System (CIS/MS).

CIS/MS отвечает за такие приложения, как системы технического обслуживания и так называемую «электронную летную сумку» - сборник навигационных документов и руководств, используемых пилотами.

По словам исследователя, использование уязвимостей CIS/MS позволяет злоумышленнику проникать в более чувствительные компоненты, которые управляют критическими для безопасности системами самолета, включая двигатель, тормоза и датчики.

Компания Boeing категорически отрицает возможность такой атаки и отвергает утверждение Сантамарты. В компании утверждают, что архитектура бортовых систем построена таким образом, что подобное проникновение невозможно в принципе.

В отсутствие доступа к системам реальных самолетов Сантамарта, по его собственному признанию, не имеет возможности подтвердить свою гипотезу. Однако настаивает, что даже таких ошибок, как те, что выявил он, в бортовых системах самолетов быть не должно.

Со своей стороны Boeing заявил, что представители корпорации изучили обнаруженные «баги», и пришли к выводу, что никакой угрозы для критических систем (авионики, в частности) они не представляют.» ***(В бортовой системе Boeing 787 найдена цифровая уязвимость // Транспортный бизнес (http://tbu.com.ua/news/v_bortovoi_sisteme_boeing_787_naidena_tsifrovaia_uiazvimost.html). 09.08.2019).***

***

«В мессенджере WhatsApp нашли уязвимость, с помощью которой хакеры могут редактировать диалоги.

Эксперты обнаружили уязвимости в мессенджере WhatsApp, позволяющие злоумышленникам редактировать сообщения пользователей. Об этом сообщается в блоге компании Check Point Research Technologies, специализирующейся на кибербезопасности.

В ходе исследования было обнаружено, что хакеры могут использовать функцию "цитирование" в групповых чатах WhatsApp, чтобы изменить личность отправителя, даже если человек не состоит в группе.

Еще одна уязвимость в приложении позволяет изменять тексты чужих сообщений в личной переписке незаметно для их автора.

Всего специалистами Check Point было выявлено три подобных лазейки в приложении, и компания уведомила о них руководство WhatsApp еще в конце 2018 года, однако две из них по сегодняшний день не устранены разработчиками мессенджера.» ***(Хакеры могут править чужие сообщения в WhatsApp // AOinform (https://www.aoinform.com/news/khakery_mogut_pravit_chuzhie_soobshhenija_v_whatsapp/2019-08-09-31465). 09.08.2019).***

***

«Специалисты компаний Google и Netflix нашли группу DoS-уязвимостей в конфигурациях HTTP/2-серверов крупных вендоров и в аналогичных решениях с открытым кодом. Обнаруженные баги позволяют даже не самому продвинутому злоумышленнику заблокировать сервер — вредоносный клиент обрушит на цель запросы без возможности предоставить адекватные ответы.

По информации на момент публикации, заплатки ко всем уязвимостям выпустила компания Cloudfare, которая работает с решением NGINX. Разработчики Apple и Microsoft залатали по пять дыр, влиявших на их системы. Специалисты Akamai, которые также отметились патчами, в пояснении к уязвимостям сравнили их с атаками на базе Slowloris — эта техника также расходовала ресурсы веб-сервера неполными запросами.

Список затронутых продуктов также включает Ambassador (API Gateway), Apache Traffic Server, Netty Project, nghttp2, Node.js, Envoy (Proxy).

Технически обнаруженные уязвимости похожи друг на друга. Различия заключаются в типе данных, которые перегружают атакуемый сервер:

CVE-2019-9511— манипулирует размерами окна и приоритизацией потоков данных.

CVE-2019-9512— заставляет сервер выстраивать внутреннюю очередь из ответов на множество «пинговых» запросов.

CVE-2019-9513— позволяет злоумышленнику создать многочисленные потоки запросов и постоянно менять их внутреннюю очередность, ломая дерево приоритетов сервера.

CVE-2019-9514— перегружает сервер некорректными потоками, что приводит к созданию чрезмерного количества фреймов RST_STREAM, которые перезапускают такие процессы.

CVE-2019-9515— блокирует работу множеством фреймов SETTINGS, на каждый из которых, согласно спецификации HTTP/2, сервер должен ответить.

CVE-2019-9516—эксплуатирует потоки заголовков с нулевой длиной.

CVE-2019-9517— использует неограниченный буферинг внутренних данных. Для этого взломщику нужно открыть окно HTTP/2 без окна TCP и отправить запрос на некий массивный объект — сервер не сможет подготовить ответ и повиснет.

CVE-2019-9518— применяет потоки фреймов с пустой полезной нагрузкой и без завершающего флага; время обработки таких объектов оказывается непропорционально больше разрешающей способности сетевых каналов.

По словам специалистов Cloudfare, с момента обнаружения уязвимостей они отслеживают появление атак на их основе. На данный момент известно о нескольких локальных инцидентах, но до масштабных атак дело пока не дошло.» ***(Egor Nashilov. HTTP/2-серверы под угрозой DoS-атак // Threatpost (https://threatpost.ru/http2-bugs-allow-dos-attacks/33807/). 16.08.2019).***

***

«В 4G-маршрутизаторах нескольких крупных производителей обнаружены многочисленные уязвимости, подвергающие пользователей опасности утечки информации и атак на выполнение команд.

Исследователь под ником «g richter» из Pen Test Partners поделился сведениями об ошибках, обнаруженных в устройствах 4G, во время конференции хакеров DEF CON в августе этого года. Он заявил, что многие существующие модемы и маршрутизаторы 4G небезопасны - при этом число вендоров, серьезно работающих с сотовыми технологиями, невелико, поэтому их устройства и программное обеспечение применяются повсеместно. Хуже всего то, что «дыры» в безопасности были обнаружены в моделях 4G-маршрутизаторов, охватывающих весь ценовой диапазон - от потребительских устройств до очень дорогих, предназначенных для использования в крупных корпоративных сетях.

Обо всех обнаруженных уязвимостях исследователь сообщил производителям, которые исправили большинство проблем до публикации отчета Pen Test Partners, но, к сожалению, не все прошло гладко. К примеру, известный вендор ZTE поначалу просто отмахнулся от уязвимостей, которые относились в

том числе к устройствам с истекшим сроком эксплуатации. Только после того, как производителю продемонстрировали, что проблемой затронуты маршрутизаторы, указанные как актуальные, компания решила исправить обнаруженные недостатки.

Кроме устройств ZTE, уязвимости были обнаружены в роутерах производства TP-LINK и Netgear. Исследователь Pen Test Partners видит основную проблему в том, что все большее число пользователей предъявляет относительно невысокие требования к полосе пропускания, применяя мобильные технологии для повседневного доступа в Интернет, а с проникновением 5G-сетей их число ещё более возрастет. При этом производители продолжают выпускать устройства для мобильного интернет-доступа, которые с точки зрения безопасности в основном далеки от совершенства.» ***(Уязвимости в ПО 4G-роутеров позволяют получить полный контроль над устройством // IKSMEDIA.RU (http://www.iksmedia.ru/news/5605162-Uyazvimosti-v-PO-4Grouterov-pozvoly.html). 14.08.2019).***

***

«Растущее число атак на устройства интернета вещей объясняется наличием хорошо известных и предсказуемых уязвимостей.

К такому выводу пришли аналитики F-Secure. Они указывают, что при этом число типов угроз для устройств интернета вещей (ИВ-устройств) выросло вдвое только в 2018 г. 87% случаев атак, по данным экспертов, связаны с использованием нелицензионного программного обеспечения и слабых паролей. Также в эту категорию попадают случаи, когда пользователи не меняют пароли, полученные от производителей или поставщиков ИВ-устройств.

В исследовании F-Secure отдельно подчеркивается, что хотя крупные поставщики ИВ-устройств уделяют больше внимания безопасности, чем в прошлом, возможности пользователей по защите от угроз по-прежнему остаются весьма скромными.

«В течение многих лет производители выпускали продукты, не задумываясь об их безопасности, поэтому существует множество умных устройств, уязвимых для относительно простых атак», – констатирует Том Гаффни (Tom Gaffney), консультант по вопросам безопасности в F-Secure.

Согласно опубликованному отчету, угрозы для ИВ-устройств редко встречались до 2014 г. Все изменил выпуск исходного кода вредоноса Gafgyt. Позже, в октябре 2016 г., ботнет Mirai, разработанный на основе кода Gafgyt, стал первым вредоносным ПО для ИВ-устройств, получившим мировую известность. Mirai быстро развивался, а среди его жертв его масштабной DDoS-атаки на инфраструктуру крупного DNS-провайдера Dyn оказались Netflix, Airbnb, Reddit и даже Twitter.

Mirai продолжает оставаться главной угрозой безопасности ИВ-устройств и сейчас. В 2018 г. аналитики F-Secure отметили, что со злосчастным ботнетом связано 59% атак на открытые порты Telnet. Стоит отметить, что если в 2017 г. выделялось пять основных семейств ИВ-вредоносов, то годом позже их стало вдвое больше.

В F-Secure коренной причиной проблемы роста числа атак называют уязвимости в цепочках поставок крупных производителей. Речь идет микросхемах, камерах и других интеллектуальных устройствах, которые серьезные вендоры получают от более мелких подрядчиков.» ***(Главной угрозой устройствам интернета вещей остается безалаберность пользователей // IKSMEDIA.RU (http://www.iksmedia.ru/news/5602977-Glavnoj-ugrozoj-ustrojstvam-interne.htm). 06.08.2019).***

***

«В общей сложности в первой половине 2019 года было обнаружено 11 092 уязвимости.

В первом полугодии 2019 года на долю лишь пяти крупных производителей пришлась почти четверть от всех уязвимостей, указывается в отчете компании Risk Based Security. В общей сложности в указанный период было обнаружено 11 092 уязвимости. Из них 54% относились к web-порталам и приложениям, для 34% проблем были доступны эксплоиты, 53% уязвимостей могли быть проэксплуатированы удаленно, а еще 34% багов не имели «задокументированного решения».

«34% уязвимостей не имеют решения, это может быть связано с тем, что производители не исправляют проблемы. Подобная ситуация может возникнуть в случаях, когда исследователи не информируют вендора о наличии проблемы. Кроме того, если организация использует сканнер уязвимостей, она может не знать обо всех своих активах. Например, если компания не анализирует IP-пространство полностью или использует решения, не способные идентифицировать 100% активов, в таких случаях уязвимости в устройствах и серверах могут оставаться неисправленными», - пояснил специалист Risk Based Security Брайан Мартин (Brian Martin).

Согласно отчету, 2,8% от общего числа багов составили уязвимости в SCADA системах, 4,5% проблем затрагивали защитное ПО, 14,7% уязвимостей получили оценку 9,0 и выше по шкале CVSSv2. Также в документе указывается, что 28,2% уязвимостей, не внесенных в базы CVE/NVD, имели уровень опасности от 7.0 до 10 баллов по классификации CVSSv2. Кроме того, 8,6% уязвимостей, получивших идентификатор CVE, имеют статус RESERVED, несмотря на публичное раскрытие информации о них.» ***(Почти 25% выявленных в 2019 году уязвимостей пришлось на долю 5 крупных вендоров // SecurityLab.ru (https://www.securitylab.ru/news/500641.php). 27.08.2019).***

***

«…Исследователь в области безопасности Лаксман Мутия (Laxman Muthiyah) обнаружил новую уязвимость в приложении для обмена фотографиями и видеозаписями Instagram, позволяющую перехватить контроль над чужой учетной записью.

В июле нынешнего года Мутия сообщил о похожей проблеме, предоставлявшей возможность взломать любой аккаунт за 10 минут. Эксплуатация уязвимости позволяла сбросить пароль для любой учетной записи Instagram и

получить полный контроль над ней. За информацию о баге исследователь получил $30 тыс. в рамках программы вознаграждения за найденные уязвимости.

Как и в предыдущем случае, новая уязвимость позволяет взломать любую учетную запись в Instagram. Мутия выяснил, что один и тот же идентификатор устройства (уникальный идентификатор, применяемый серверами Instagram для проверки кодов сброса пароля) может быть использован для запроса нескольких кодов различных пользователей, в результате позволяя взломать учетные записи в сервисе.

«Существует 1 млн вероятностей шестизначного пароля (от 000001 до 999999). При запросе паролей нескольких пользователей возможность взлома аккаунтов возрастает. Например, если вы запрашиваете пароли 100 тыс. пользователей, используя один и тот же идентификатор устройства, вероятность успеха составит 10%. Если мы запросим пароли для 1 млн пользователей, то сможем с легкостью взломать 1 млн учетных записей», - пояснил Мутия.

Исследователь сообщил о своей находке командам безопасности Instagram и Facebook. В этот раз за информацию об уязвимости он получил $10 тыс.» ***(Уязвимость в Instagram позволяет взломать чужие аккаунты // SecurityLab.ru (https://www.securitylab.ru/news/500625.php). 26.08.2019).***

***

«Сайт, где размещались данные BioWatch, был подвержен опасным и критическим уязвимостям.

Министерство внутренней безопасности США хранило данные национальной анти-биотеррористической программы BioWatch на незащищенном сайте, который в течение более десятка лет оставался уязвимым к хакерским атакам, пишет газета The Los Angeles Times.

По данным издания, информация включала сведения о местоположении ряда устройств для мониторинга биологических угроз, установленных в метро и других публичных локациях в более чем 30 городах США. Каждые сутки система изучает пробы воздуха и передает данные в лаборатории, специалисты которых ищут токсины или патогены. Эти датчики предназначены для обнаружения сибирской язвы и другого воздушного биологического оружия. Кроме того, данные включали результаты тестирования на наличие возможных патогенов, список биологических агентов и планы реагирования на случай атак.

Сведения располагались на сайте, находящемся в ведении частного подрядчика. В мае нынешнего года данный ресурс был отключен. Как отмечает газета, чиновники МВБ признались, что им неизвестно, получали ли хакеры когда-либо доступ к данным.

Web-сайт отображался в выдаче поисковых систем, однако для доступа к конфиденциальной информации требовалось ввести логин и пароль. Аудит безопасности сайта, проведенный в 2017 году, показал наличие опасных и критических уязвимостей, включая ненадежное шифрование, подвергающих ресурс высокому риску кибератак. Важная информация хранилась на портале BioWatch с 2007 года и все это время была уязвима к хакерским атакам.

Неясно, насколько ценными эти данные могли быть для террористических групп и враждебных государств, отмечает издание. Ученые неоднократно предупреждали, что технология BioWatch является ненадежной - система распознает только узкий ряд микробов и не умеет различать типичные бактерии и серьезные угрозы.» ***(Хакеры более 10 лет могли иметь доступ к данным программы мониторинга биологических угроз BioWatch // SecurityLab.ru (https://www.securitylab.ru/news/500624.php). 26.08.2019).***

***

«…В программном обеспечении Lenovo Solution Centre (LSC), предустановленном на миллионах компьютеров Lenovo, обнаружена уязвимость повышения привилегий, с помощью которой злоумышленник может выполнить код и получить права администратора или уровня SYSTEM на атакуемой системе.

Инструмент Lenovo Solution Centre предназначен для диагностики и контроля за состоянием устройств Lenovo. Утилита следит за состоянием батареи, межсетевого экрана и проверяет доступность обновлений драйверов. ПО предустановлено на большинстве устройств Lenovo, включая десктопы и ноутбуки.

Как пояснили исследователи из Pen Test Partners, проблема (CVE-2019-6177) связана с DACL (Discretionary Access Control List, список избирательного управления доступом), то есть высокопривилегированный процесс Lenovo может перезаписать разрешения файла, которым может управлять пользователь с низкими привилегиями. Данная уязвимость предоставляет возможность атакующим с ограниченным доступом к компьютеру записать жесткую ссылку на файл в контролируемую локацию.

«Процесс Lenovo перезаписывает привилегии такого файла, что позволяет пользователю с низкими правами управлять файлами, которыми в обычной ситуации он управлять не может. Этим можно воспользоваться для выполнения произвольного кода на системе с правами администратора или системными привилегиями», - пишут исследователи.

Уязвимость затрагивает версию Lenovo Solution Centre 03.12.003. По словам производителя, LSC не поддерживается с апреля 2018 года. Тем не менее, на сайте Lenovo утилита по-прежнему доступна для загрузки. Компания признала наличие проблемы и порекомендовала пользователям деинсталлировать Lenovo Solution Centre и прейти на использование ПО Lenovo Vantage или Lenovo Diagnostics.» ***(Уязвимость в предустановленном ПО позволяет взломать ноутбуки Lenovo за 10 минут // SecurityLab.ru (https://www.securitylab.ru/news/500606.php). 25.08.2019).***

***

«…Компания Mozilla выпустила обновление для браузера Firefox, исправляющее уязвимость в менеджере паролей. Эксплуатация уязвимости (CVE-2019-11733) позволяет злоумышленнику копировать пароли в «сохраненных учетных данных» без ввода мастер-пароля.

После установки мастер-пароля необходимо ввести его, прежде чем к паролям можно будет получить доступ в диалоговом окне «сохраненные учетные данные». По словам исследователей, злоумышленник способен копировать локальные данные в буфер обмена с помощью пункта контекстного меню «копировать пароль» без предварительного ввода мастер-пароля.

Разработчики рекомендуют пользователям Firefox обновить браузер до версии 68.0.2 в целях безопасности.

Несмотря на быстрое исправление новых уязвимостей, Firefox не обращает внимание на некоторые старые. Так, например, в начале июля нынешнего года независимый эксперт Барак Тавили (Barak Tawily) продемонстрировал способ хищения данных через 17-летнюю уязвимость.» ***(В браузере Firefox исправили уязвимость обхода мастер-пароля // SecurityLab.ru (https://www.securitylab.ru/news/500489.php). 16.08.2019).***

***

«…Как известно, неуязвимых систем не бывает. Ежегодно идентификаторы CVE присваиваются тысячам обнаруженных уязвимостей, и следить за каждой новой практически не реально. Как понять, какие из них компаниям следует исправлять в первую очередь, а с какими можно повременить, пытались разобраться специалисты на конференции Black Hat USA, проходившей на прошлой неделе в Лас-Вегасе.

Эксперты компании Kenna Security Майкл Ройтман (Michael Roytman) и компании Cyentia Institute Джей Джейкобс (Jay Jacobs) назвали управление уязвимостями «злостной проблемой», поскольку оно не соизмеримо с количеством обнаруживаемых уязвимостей. По их словам, каждый месяц исправляется всего 10% от всех уязвимостей. Их слишком много, чтобы компании могли исправить все, поэтому необходимо разработать стратегию, которая решила бы эту проблему, считают специалисты.

Новая стратегия должна помочь организациям разобраться, какие уязвимости действительно необходимо исправлять. Теоретически, в этом должна помочь система оценки CVSS – чем выше оценка, тем серьезнее проблема. Тем не менее, все уязвимости, получившие 7 и выше баллов согласно CVSS, считаются критическими. Таких «критических» уязвимостей все равно слишком много и понять, какие из них должны быть в приоритете, невозможно. «CVSS просто DoS-ит ваши политики установки патчей и заставляет бросать деньги на ветер», - отметили Ройтман и Джейкобс.

По словам исследователей, только 2-5% от всех критических уязвимостей действительно эксплуатируются в реальных атаках. Поэтому нужно создать систему оценки опасности уязвимостей, которая принимала бы в учет потенциальную возможность их эксплуатации на практике.

Такой системой может стать Exploit Prediction Scoring System (EPSS), представленная Ройтманом и Джейкобсом на Black Hat USA. Для определения возможности реальной эксплуатации уязвимости EPSS использует более десятка критериев. Сюда входит CVE, оценка CVSS, наличие PoC-эксплоитов и эксплоитов, используемых киберпреступниками, операционная система, вендор и прочие переменные. Учтя все вышеперечисленные критерии, EPSS выдает процент вероятности эксплуатации той или иной уязвимости в реальных атаках.

Исследователи выпустят свою систему в виде как алгоритма для реализации в других продуктах, так и online-калькулятора.» ***(Представлена система оценки вероятности использования уязвимостей в реальных атаках // SecurityLab.ru (https://www.securitylab.ru/news/500398.php). 13.08.2019).***

***

«…Специалист подразделения Microsoft Defender ATP Research Бхавна Соман (Bhavna Soman) представил на конференции Black Hat USA 2019, состоявшейся на этой неделе в Лас-Вегасе, систему автоматизации неструктурированных текстовых данных для анализа безопасности и сбора информации об угрозах.

С помощью технологий машинного обучения и обработки естественного языка система идентифицирует и извлекает из неструктурированного текста шаблоны, описывающие подробности о кибератаках. Система обучена распознавать известные угрозы и способна из неструктурированного текста извлекать сведения об атакующем, методах осуществления атаки, семействах вредоносного ПО.

В процессе обработки естественного языка извлечение именованного объекта используется для классификации текстовых фраз по заранее установленным категориям. Как правило, этот процесс предшествует более сложным задачам, таким как идентификация псевдонимов, связи между атакующими и их тактик, техник и процедур и т.д.

Для обучения модели искусственного интеллекта (ИИ) специалисты Microsoft Defender ATP Research использовали текстовую базу данных, состоящую более чем из 2,7 тыс. публично доступных документов, описывающих действия, поведение и инструменты различных киберпреступников. Каждый документ в БД состоял в среднем из двух тысяч токенов.

В дополнение к традиционным функциям, применяемым в процессе обработки естественного языка (словарная форма, части речи и орфография), специалисты также экспериментировали с кастомизированным вложением слов, что дало им возможность выявлять связи между двумя словами, имеющими одно и то же значение или используемыми в одном контексте.

Разработанная специалистами система придет на помощь там, где одного лишь сбора индикаторов компрометации (IoC) недостаточно. IoC наподобие IP-

адресов, доменных имен и хешей файлов легко получить, но их также легко можно подделать с целью обхода обнаружения.» ***(Система на базе ИИ использует обработку естественного языка для выявления угроз // SecurityLab.ru (https://www.securitylab.ru/news/500350.php). 09.08.2019).***

***

«В надежде добавить популярности модели безопасности с нулевым доверием (zero-trust) BeyondCorp среди своих корпоративных клиентов, компания Google вчера усовершенствовала облачный сервис Identity-Aware Proxy возможностью контекст-ориентированного доступа.

Модель безопасности с нулевым доверием перемещает контроль доступа с периметра сети на индивидуальные устройства и пользователей. Она позволяет служащим безопасно работать независимо от местоположения, не используя традиционного VPN-клиента, межсетевого экрана, без необходимости предоставлять виртуальным машинам публичные IP-адреса.

Google создала такую модель для внутреннего пользования в 2010 году, после того как стала жертвой атаки китайских хакеров, похитивших интеллектуальную собственность из её сети.

Модель нулевого доверия не делает различия между пользователем внутри и снаружи корпоративной сети. Как результат, решение о предоставлении доступа принимается на основании информации о конкретном пользователе, о роде его занятий, местоположении и статусе безопасности используемого им устройства.

Google уже несколько лет пытается убедить предприятия в преимуществах модели нулевого доверия. Недавно она реализовала возможности контекст-ориентированного доступа в сервисе IAP, чтобы помочь защитить организации от неавторизованного проникновения в их виртуальные машины. Анонсированные в январе в ознакомительном варианте (preview), эти возможности теперь стали полноценно доступны, о чём в блоге сообщил менеджер продукта Google Cloud, Христиан Бранд (Christiaan Brand).

Доступ к новой функциональности осуществляется с панели администрирования Google Cloud Platform.» ***(Google расширила модель нулевого доверия контекстным доступом для ВМ // «Компьютерное Обозрение» (https://ko.com.ua/google_rasshirila_model_nulevogo_doveriya_kontekstnym_dostupom_dlya_vm_129737). 08.08.2019).***

***

«Незалежна лабораторія AV-TEST оприлюднила результати чергового етапу тестування антивірусів для домашнього використання на Windows. Найкращим антивірусом визнали вбудований у Windows продукт — Microsoft Defender 4.18.

Як повідомляє PCmag, Microsoft Defender 4.18. набрав максимальні 18 балів за рівень захисту, продуктивність та інтерфейс. Такі ж оцінки отримали F-Secure SAFE, Kaspersky Internet Security та Symantec Norton Security, але ці антивіруси працюють на основі передплати.

Інші популярні продукти, такі як Avast Free Antivirus, AVG Internet Security, Bitdefender Internet Security, Trend Micro Internet Security, VIPRE Security AdvancedSecurity, набрали 17,5 балів.

Найгіршим антивірусом виявився Webroot SecureAnywhere з результатом 11,5 балів. Він отримав 2 бали за захист, 5,5 балів за продуктивність та 4 бали за інтерфейс…» ***(Експерти назвали найкращий антивірус для Windows // MediaSapiens (https://ms.detector.media/web/cybersecurity/eksperti_nazvali_naykraschiy_antivirus_dlya_windows/). 07.08.2019).***

***

«Компания Google подвела первые итоги работы расширения Password Checkup, предупреждающего пользователей Chrome о скомпрометированных паролях. По информации производителя, плагин установили более 650 тыс. пользователей браузера, однако лишь четверть из тех, кто получил предупреждение о небезопасном пароле, изменили его. Вендор выпустил обновление программы, добавив возможность обратной связи с разработчиками и возможность отказаться от отправки анонимизированной статистики.

Ежемесячно Password Checkup проверяет десятки миллионов паролей в Chrome

По информации Google, за первый месяц после выпуска расширения оно проверило 21 млн пар логин-пароль. Каждый раз при вводе учетных данных плагин обращался к базе данных скомпрометированных учетных записей и, обнаружив совпадения, предупреждал пользователя об угрозе угона аккаунта. Как заявили разработчики, расширение Password Checkup пометило как ненадежные 315 тыс. паролей, что составляет около 1,5% от общего числа проверок.

Специалисты отмечают, что лишь 26% предупрежденных пользователей решили сменить пароль. При этом около 15% из них выбрали в качестве нового секретного ключа ненадежную последовательность символов, которую легко подобрать. К позитивным результатам работы плагина можно отнести тот факт, что более 60% новых паролей оказались устойчивыми к брутфорс-атакам.

Согласно анонимной статистике, собранной расширением Password Checkup, чаще всего пользователи используют слабые пароли на развлекательных сайтах — количество срабатываний плагина на таких ресурсах доходило до 6,3% от общего числа проверок. Для онлайн-магазинов этот показатель составил 1,2%, а для почтовых сервисов — всего полпроцента.

Google выпустила Password Checkup в феврале этого года. В его базе содержится информация о более чем 4 млрд скомпрометированных учетных записей. Для того чтобы не допустить утечки данных при передаче сведений об используемом пароле, создатели расширения применили многоэтапную технологию хэширования данных, созданную при содействии ученых Стэнфордского университета. В новой версии программы разработчики предоставили пользователю возможность отказаться от участия в сборе анонимной статистики, а также напрямую отправить сообщение в службу поддержки продукта.» ***(Julia Glazova. Более 650 тыс. пользователей установили Password***

Checkup // Threatpost (https://threatpost.ru/password-checkup-plugin-installed-by-over-650-thousand-users/33826/). 20.08.2019).

***

«…На этой неделе состоялся релиз бесплатного инструмента для проведения диагностики систем на предмет наличия в них уязвимостей Urgent/11.

Напомним , в прошлом месяце в операционной системе реального времени (ОСРВ) VxWorks от компании Wind River Systems были обнаружены 11 уязвимостей, позволяющих злоумышленникам захватить контроль над уязвимыми устройствами. Проблемы затрагивают версии VxWorks 6.9.4.11, Vx7 SR540 и Vx7 SR610. В каждой из них присутствует одна или более уязвимостей, позволяющих удаленно выполнить код, осуществить DoS-атаку или похитить информацию.

По данным обнаруживших Urgent/11 экспертов компании Armis, уязвимости затрагивают более 200 млн критически важных устройств, используемых в том числе в критической инфраструктуре, технологической сфере и сфере промышленной автоматизации.

Для того чтобы создать карту присутствующих в сети уязвимых устройств, предприятию потребуется провести полную инвентаризацию моделей и версий прошивки, а это весьма непростая задача. Однако без такой видимости выявить уязвимые устройства и привести их в соответствие к требованиям не представляется возможным.

Компания Claroty решила упростить задачу операторам АСУ ТП и выпустила бесплатный диагностический инструмент с открытым исходным кодом. Инструмент предназначен для выявления одной из уязвимостей Urgent/11 (CVE-2019-12258), позволяющей осуществить DoS-атаку.

Инструмент доступен для загрузки на сайте GitHub.» ***(Вышел бесплатный инструмент для выявления уязвимостей Urgent/11 // SecurityLab.ru (https://www.securitylab.ru/news/500602.php). 23.08.2019).***

***

«…В течение следующих 15-20 лет кибербезопасность медицинского оборудования будет оставлять желать лучшего, считают эксперты. Толковые руководства по обеспечению безопасности устройств, используемых в здравоохранении, уже составлены и выпущены, однако оборудование, которое будет им соответствовать, войдет в обиход еще не скоро. Об этом сообщил старший директор по информационной безопасности сети больниц Ramsay Health Care Кристофер Нил (Christopher Neal) на конференции Gartner Security and Risk Management Summit.

«Все (медицинское оборудование – ред.), что вы покупаете сегодня, вероятнее всего, не было создано с учетом безопасности. Эта проблема будет оставаться актуальной в сфере здравоохранения в течение последующих 15-20 лет», – уверен Нил.

По словам Нила, когда он устроился на работу в Ramsay Health Care, понять, где расположены IT-системы и какие устройства подключены, было сложно, и какой-либо зафиксированный централизованный список активов отсутствовал.

Если архитектура корпоративной сети является плоской, то медицинские сети в каждой больнице разделяются с использованием DMZ. Нил заключил, что, не имея никакой информации об устройствах, он не сможет обеспечить их безопасность, в связи с чем начал создавать карту устройств во всех 74 больницах Ramsay Health Care.

В процессе картирования Нил обнаружил большое количество устройств с заводскими учетными данными и настройками, причем не в корпоративной сети, а в DMZ. Однако переходить на модель «нулевого доверия» (zero trust) Ramsay Health Care еще не готова. Для принятия данной модели безопасности организация должна достичь определенного уровня организационной и IT-зрелости, и здесь Ramsay Health Care еще есть куда расти.

По словам Нила, зрелая организация может перейти на «нулевое доверие» в течение 2-3 лет. Однако попытка форсировать события и освоить эту концепцию в более быстрые сроки может закончиться провалом, предупредил эксперт…» ***(Медицинское оборудование будет представлять угрозу безопасности еще 15-20 лет // SecurityLab.ru (https://www.securitylab.ru/news/500576.php). 22.08.2019).***

***

«Компания Eaton представила новые возможности карт Gigabit network и Industrial Gateway. По ее заявлению, это первые в отрасли устройства для подключения ИБП, соответствующие стандарту кибербезопасности UL 2900-2-2-2. До сих пор Gigabit network поддерживала только однофазные ИБП, но последние обновления позволяют подключать карту к 3-фазным ИБП Eaton 93PM, Eaton 93PS, Eaton 91PS и Eaton 9PHD, чтобы обеспечивать новые функции и протоколы подключения для крупных центров обработки данных и промышленного оборудования.

Карты соответствуют стандарту UL 2900-2-2-2, который обеспечивает высочайший уровень защиты оборудования от угроз кибербезопасности. Средства кибербезопасности включают усиленное шифрование, настраиваемые режимы работы с паролями, маркированную прошивку и использование цифровых сертификатов. Используя функции системного журнала карты, ИТ-менеджеры могут централизованно отслеживать и получать уведомления о действиях входа на каждую карту, обеспечивая своевременное обнаружение подозрительной деятельности, что обеспечивает дополнительную кибербезопасность. Новые функции, доступные в Gigabit network card, включают удаленную и централизованную аутентификацию через LDAP/Active Directory и Radius.

«С тех пор как Gigabit Network Eaton была выпущена чуть более полугода назад, в отрасли наблюдается феноменальный отклик, — говорит менеджер по продуктам Eaton Тату Вальякка. — Эти карты предназначены для обеспечения повышенной безопасности подключенных ИБП. Последние улучшения позволяют ИТ-специалистам и руководителям объектов использовать одни и те же сетевые

карты для однофазных и трехфазных ИБП, что упрощает управление и мониторинг и, в конечном счете, повышает уровень кибербезопасности».

Eaton также представляет карту Industrial Gateway, которая совместима с протоколом связи MODBUS. Эта карта имеет ту же защиту от киберугроз, что и сетевая карта, и предназначена для управления зданиями, промышленными объектами и крупными центрами обработки данных. Карта усиливает защиту, предоставляемую ИБП, обеспечивая мониторинг в реальном времени его системы и окружающей среды через систему управления зданием (BMS) или систему промышленной автоматизации (IAS). Карта позволяет менеджерам объекта контролировать состояние ИБП, условия электропитания, температуру и влажность в сети ИБП, что позволяет заблаговременно предупреждать о любых угрозах системе.

Карты Gigabit Network и Industrial Gateway позволяют обновлять функции и безопасность, а также обладают увеличенной памятью и возможностью «горячей» замены внешних компонентов. Обе карты совместимы с новым датчиком мониторинга окружающей среды Eaton для определения влажности, температуры и контактных входов и обеспечивают эффективный мониторинг среды в стойке.

У Gigabit Network и Industrial Gateway есть дополнительные функции, с помощью которых можно последовательно подключать до трех датчиков нового поколения на одну карту и на больших расстояниях, что важно для таких приложений мониторинга, как естественное охлаждение. При использовании с Eaton Intelligent Power Manager (IPM) карты улучшают непрерывность бизнеса, обеспечивают работу критически важных приложений. Кроме того, они совместимы с широко распространенными сегодня гигабитными сетевыми коммутаторами.» ***(Eaton наделяет карты Gigabit network и Industrial Gateway новыми возможностями по мониторингу и кибербезопасности // Компьютерное Обозрение (https://ko.com.ua/eaton_nadelyaet_karty_gigabit_network_i_industrial_gateway_novymi_vozmozhnostyami_po_monitoringu_i_kiberbezopasnosti_129921). 27.08.2019).***

***

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

Бодрецький М. В. Антикризове управління: боротьба з шахрайством із використанням електронного обладнання (ПТКС) / М. В. Бодрецький // Науковий вісник Львівського державного університету внутрішніх справ. серія економічна. - 2018. - Вип. 2. - С. 3-10.

Подано результати останніх досліджень у сфері методів і принципів, що застосовуються кібершахраями в Україні. Описано обладнання шахраїв. Надано науково обґрунтовані рекомендації для забезпечення мінімізації витрат банківської установи як складової антикризових дій у сфері управління банком.

Шифр зберігання НБУВ: Ж70364/ек

***

Захист прав людини: міжнародний та вітчизняний досвід = Human rights protection: International and Ukrainian experience : матеріали І Міжнар. наук.-практ. конф., 16 трав. 2019 р. - Київ, 2019. - 711 с.

Зі змісту:

- Петров С.Г. Права людини і завдання кіберзахисту об’єктів критичної інформаційної інфраструктури.

Шифр зберігання НБУВ: ВС65990

***

Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій, призначення комп'ютерно-технічних судових експертиз : наук.-практ. посіб. - Київ : Паливода А. В., 2019. - 167 с.

Наведено кримінально-правову характеристику злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Висвітлено проведення слідчих (розшукових) дій. Окреслено завдання, об’єкти та питання комп'ютерно-технічних судових експертиз.

Шифр зберігання НБУВ: ВА834381

***

Інтегровані інтелектуальні робототехнічні комплекси (ІНТК-2019). Дванадцята міжнародна науково-практична конференція, 21-22 травня 2019 р., Київ, Україна : зб. тез. - Київ, 2019. - 279 с.

Зі змісту:

- Бахмач А.В. Аналіз моделей криптографічного захисту інформації на інформаційних носіях;
- Єгоров С.В., Шкварницька Т.Ю. Базовий статичний аналіз шкідливого коду в Windows;
- Орлова М.М., Гришин С.О. Способи виявлення та попередження D(DOS)-атак на контролер в програмно-конфігурованих мережах SDN;
- Черненко П.Р., Орлова М.М. Аналіз загроз безпеки ОС Android та їх виявлення;
- Шевель О.С. Аналіз безпеки Telegram.

Шифр зберігання НБУВ: ВА834415

***

Інтернет речей: проблеми правового регулювання та впровадження. Друга науково-практична конференція, 29 листопада 2018 року. - Київ : КПІ ім. І. Сікорського, 2018. - 166 с.

Зі змісту:

- Заярний О.А. Деякі проблеми правового забезпечення правомірної обробки біометричних персональних даних у процесі використання Інтернету речей;

- Неділько Я.В. Поняття кіберзлочину та особливості його закріплення в національному законодавстві;
- Гущин О.О., Роллер В.М. Кіберпростір як новітній вимір безпеки і оборони України;
- Довгаль Ю.С. Безпека мережевих та інформаційних систем;
- Алексєєв М.М. Кроки Польщі щодо протидії кібернетичним загрозам: досвід для України;
- Фарадж Д.Ю. Сучасний стан забезпечення кібербезпеки в Україні;
- Стародубов В.В. Кібербезпека в умовах розвитку права Республіки Білорусь.

Шифр зберігання НБУВ: ВА834165

***

Інформаційне право: сучасні виклики і напрями розвитку : матеріали першої наук.-практ. конф., 18 жовт. 2018 р. - Київ : КПІ ім. Ігоря Сікорського : Політехніка, 2018. - 195 с.

Зі змісту:

- Бежевець А.М. Кіберпростір як необхідна складова кібербезпеки суспільства.

Шифр зберігання НБУВ: ВА834030

***

Калиновський О. В. Застосування класичних методів криміналістики та сучасних технологічних можливостей у приватній детективній практиці при розслідуванні кібершахрайства / О. В. Калиновський, Р. О. Болгов // Держава і право. Юридичні науки. - 2019. - Вип. 83. - С. 269-280.

Подано ознаки, за якими можна розпізнати інтернет-шахрая. Розкрито механізми протидії та запобігання таких злочинів. Наведено приклади викриття деяких кібершахрайських схем як за допомогою класичних методів криміналістики так і з використанням сучасних технологічних можливостей. Висвітлено унікальний досвід досудового розслідування з залученням приватних детективів, співробітників Департаменту кіберполіції Національної поліції України та журналістів.

Шифр зберігання НБУВ: Ж69395/юрид.н.

***

Лісовська Ю. П. Адміністративно-правовий захист критичної нформаційної інфраструктури в сучасному кіберпросторі /Ю. П. Лісовська // Держава і право. Юридичні науки. - 2019. - Вип. 83. - С. 161-171.

Розглянуто нормативні аспекти підстав й умов застосування сили щодо захисту критичної інфраструктури від будь-яких загроз. Проаналізовано сучасні технології, що впливають на технічні засоби критичної інфраструктури.

Шифр зберігання НБУВ: Ж69395/юрид.н.

***

Москаль О.Б. Розробка захищеного чату та його впровадження в соціальну мережу / Москаль О.Б., Цвєткова Т.П. // Вісник навчально-

наукового інституту автоматики, кібернетики та обчислювальної техніки НУВГП.- 2018.- Вип. 5.- С. 53-59.

Проведено дослідження конфіденційної інформації в популярних соціальних мережах. Запропоновано алгоритм шифрування даних та realtime видалення прочитаних повідомлень, що забезпечує конфіденційність надісланих та отриманих даних.

Шифр зберігання НБУВ: Ж74638

***

Назарчук В.Д. Методика оцінки загроз в системах електронного документообігу, призначених для навчально-наукових процесів / Назарчук В.Д., Зварич А.В. // Вісник навчально-наукового інституту автоматики, кібернетики та обчислювальної техніки НУВГП.- 2018.- Вип. 5.- С. 35-46.

Подано аналіз та рекомендації щодо оптимізації визначення необхідних компонентів функціонування комплексів засобів захисту із врахуванням специфіки освітньо-наукової діяльності.

Шифр зберігання НБУВ: Ж74638

***

Научно-техническая конференция «Перспективные сетевые и компьютерные технологии (ПерСиК 2019)», Украина, Харьков - 2019 = Perspective network and computer technologies : материалы конф. - Харьков, 2019. - 128 с.

Зі змісту:

- Ємельянова В.В. Розробка програмних компонентів забезпечення кібербезбеки у циклі розробки ПО;
- Климов В.С., Семенец В.М. Десять самых критичных угроз безопасности WEB приложений по версии OWASP 2017 года;
- Воронько В.О. Аналіз можливості детальної класифікації загрозам базам даних;
- Шорский А.Э. Устройство для безопасносного хранения информации PRIVATEBOX.

Шифр зберігання НБУВ: ВА833550

***

Національна безпека у фокусі викликів глобалізаційних процесів в економіці. ІІІ-тя Міжнародна наукова Інтернет-конференція, 15-17 лютого 2019 року. - Київ ; Баку, 2019. - 111 с.

Зі змісту:

- Нестеренко О.В., Нетесін І.Є., Поліщук В.Б., Шевченко В.Л., Шевченко А.В. Прогностичне моделювання зараження комп'ютерними вірусами веб-ресурсів органу державного управління на основі епідеміологічного підходу.

Шифр зберігання НБУВ: ВА833553

***

Сучасна цивілістика в умовах Євроінтеграції : матеріали XIV Міжнар. наук.-практ. конф., 11-12 квіт. 2019 р., м. Одеса. - Одеса : Юридична література, 2019. - 618 с.

Зі змісту:

- Гедіков В.В., Звєрєва Т.В. До питання забезпечення кібербезпеки на міжнародній арені;
- Кулішова Л.В. Регулювання охорони і захисту персональних даних у сфері ІТ-права.

Шифр зберігання НБУВ: ВА834124

***